DISSERTAÇÃO DE MESTRADO PROFISSIONAL

# 3SW: Um Modelo Adaptado do CIS Controls v8.1 para Mitigação de Ameaças a Servidores Web

**Tássio Correia da Silva**

**Orientadora Profa. Dra. Fabiana Freitas Mendes**

Programa de Pós-Graduação Profissional em Engenharia Elétrica

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

# 3SW: Um Modelo Adaptado do CIS Controls v8.1 para Mitigação de Ameaças a Servidores Web

# 3SW: An Adapted CIS Controls v8.1 Model for Web Server Threat Mitigations

**Tássio Correia da Silva**

**Orientadora: Profa. Dra. Fabiana Freitas Mendes, FGA/UnB**

PUBLICAÇÃO: PPEE.MP.098

BRASÍLIA-DF

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

# 3SW: Um Modelo Adaptado do CIS Controls v8.1 para Mitigação de Ameaças a Servidores Web

**Tássio Correia da Silva**

**Orientadora Profa. Dra. Fabiana Freitas Mendes**

*Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica*

Banca Examinadora

Prof. Dra. Fabiana Freitas Mendes, PPEE/UnB _____
*Presidente*

Prof. Dr. Rafael Rabelo, PPEE/UnB _____
*Examinador Interno*

Prof. Dr. Altair Olivo Santin, PPGI/PUC-PR _____
*Examinador externo*

Profa. Dra. Edna Dias Canedo, PPEE/UnB _____
*Suplente*

**FICHA CATALOGRÁFICA**

DA SILVA, TÁSSIO CORREIA
3SW: Um Modelo Adaptado do CIS Controls v8.1para Mitigação de Ameaças a Servidores Web [Distrito Federal] 2025.
xvi, 88 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2025).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica
1. Segurança da Informação
2. CIS Controls
3. Administração Pública
4. Servidores Web
I. ENE/FT/UnB
II. Título (série)

**REFERÊNCIA BIBLIOGRÁFICA**

DA SILVA, T. C. (2025). *3SW: Um Modelo Adaptado do CIS Controls v8.1para Mitigação de Ameaças a Servidores Web* . Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 88 p.

**CESSÃO DE DIREITOS**

AUTOR: Tássio Correia da Silva
TÍTULO: 3SW: Um Modelo Adaptado do CIS Controls v8.1para Mitigação de Ameaças a Servidores Web .
GRAU: Mestre em Engenharia Elétrica ANO: 2025



---

Tássio Correia da Silva
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

## DEDICATÓRIA

Dedico esta dissertação à memória da minha avó, Dona Argentina, e do meu tio Ary. Pessoas incríveis, de um coração sem igual, que sempre acreditaram em mim e, ao partirem, deixaram um vazio enorme. Que Deus os tenha em um ótimo lugar. Não seria nada sem eles.

## AGRADECIMENTOS

Inicio esta etapa com o maior dos agradecimentos a Deus, por permitir-me ter a ímpar oportunidade de cursar o mestrado. Há uma frase que diz: “o processo é mais importante que o resultado”. Sem dúvidas, viver esse processo trouxe ganhos muito maiores que o próprio resultado. O método científico é uma ferramenta valiosa que, a partir deste mestrado, levarei para a vida.

Agradeço especialmente aos meus pais, minhas tias, meus primos e amigos, que me deram força para continuar e foram pacientes nos momentos em que precisei abdicar de seu convívio.

Expresso também minha gratidão aos meus colegas de turma pelo compartilhamento de experiências. Em especial, agradeço ao Paulo Victor, que esteve ao meu lado em grande parte dessa jornada. Essa é uma das grandes vantagens de um mestrado profissional: aproximar a academia do setor laboral, enriquecendo ambos os lados.

Sou profundamente grato a todos os professores que me guiaram nessa jornada. Entre eles, Rafael Rabelo, Robson, Georges, Giozza, Demétrio e, em especial, à professora Fabiana Mendes, que foi incansável ao me orientar na conclusão deste trabalho e me ensinar mais sobre o método científico. Os professores talvez não compreendam a magnitude do impacto que têm em nossas vidas, mas sua dedicação nos contagia e nos motiva a seguir em frente. Sinto-me honrado por ter vivido e aprendido com vocês.

Não posso deixar de agradecer aos meus colegas de trabalho pelo apoio durante essa etapa. Em especial, agradeço ao meu chefe, Vinícius Eloy, que foi o maior incentivador para que eu iniciasse o mestrado. Sem esse apoio e incentivo, dificilmente teria dado início a essa fase da vida de aprendizado.

Também adiciono agradecimento ao meu parça Luiz, que me acompanhou na jornada pré PPEE e fez o dia-a-dia ser mais interessante. Ao meu grande mentor Ney, cujos ensinamentos levo para a vida.

Um obrigado muito especial a Ana e a Cláudia por transformarem a pausa para o almoço em um momento único e muito desejado por mim. Estar com vocês foi divertido e de muito aprendizado.

Aos meus amigos de longa data — Deivison, Igor, Jamisson, Adson, Vladson, Kléber e Rafael — minha gratidão eterna. Apesar da distância e do tempo transcorrido, sempre que nos encontramos, o prazer do convívio permanece o mesmo, como se o tempo não tivesse passado. Exceto, é claro, pelas “garagens” e as novas pavimentações em branco no piso cabeludo!

Um outro amigo de longa data e que merecia um parágrafo separado é o José Thiago, compartilhamos muitas alegrias indo ver nosso clube do coração ao longo desses últimos 20 anos, em especial a Copa do Brasil em 2008. Que venham mais alegrias e não poderia faltar: Pelo Sport Tudo!

Por fim, a todos vocês, nomeados ou não, que participaram direta ou indiretamente desta jornada, saibam que são especiais para mim. Registro, mais uma vez, meus mais sinceros votos de agradecimento.

## RESUMO

A crescente dependência tecnológica e expansão dos serviços digitais, aliada ao aumento expressivo das ameaças cibernéticas, exige que a Administração Pública eleve sua maturidade em segurança da informação, especialmente em relação aos ativos críticos, como os servidores web. Dessa forma, há a necessidade de reduzir riscos imediatos e fortalecer a segurança cibernética por meio de ações práticas, aplicáveis e priorizadas.

Esta dissertação propõe o modelo 3SW (Subconjunto de Salvaguardas para Servidores Web), um conjunto específico de medidas de segurança derivadas do CIS Controls v8.1, voltado à proteção de servidores web em ambientes institucionais.

A metodologia da pesquisa para a construção do 3SW baseou-se em uma adaptação da análise de conteúdo proposta por Bardin, estruturada em três fases: Pré-análise, Aplicação de Critérios e Análise dos Resultados. A partir de critérios qualitativos, foram selecionadas 93 medidas de segurança distribuídas em 17 dos 18 controles do CIS Controls v8.1, com foco exclusivo em servidores web. O modelo foi então validado por meio de um estudo de caso. Inicialmente foi realizado um diagnóstico na organização no qual o modelo seria aplicado utilizando-se de análise documental e entrevistas. O modelo 3SW foi então aplicado ao Sistema Alpaca, enquanto o modelo de referência WAH (Web Application Hacking do Commmunity Defense Model) foi utilizado no Sistema Lhama. Finalmente, os resultados obtidos foram comparados com objetivo de concluir sobre a efetividade do 3SW.

O diagnóstico apontou que, embora o CIS Controls já fosse adotado na organização por meio do Programa de Privacidade e Segurança da Informação (PPSI), sua aplicação generalista não atendia com precisão as demandas dos servidores web. Dentre as limitações observadas estão a ausência de foco por ativo e a baixa granularidade nas escalas de avaliação.

A comparação dos resultados de aplicação dos modelos nos dois sistemas indicou que o modelo 3SW alcançou 82% de efetividade (76 de 93 medidas implementadas) e 97% de cobertura de mitigações ativas (baseadas no MITRE ATT&CK). Já o modelo WAH alcançou 74% de efetividade e 95% de cobertura. Além disso, o 3SW apresentou maior completude por controle (59% dos controles com implementação total, contra 38% do WAH), demonstrando seu alinhamento técnico aos servidores web e a realidade operacional do órgão público que participou do estudo de caso.

O 3SW representa uma proposta aplicável, com potencial de impacto direto na segurança cibernética da Administração Pública, atuando de forma sinérgica ao já existente PPSI. Além disso, por sua abordagem metodológica rigorosa, resultados práticos e relevância institucional, espera-se que esta pesquisa contribua para o debate acadêmico e técnico em torno da aplicação contextualizada de *frameworks* de segurança e da proteção de ativos estratégicos em ambientes públicos.



**Palavras-chave: Segurança da Informação, CIS Controls, Servidores Web, Medidas de Segurança, 3SW, Mitigações Cibernéticas, Administração Pública, Caso de Estudo**

## ABSTRACT

The increasing dependence on technology and the expansion of digital services, combined with a significant rise in cyber threats, require that Public Administration improve its information security maturity, particularly concerning critical assets such as web servers. Therefore, it is essential to reduce immediate risks and strengthen cybersecurity through practical, applicable, and prioritized actions.

This thesis introduces the 3SW model (Subset of Safeguards for Web Servers), a specific set of security measures derived from the CIS Controls v8.1, designed to protect web servers in institutional environments.

The research methodology for developing the 3SW was based on an adaptation of the content analysis proposed by Bardin, structured in three phases: Pre-analysis, Application of Criteria, and Analysis of Results. Using qualitative criteria, 93 security measures were selected, distributed across 17 of the 18 controls in CIS Controls v8.1, with a focus on web servers. The model was then validated through a case study. First, we conducted a diagnosis in the organization where the model would be implemented using document analysis and interviews. The 3SW model was subsequently applied to the Alpaca System, while the reference model WAH (Web Application Hacking from the Community Defense Model) was used in the Llama System. Finally, the results were compared to determine the effectiveness of the 3SW model.

The diagnosis revealed that although the CIS Controls were already implemented within the organization through the Privacy and Information Security Program (PPSI), their general application did not fully address the specific needs of web servers. Some observed limitations included lack of focus on web servers and low granularity in the evaluation scales.

The comparison of the application results of the models in the two systems indicated that the 3SW model achieved 82% effectiveness (76 of 93 measures implemented) and 97% coverage of active mitigations (based on MITRE ATT&CK). In contrast, the WAH model achieved 74% effectiveness and 95% coverage. Moreover, the 3SW demonstrated greater completeness per control, with 59% of controls fully implemented compared to 38% for the WAH model. This indicates that the 3SW model is better aligned with the technical needs of web servers and with the operational context of the public agency that participated in the case study.

The 3SW represents a practical proposal that could significantly improve the cybersecurity of Public Administration, working synergistically with the existing PPSI. Additionally, due to its rigorous methodological approach, practical results, and institutional relevance, this research can contribute to the academic and technical discussions on the contextualized application of security frameworks and the protection of strategic assets in public environments.



**Keywords: Information Security, CIS Controls, Web Servers, Safeguards, 3SW, Cybersecurity Countermeasures, Public Sector, Case Study**

# SUMÁRIO

# LISTA DE FIGURAS

# LISTA DE TABELAS

# LISTA DE SÍMBOLOS E ABREVIAÇÕES

| | |
|---|---|
| 3SW | Subconjunto de Salvaguardas para Servidores Web |
| AMT | Adota em Maior Parte ou Totalmente |
| ANPD | Autoridade Nacional de Proteção de Dados |
| APF | Administração Pública Federal |
| Audin | Auditoria Interna |
| CDM | Community Defense Model |
| Cetic.br | Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação |
| CGU | Controladoria-Geral da União |
| CIS | Center for Internet Security |
| Ciset | Secretaria de Controle Interno |
| COSO ERM | *Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management* |
| CP | Critérios Priorização |
| CPF | Cadastro de Pessoa Física |
| CS | Critérios de Seleção |
| DDoS | *Distributed Denial of Service* |
| DIRB | *Verizon Data Breach Investigations Report* |
| FMX | Fort Meade eXpérience |
| GSI/PR | Gabinete de Segurança Institucional da Presidência da República |
| ICS | *Industrial Control System* |
| IoT | *Internet of Things* |
| ISO | *International Organization for Standardization* |
| LGPD | Lei Geral de Proteção de Dados Pessoais |
| MCDA | *Multi Criteria Decision Analysis* |
| MGI | Ministério da Gestão e Inovação |

| | |
|---|---|
| MP | Ministério do Planejamento, Desenvolvimento e Gestão |
| NIST | *National Institute of Standards and Technology* |
| OA | Objetivo de Apoio |
| OCDE | Organização para a Cooperação e Desenvolvimento Econômico |
| OE | Objetivo Específico |
| OWASP | Open Worldwide Application Security Project |
| PNCiber | Política Nacional de Cibersegurança |
| PNSI | Política Nacional de Segurança da Informação |
| PPSI | Programa de Privacidade e Segurança da Informação |
| PTD | Plano de Transformação Digital |
| QP | Questão de Pesquisa |
| RGPD | Regulamento Geral sobre a Proteção de Dados |
| SEI | Sistema Eletrônico de Informações |
| SGD/MGI | Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos |
| SI | Segurança da Informação |
| SISP | Sistema de Administração dos Recursos de Tecnologia da Informação |
| TCU | Tribunal de Contas da União |
| TIC | Tecnologia da Informação e Comunicação |
| TRV | Taxa de Redução de Vulnerabilidades |
| WAH | *Web Application Hacking* |

# 1 INTRODUÇÃO

A sociedade brasileira tem vivenciado rápidas transformações digitais, muitas delas disruptivas, que alteram profundamente a forma como os indivíduos relacionam-se, consomem e acessam serviços. Um exemplo emblemático é o Pix, o sistema brasileiro de pagamentos instantâneos, que, em apenas quatro anos desde o lançamento em 2020, já alcançou 155,5 milhões de pessoas físicas cadastradas, numa população estimada de 212 milhões em 2024 [7, 8].

O fenômeno Pix ilustra uma nova era da sociedade brasileira, a era da adoção em larga escala de tecnologias digitais. Tecnologias que dependem diretamente do acesso e da qualidade da conexão à Internet disponíveis aos usuários. Segundo dados do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), 84% dos domicílios brasileiros possuíam acesso à Internet em 2023, um avanço de 65% em relação à última década [9]. Esse aumento no acesso à Internet tem permitido que a maioria da população participe de uma economia digital de serviços e produtos, eliminando barreiras transfronteiriças.

Apesar do avanço tecnológico e do crescente acesso à internet, um outro setor da sociedade, o setor público, ainda apresenta barreiras ao avanço digital, como a restrição de serviços ao público no formato presencial, o que evidencia um descompasso em relação ao progresso digital da sociedade [10, 11]. Essa burocracia "analógica" gera custos significativos ao cidadão, estimados em mais de 4,7 bilhões de reais por ano [11, 12].

Diante desse cenário, para acompanhar a nova realidade brasileira, em 2019, o governo federal criou o portal único "gov.br" com a missão de unificar os canais de serviços públicos federais. Essa iniciativa buscou facilitar o acesso aos serviços públicos, reduzir a burocracia, bem como prestar um serviço com qualidade a toda a população brasileira [13]. Para alcançar níveis adequados de maturidade digital, os órgãos federais necessitam propor um Plano de Transformação Digital (PTD) que contemple, entre outros aspectos, ações de segurança da informação durante a digitalização de seus serviços [14]. Essas medidas de fomento com o PTD registram, em janeiro de 2025, 90% dos serviços públicos transformados em digitais [10].

As ações de modernização digital no serviço público têm permitido ao Brasil melhorar sua posição em *rankings* internacionais. Levantamento de 2023 da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) apresentou o país na $15^a$ posição entre 38 países pesquisados [15], enquanto, no *ranking* do Banco Mundial de 2022, passou da $7^a$ posição em 2021 para a $2^a$ posição entre 198 economias avaliadas [16, 17]. Apesar de ainda apresentar serviços presenciais, as ações para transformação digital têm mostrado resultados e posicionado bem o país na oferta de serviços frente a economias mais fortes.

Os dados de serviços transformados e a comparação internacional exibem uma realidade de aproximação do setor público com a era digital vivida pela sociedade, entretanto, novos desafios relacionados a risco com a segurança da informação e a privacidade dos dados pessoais adicionam-se a esse momento [18], visto que assegurar a disponibilidade contínua de serviços essenciais e proteger os dados contra violações tornam-se o novo calcanhar de Aquiles, devido ao aumento na exposição desses serviços com a

transformação digital.

Ataques cibernéticos que causam a indisponibilidade do serviço ou o vazamento de dados podem comprometer a vida de milhares ou milhões de cidadãos que dependem desses serviços [19, 20]. No caso da instituição analisada nesta dissertação, nomeada de Empresa ALFA, além de comprometer a imagem, as consequências podem impactar a atividade econômica, pois, em muitas situações, são tratados processos com informações sigilosas, o que eleva as consequências de vazamentos de dados.

Nesse contexto cibernético, o Tribunal de Contas da União (TCU), em seu papel constitucional de fiscalização [21], tem observado com atenção o processo de transformação digital, principalmente, devido à disparada nos números de incidentes relacionados a ataques cibernéticos, como os casos de *ransomware* ("sequestro" de dados), que de 2020 a 2021, aumentaram em 90% [22]. Em adição, levantamento da Verizon, de 2023, informa que no setor público, houve um aumento das ameaças oriundas de agentes externos, quando comparado a 2022, de 78% para 85% [23, 24], o que alerta para os riscos da transformação digital, devido à alta exposição de serviços digitais na Internet.

Reconhecendo esse cenário alarmante e a necessidade de garantir serviços resilientes e seguros, o governo federal do Brasil conta com dois órgãos estratégicos para tratar a segurança da informação na Administração Pública Federal (APF): o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e a Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI) [25]. Em questão de ações provocadas, várias têm sido conduzidas por esses órgãos para enfrentar os crescentes desafios cibernéticos, entre as quais encontra-se o Programa de Privacidade e Segurança da Informação (PPSI), lançado pela SGD/MGI, em 2023 [3], fundamentado em práticas reconhecidas internacionalmente [26], como as normas da International Organization for Standardization (ISO) [27], do National Institute of Standards and Technology (NIST) [28] e do *framework* CIS Controls [2], que se destaca por priorizar ações críticas de proteção organizacional [29].

Apesar dessa iniciativa, dados do PPSI divulgados pelo TCU, em 2024, indicam que quase 70% dos órgãos públicos permanecem em níveis iniciais de maturidade quanto à implementação das medidas previstas no programa. Esse cenário é agravado pela escassez de recursos humanos e pela falta de profissionais qualificados [30], dificultando a consolidação de uma estrutura robusta de segurança digital na administração pública.

Diante desses desafios, este trabalho propõe uma metodologia de referência que, ao aproveitar a estrutura do CIS Controls e PPSI, tem o objetivo de ajudar as organizações públicas a elevar o nível de maturidade em segurança cibernética, com foco em sistemas que possam comprometer a missão crítica da instituição.

## 1.1 MOTIVAÇÃO E JUSTIFICATIVA

A transformação digital em ritmo acelerado e em um ambiente de baixa cultura organizacional de Segurança da Informação (SI) [31] eleva a probabilidade de exposição a falhas de processos ou de sistemas para públicos que anteriormente não teriam esses acessos disponíveis. Esse cenário pode explicar o aumento de 93% no número de ataques cibernéticos às instituições governamentais entre 2023 e 2024 [32, 33] e

corrobora a necessidade de uma abordagem mais estruturada e eficiente para a segurança cibernética no setor público.

No entanto, é importante contextualizar que a administração pública no Brasil opera sob o princípio constitucional da legalidade, que determina que todo ato administrativo deve estar amparado por uma norma jurídica prévia [34]. Dessa forma, no que tange à questão legislativa sobre segurança da informação, o aparato legal é vasto, composto por leis, decretos, portarias, instruções normativas, muitos dos quais estão condensados no sítio eletrônico do GSI/PR [6]. Além disso, o GSI/PR tem publicado uma série de normativos de caráter infralegal [1], que, nos termos do acórdão 1233/2012 do TCU, item 9.8.2 [36], não faculta à alta administração implantar os controles gerais de Segurança da Informação (SI) constantes nessas normas, e sim obriga-a, exceto se devidamente justificado [36].

Além do arcabouço legal, guias e orientações também são fornecidos pelas entidades do TCU, do GSI/PR e da SGD/MGI [37, 38, 39]. Esses documentos reforçam o apoio à Segurança da Informação no âmbito do governo federal, fornecendo diretrizes e boas práticas para a implementação de controles de segurança. O PPSI é um exemplo notório dessas orientações, pois utiliza como ações de segurança todas as medidas presentes no *framework* CIS Controls v8 [2, 3].

Entretanto, apesar da existência desses marcos regulatórios, persistem lacunas significativas que representam riscos críticos à segurança dos serviços públicos. Como destacado pelo TCU, a maioria das instituições públicas apresenta baixa maturidade em segurança da informação, além de enfrentar escassez de recursos financeiros e humanos [30, 31]. Essas instituições necessitam de ações focadas no que devem proteger, ao mesmo tempo em que promovem a evolução da maturidade em segurança da informação ao longo do tempo.

Portanto, uma proposta que busque mitigar riscos imediatos torna-se não apenas viável, mas essencial. Este trabalho justifica-se pela necessidade de preencher essas lacunas, oferecendo uma metodologia de referência que favoreça a priorização de ações para a proteção de sistemas essenciais e dados pessoais.

## 1.2 PROBLEMA DE PESQUISA

A transformação digital no setor público brasileiro, embora necessária e benéfica, trouxe consigo desafios significativos no que diz respeito à segurança cibernética. Como discutido anteriormente, a rápida adoção de tecnologias digitais e a disponibilização de serviços na Internet expõem as organizações públicas a riscos cada vez maiores, como ataques cibernéticos e violações de dados. Esses riscos são agravados pela baixa maturidade em segurança da informação e pela escassez de recursos humanos e financeiros, como destacado pelo TCU [30, 31], exigindo uma alocação eficiente desses recursos de modo a atender às prioridades institucionais e assegurar que as ações de segurança concentrem-se nos vetores de ataque mais críticos.

Ademais, apesar da existência de um arcabouço jurídico robusto e de diretrizes para a implementação

[1] Normativos infralegais são instrumentos complementares às leis e aos decretos, como portarias, resoluções e instruções normativas, que possuem caráter vinculativo e regulamentam a aplicação de dispositivos legais, detalhando procedimentos e orientações específicas. Eles são editados diretamente pelas autoridades públicas, podendo ser considerados como atos administrativos [35]

de controles de segurança com o PPSI, a efetividade dessas normas tem sido limitada. Dados do TCU mostram que mais de 70% dos órgãos públicos federais não estão em conformidade com os requisitos mínimos de segurança cibernética [40]. Essa não conformidade expõe as organizações a vulnerabilidades críticas, especialmente em um contexto de aumento acelerado de ameaças cibernéticas.

Diante desse cenário, o problema central desta pesquisa é: como desenvolver uma metodologia de referência que, aproveitando a estrutura existente do CIS Controls v8 e do PPSI, permita às organizações públicas elevar seu nível de maturidade em segurança cibernética, com foco na proteção de servidores web e sistemas críticos, mitigando os riscos de ataques cibernéticos de forma eficiente e direcionada.

Com base nesse problema, propõe-se a seguinte hipótese para guiar a pesquisa:

**Hipótese:** A implementação de uma adaptação do CIS Controls v8.1 para servidores web —— denominada, a partir deste ponto, Modelo 3SW —— focada em sistemas expostos à internet, pode reduzir significativamente a probabilidade de êxito de ataques cibernéticos.

## 1.3 OBJETIVOS

O objetivo geral deste trabalho é **propor uma adaptação do CIS Controls v8.1 para servidores web**, com o intuito de reduzir a probabilidade de êxito de ataques cibernéticos em sistemas expostos à internet. Para atingir esse objetivo, adota-se a técnica de estudo de caso, permitindo uma análise aprofundada da aplicação das medidas de segurança propostas. Para tanto, é necessário alcançar os seguintes Objetivos Específicos (OE):

OE1 Adaptar o CIS Controls v8.1 para o contexto de servidores web;

OE2 Identificar e classificar os sistemas críticos; e

OE3 Verificar a efetividade da solução proposta.

## 1.4 MÉTODO DE PESQUISA

A metodologia desta dissertação foi estruturada em quatro fases principais. As duas primeiras — Planejamento da Pesquisa e Fundamentação Teórica — ofereceram suporte conceitual e metodológico à construção do modelo. As fases centrais consistiram no Desenvolvimento e Validação do Modelo 3SW (Subconjunto de Salvaguardas para Servidores Web), voltado à adaptação do *framework* CIS Controls v8.1 [2] ao contexto de servidores web.

Na fase de desenvolvimento, utilizou-se uma abordagem exploratória de natureza qualitativa. O método de pesquisa consistiu na análise documental de *frameworks* de segurança reconhecidos internacionalmente [26], utilizando a técnica de análise de conteúdo de Bardin [41] para examinar criticamente a documentação do CIS Controls v8.1, MITRE ATT&CK e CDM v2.0. Foram definidos critérios de seleção e priorização

para identificar um subconjunto de medidas de segurança aplicáveis diretamente a servidores web. A partir desses critérios, estruturou-se o Modelo 3SW, composto por controles selecionados de acordo com sua aplicabilidade, esforço de implementação e de manutenção.

A fase de validação do 3SW foi conduzida por meio de um estudo de caso aplicado em uma organização pública federal, denominada Empresa ALFA. Essa etapa envolveu entrevistas com profissionais da área tecnologia da informação (incluindo a segurança da informação), análise documental e o uso de ferramentas técnicas para coleta e verificação de vulnerabilidades nos sistemas participantes do estudo de caso. A análise dos dados combinou técnicas quantitativas — como a Taxa de Redução de Vulnerabilidades — e qualitativas, com base na percepção dos profissionais entrevistados, resultando numa triangulação de dados.

Essa abordagem metodológica permitiu avaliar, de forma empírica e estruturada, a aplicabilidade e a efetividade do modelo proposto no fortalecimento da segurança de servidores web em ambientes institucionais reais.

## 1.5 PUBLICAÇÃO RESULTANTE DESSE TRABALHO

- Silva, Tássio; Mendes, Fabiana. 3SW: Um Conjunto de Medidas de Segurança para Mitigar Vulnerabilidades em Servidores Web. Revista Ibérica de Sistemas e Tecnologias de Informação - RISTI, 2024 [42]. (Qualis A4)

## 1.6 ESTRUTURA DA DISSERTAÇÃO

Esta dissertação está organizada em sete capítulos, sendo este o primeiro deles. No Capítulo 2 estão presentes os principais conceitos e definições relacionados ao tema deste trabalho, abordando transformação digital, legislações voltadas à segurança da informação no âmbito da administração pública federal do Brasil, riscos cibernéticos e *frameworks* de segurança.

O Capítulo 3 apresenta o método adotado para o desenvolvimento desta pesquisa. Por sua vez, o Capítulo 4 descreve como o Modelo 3SW —– principal resultado desta dissertação —– foi criado, seguido dos procedimentos adotados para a validação do modelo (Capítulo 5) e da análise dos resultados obtidos (Capítulo 6). Por fim, o Capítulo 7 apresenta as conclusões, as contribuições e os trabalhos futuros relacionados a este estudo.

# 2 REFERENCIAL TEÓRICO E TRABALHOS RELACIONADOS

Neste capítulo são discutidos tópicos importantes relacionados a esta dissertação, em que destacam-se o arcabouço jurídico e as iniciativas do governo federal do Brasil para combater ameaças cibernéticas, bem como os trabalhos relacionados àquele desenvolvido nesta dissertação.

## 2.1 TRANSFORMAÇÃO DIGITAL NO SETOR PÚBLICO BRASILEIRO

A transformação digital é uma expressão que ganhou força a partir da pandemia de COVID-19, quando restrições à aglomeração em diversos países exigiram que o atendimento ao público se adaptasse a novas demandas, marcadas por urgência e inovação [43]. Antes da pandemia, a transformação digital tinha como principal objetivo desenvolver a organização de forma estratégica [43, 44].

Para Albertin & Albertin [45], a transformação digital pode ser compreendida como a utilização de inovações digitais para criar algo novo, distinto e aprimorado, trazendo benefícios tanto para a sociedade quanto para as empresas. Já Mergel et al. [46], numa visão específica do setor público, a definem como um processo contínuo que vai além da simples digitalização, envolvendo a reestruturação de políticas, processos e serviços governamentais para atender melhor às necessidades dos cidadãos, com foco em novas formas de entrega e ampliação do acesso.

No Brasil, a trajetória histórica da transformação digital na administração pública passou por diversas fases, estendendo-se desde os primeiros programas de computador utilizados pelo governo na década de 1950 [47] até os dias atuais, em que há uma expansão no uso de ferramentas de tecnologia da informação na prestação de serviços públicos, tornando-as elemento central na modernização do setor público [48].

Atualmente, a regulamentação que trata do tema de transformação digital na administração pública federal é o Decreto nº 12.198/2024, que estabelece a estratégia de Governo Digital para o período de 2024 a 2027 [14]. O Decreto aponta para objetivos e iniciativas que visam formalizar a transformação digital como uma prioridade estratégica, ampliar a prestação de serviços digitais e estimular a participação social na gestão pública [49, 50].

Apesar dos avanços normativos e institucionais, ainda persistem desafios significativos para a plena realização da transformação digital no setor público brasileiro [51]. Entre eles, destacam-se os desafios voltados para a segurança e a privacidade dos dados pessoais [52].

A pandemia da COVID-19 acelerou processos de digitalização em todo o mundo, e no Brasil não foi diferente [1]. A emergência sanitária evidenciou a importância de serviços públicos digitais acessíveis e eficientes, ao mesmo tempo em que expôs as fragilidades das infraestruturas tecnológicas e das competências

[1] Em janeiro de 2025, 90% dos serviços públicos constavam como transformados em digitais [10], o que representa um aumento de 157% desde abril de 2020 [53].

digitais existentes no setor público [54, 55].

Diante disso, neste estudo, a transformação digital é considerada um contexto crítico para a análise da segurança da informação em servidores web na Administração Pública, uma vez que a ampliação dos serviços digitais também amplia as superfícies de ataque e as vulnerabilidades que precisam ser geridas de forma eficaz.

Na seção a seguir, contextualiza-se o arcabouço jurídico sobre segurança da informação para a administração pública federal. Essa contextualização é importante por dois motivos principais: como mencionado por Tácito [34], todo ato administrativo deve estar amparado por uma norma jurídica prévia; e a evidência de que há um aparato legal vasto sobre o tema segurança da informação.

## 2.2 ARCABOUÇO JURÍDICO SOBRE SEGURANÇA DA INFORMAÇÃO NO GOVERNO FEDERAL BRASILEIRO

O tema da segurança da informação no setor público federal do Brasil é disciplinado por dois órgãos: o GSI/PR, regulamentado pelo Decreto nº 11.776/2023 [56], e a SGD/MGI, regida pelo Decreto nº 12.102/2024 [57]. Esses órgãos, além de proverem aparato normativo, desempenham papéis educativos importantes tanto na oferta de conteúdo técnico quanto na promoção da conscientização. Sob sua governança estão mais de 300 entidades federais [58] e um contingente de mais de 1,1 milhão de servidores ativos [59], que, no dia a dia, por meio do corpo técnico de TI, buscam seguir suas diretrizes e suas proposições. Além disso, quando não são diretamente os precursores dos normativos de segurança da informação, esses órgãos atuam como partícipes em sua elaboração.

Em relação ao arcabouço jurídico brasileiro em segurança da informação, ele é extenso e abrange desde políticas nacionais até normas específicas para contratações de TI, proteção de dados e gestão de incidentes. Para uma visão sistêmica desses instrumentos, o Apêndice C apresenta uma compilação das 56 principais legislações que regulam a matéria na administração pública federal, organizadas por classificação normativa (leis, decretos, portarias). Essa base legal reflete tanto a evolução histórica do tema quanto a complexidade de sua implementação prática.

Desses normativos, dois ganham destaque no âmbito da administração pública federal:

- A Política Nacional de Segurança da Informação (PNSI), instituída pelo Decreto nº 9.637/2018, que estabelece princípios e diretrizes para assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações governamentais [60, 61]; e
- A Política Nacional de Cibersegurança (PNCiber), instituída pelo Decreto nº 11.856/2023, com a finalidade de orientar a atividade de segurança cibernética no País [62].

Essas políticas, além de serem importantes marcos legais para os órgãos públicos federais [63], são operacionalizadas por meio da Estratégia Nacional de Segurança da Informação [64, 65] e do Programa de Privacidade e Segurança da Informação (PPSI) [66, 67], que visam fortalecer a proteção dos ativos digitais e a governança de riscos em órgãos públicos [68, 69].

Apesar do arcabouço normativo consolidado, o cenário atual revela desafios significativos [70]. Como mencionado no Capítulo 1, nas recentes auditorias do Tribunal de Contas da União (TCU), foi identificada baixa maturidade em segurança cibernética nas organizações do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), com a ausência da implementação integral dos controles básicos para sair dos níveis iniciais de maturidade em segurança da informação [30]. Entre os fatores críticos estão a insuficiência de recursos financeiros e humanos, a falta de priorização do tema pela alta administração e a ausência de uma estrutura de coordenação com autoridade responsável pela execução da política nacional de cibersegurança.

O TCU recomenda a priorização da segurança cibernética pelo Estado brasileiro, com especial atenção para o fortalecimento do GSI/PR e da Secretaria de Governo Digital na condução das políticas e na orientação das organizações do SISP (ao todo 250 entidades federais [71]). A liderança da alta administração é apontada como fator determinante para o sucesso da gestão de riscos cibernéticos, reforçando a necessidade de que os gestores assumam responsabilidade explícita pela segurança da informação em suas instituições [30].

Além disso, a governança de tecnologia da informação no setor público federal deve ser aprimorada com a implantação de políticas claras, planos estratégicos de TIC e mecanismos transparentes de monitoramento e controle, alinhados às melhores práticas internacionais [72]. A capacitação contínua, a conscientização dos servidores e a modernização da infraestrutura tecnológica são pilares essenciais para elevar o nível de maturidade em segurança cibernética e garantir a continuidade dos serviços públicos digitais [73].

O fortalecimento da segurança da informação no setor público federal brasileiro é fundamental para proteger dados sensíveis, assegurar a confiança dos cidadãos nos serviços digitais e garantir a soberania digital do país, especialmente no contexto da crescente transformação digital da administração pública [51].

As subseções a seguir detalham as duas principais iniciativas do governo federal nesse contexto de proteção de dados e informações: a Lei Geral de Proteção de Dados Pessoais (2.2.1) e o Programa de Privacidade e Segurança da Informação (2.2.2).

### 2.2.1 Lei Geral de Proteção de Dados Pessoais

A Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD) [18], estabelece normas sobre o tratamento de dados pessoais no Brasil, tanto no setor público quanto no privado. Trata-se de uma legislação de caráter geral, aplicável a qualquer operação de tratamento de dados pessoais realizada no território nacional.

Embora a proteção de dados também seja mencionada em outras normativas brasileiras, como a Política Nacional de Segurança da Informação (PNSI) e a Política Nacional de Cibersegurança (PNCiber), essas possuem escopo mais restrito por serem formalizadas por decretos. A PNSI, por exemplo, prevê a proteção de dados pessoais no art. 4º, inciso VI, alínea "c" [2]. Da mesma forma, a PNCiber trata do tema no art. 2º,

[2]Decreto nº 9.637, Art. 4º, VI, c: proteção das informações das pessoas físicas que possam ter sua segurança ou a segurança de suas atividades afetada, observada a legislação específica.

inciso II [3].

No entanto, por sua natureza de lei ordinária, a LGPD possui hierarquia normativa superior e maior abrangência em relação aos decretos, estabelecendo princípios, direitos e obrigações específicas para o tratamento de dados pessoais no Brasil [35].

No âmbito da proteção de dados pessoais, a LGPD define tratamento como **toda operação realizada com dados pessoais, incluindo coleta, utilização, armazenamento, eliminação e outras ações correlatas** [4]. Essa legislação representa um marco fundamental na regulação do uso de dados pessoais no país [74]. Seu surgimento foi impulsionado, em parte, pela necessidade de alinhamento internacional, especialmente com o Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia [75], cuja vigência, em 2018, exigiu padrões equivalentes de proteção de dados para países e organizações que mantêm relações comerciais com o bloco europeu [76].

A proteção dos dados pessoais é o núcleo da LGPD —– o termo "proteção" aparece mais de 60 vezes ao longo do texto legal —– e orienta a adoção de medidas de segurança robustas. O Capítulo VII da lei (arts. 46 a 51) trata especificamente da segurança e das boas práticas, estabelecendo a necessidade de salvaguardas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Em caso de incidente de segurança envolvendo dados pessoais, a comunicação à Autoridade Nacional de Proteção de Dados (ANPD) é obrigatória e deve ser realizada pelo controlador dos dados, conforme previsto na legislação (Art. 48 [5]). Esse requisito visa garantir a transparência e a pronta resposta a eventos que possam comprometer os direitos dos titulares de dados.

Além de atender a demandas internacionais, a LGPD introduziu um novo paradigma para a governança de dados pessoais no setor público brasileiro. Sua implementação exige a articulação entre áreas jurídicas, de tecnologia da informação e de segurança da informação, configurando um desafio ainda em andamento, o que fica evidente nas auditorias recentes do TCU [30].

Para viabilizar a implementação da LGPD no âmbito da administração pública federal, tornou-se necessário o desenvolvimento de instrumentos que orientassem tecnicamente os órgãos e as entidades quanto à adoção de práticas de privacidade e de segurança da informação. Nesse contexto, a Secretaria de Governo Digital (SGD/MGI) recebeu esse papel central na formulação de diretrizes e mecanismos de apoio institucional [77, 57].

### 2.2.2 Programa de Privacidade e Segurança da Informação (PPSI)

Diante da promulgação da LGPD, a SGD/MGI necessitava prover orientações aos órgãos sobre como atuar perante os novos desafios [57]. Os primeiros guias orientativos para a LGPD e a segurança da

[3] Decreto nº 11.856, Art. 2º, II: a garantia dos direitos fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação.

[4] Lei nº 13.709, Art. 5º, inciso X — tratamento: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[5] Lei 13.709, art 48: O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

informação foram publicados entre 2020 e 2021, sendo eles o Guia de Boas Práticas para Implementação na Administração Pública Federal [78], o Guia do Framework de Segurança e o Guia de Avaliação de Riscos de Segurança e Privacidade [79, 80, 81]. No entanto, por se tratarem de documentos com fraca força normativa [34, 35, 82], identificou-se a necessidade de fortalecimento institucional dessas diretrizes. Como resposta, os dois guias de segurança foram unificados em 2022, resultando no Guia do Framework de Privacidade e Segurança da Informação. Em 2023, com a publicação da Portaria SGD/MGI nº 852, esse guia passou a ser institucionalizado como parte integrante do PPSI [6] [7].

A partir da vigência da portaria, cada órgão ou entidade da administração pública federal passou a ser responsável por instituir uma estrutura de governança voltada ao PPSI, composta pelos seguintes papéis e responsabilidades [66]:

- **Gestor de Tecnologia da Informação e Comunicação**: responsável por planejar, implementar e aprimorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações[8];
- **Gestor de Segurança da Informação**: responsável por planejar, implementar e aprimorar continuamente os controles de segurança da informação em ativos de informação[9];
- **Encarregado pelo Tratamento de Dados Pessoais**: responsável por conduzir diagnósticos de privacidade e orientar, quando necessário, os gestores proprietários dos ativos de informação quanto ao planejamento, implementação e aprimoramento dos controles de privacidade aplicáveis a dados pessoais ou sensíveis[10]; e
- **Responsável pela Unidade de Controle Interno**: responsável por apoiar, supervisionar e monitorar as atividades da primeira linha de defesa[11].

Encerrada a definição de papéis e responsabilidades, é importante compreender a composição do Guia do Framework de Privacidade e Segurança da Informação, uma vez que ele orienta a implementação prática das diretrizes estabelecidas pela Portaria. Esse guia é formado por 31 controles, organizados em três categorias principais [3]:

- **Estruturação básica da gestão em privacidade e segurança da informação** — Com medidas verificáveis no Controle 0. Este controle contempla aspectos normativos e institucionais, como a nomeação do encarregado de dados, do gestor de segurança e a existência de uma Política de Segurança da Informação;
- **Segurança cibernética** — Com medidas verificáveis nos Controles 1 a 18. Esses controles, em conjunto com suas medidas, correspondem integralmente aos controles e as medidas presentes no *framework* CIS Controls v8 [2]; e

[6] Portaria SGD/MGI nº 852 - Art. 7º. Institui-se o Framework de Privacidade e Segurança da Informação, composto por um conjunto de controles, metodologias e ferramentas de apoio [66].

[7] Portaria SGD/MGI nº 852 - Art. 3º O PPSI tem como objetivo elevar a maturidade e a resiliência dos órgãos e entidades, em termos de privacidade e segurança da informação, no âmbito do SISP [66].

[8] Portaria SGD/MGI nº 852 - Art. 6º, Inciso I.

[9] Portaria SGD/MGI nº 852 - Art. 6º, Inciso II.

[10] Portaria SGD/MGI nº 852 - Art. 6º, Inciso III.

[11] Portaria SGD/MGI nº 852 - Art. 6º, Inciso IV.

- **Privacidade** — Com medidas verificáveis nos Controles 19 a 31. Essas medidas foram definidas com base em normas internacionais, como ISO/IEC 29100:2011, ISO/IEC 29151:2017, ABNT NBR ISO/IEC 27701:2019, ISO/IEC 27018:2014, ISO/IEC 29134:2017 e ABNT NBR ISO/IEC 29184:2021.

Como as medidas previstas no guia abrangem toda a instituição, adotou-se um método de avaliação baseado em níveis de implementação [3], conforme demonstrado na Tabela 2.1:

Tabela 2.1: Níveis de implementação e pontuação para avaliação das medidas de privacidade e de segurança no PPSI. Fonte: Guia do Framework de Privacidade e Segurança da Informação [3]

| **Nível de Implementação** | **Descrição** | **Pontuação** |
|---|---|---|
| Adota em maior parte ou totalmente | Há decisão formal ou plano aprovado, e a medida está implementada integralmente em mais de 50% ou em todos os:<br>• ativos (no caso de medidas de segurança da informação); ou<br>• processos/serviços (no caso de medidas de privacidade). | 1 |
| Adota em menor parte | Há decisão formal ou plano aprovado, e a medida está implementada integralmente em menos de 50% dos:<br>• ativos (segurança da informação); ou<br>• processos/serviços (privacidade). | 0,75 |
| Adota parcialmente | Há decisão formal ou plano aprovado, e a medida está implementada parcialmente em mais de 50% ou em todos os:<br>• ativos (segurança da informação); ou<br>• processos/serviços (privacidade). | 0,5 |
| Há decisão formal ou plano aprovado para implementar | Há decisão formal ou plano aprovado, mas a medida ainda não foi implementada ou está parcialmente implementada em menos de 50% dos:<br>• ativos (segurança da informação); ou<br>• processos/serviços (privacidade). | 0,25 |
| A organização não adota essa medida | Não há decisão formal, plano aprovado ou qualquer forma de implementação. | 0 |
| Não se aplica | A medida não se aplica a nenhum ativo (segurança da informação) ou processo/serviço (privacidade), de acordo com avaliação fundamentada dos gestores e com base em análise de risco. | N/A |

A avaliação das medidas sob o prisma institucional dispersa o foco da atuação dos órgãos, uma vez que apenas no tema de segurança existem 18 controles (totalizando 153 medidas) a serem analisados. Ainda que essas medidas estejam organizadas segundo os Grupos de Implementação do CIS Controls v8 — que as distribuem de acordo com sua complexidade [2] —, há o risco de não contemplar adequadamente as particularidades de exposição a riscos específicos de cada instituição, especialmente no contexto da transformação digital [51].

Considerando que o PPSI adota integralmente os controles do CIS Controls v8, a adaptação desse *framework* para servidores web neste trabalho aproveita as experiências acumuladas ao longo dos últimos

quatro anos, desde a publicação do primeiro Guia do Framework de Segurança [79].

## 2.3 GESTÃO DE RISCOS NO SETOR PÚBLICO BRASILEIRO

A gestão de riscos tem se tornado uma referência essencial para a boa governança corporativa, tanto no setor privado quanto no público [83]. No cenário brasileiro, a administração pública federal passou a adotar sistematicamente práticas de gestão de riscos a partir da Instrução Normativa Conjunta CGU/MP nº 1, de 10 de maio de 2016, que estabeleceu a obrigatoriedade da sistematização de práticas relacionadas à gestão de riscos, controles internos e governança para todos os órgãos e entidades do Poder Executivo federal [84].

Em 2017, o Ministério do Planejamento, Desenvolvimento e Gestão (MP) publicou o *Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão*, que se tornou um marco para a implementação dessas práticas na administração pública federal [85]. O manual define gestão de riscos como "um processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza no alcance dos objetivos da organização" [86]. Essa definição alinha-se com a norma ABNT NBR ISO 31000, que conceitua risco como "o efeito da incerteza nos objetivos", ressaltando que esse efeito pode ser positivo, negativo ou ambos, podendo criar oportunidades ou ameaças [87].

A abordagem adotada pelo MP no seu manual baseia-se no *framework* COSO ERM (*Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management*), que compreende o risco como um processo conduzido pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias para identificar eventos potenciais capazes de afetar a organização e administrar os riscos de modo compatível com seu apetite ao risco [86].

O manual ainda traz orientações acerca do modelo de **Três Linhas de Defesa** [88], que consiste na organização da instituição para alcançar a efetividade de programas de *compliance* público [89]. A seguir, descreve-se como as áreas responsáveis pela gestão operacional, gerenciamento de riscos e conformidade e auditoria interna encaixam-se nesse modelo:

- **1ª Linha de Defesa**: *gestão operacional*, é responsável pela implementação direta de controles [86];
- **2ª Linha de Defesa**: *gerenciamento de riscos e conformidade*, é responsável por monitorar e apoiar a implementação dos controles da primeira linha [86]; e
- **3ª Linha de Defesa**: *auditoria interna*, é responsável por avaliar de forma independente a eficácia da governança, do gerenciamento de riscos e controle [86].

Essa estrutura foi posteriormente replicada no **Programa de Privacidade e Segurança da Informação (PPSI)** [66, 3], onde :

- A **1ª Linha** engloba os Gestores de TI, os Gestores de Segurança da Informação, os Proprietários de Ativos e os Gestores do negócio ou de políticas públicas envolvidos;

- A **2ª Linha** é representada pelas Unidades de Controle Interno; e
- A **3ª Linha** inclui a Controladoria-Geral da União (CGU), a Auditoria Interna (Audin) e a Secretaria de Controle Interno (Ciset).

No que tange à classificação dos riscos, o modelo proposto classifica os riscos em quatro categorias principais: 1. **Estratégicos**: relacionados às metas gerais alinhadas com a missão organizacional; 2. **Operacionais**: concernentes à utilização eficaz e eficiente dos recursos; 3. **Comunicação**: associados à confiabilidade de relatórios; e 4. **Conformidade**: vinculados ao cumprimento de leis e regulamentos aplicáveis [86].

A metodologia de gestão de riscos proposta pelo MP estrutura-se em cinco etapas principais [86]:

- análise de ambiente e fixação de objetivos;
- identificação de eventos de riscos;
- avaliação de eventos de riscos e controles;
- resposta a risco; e
- informação, comunicação e monitoramento.

Essa abordagem sistemática visa assegurar que os riscos sejam gerenciados de forma integrada aos processos organizacionais, contribuindo para o alcance dos objetivos estratégicos [86].

No entanto, como apontam Silva et al. [83], a implementação da gestão de riscos no setor público brasileiro ainda enfrenta desafios significativos, incluindo a necessidade de maior embasamento teórico-empírico e a adaptação de modelos internacionais à realidade organizacional da administração pública. Apesar desses desafios, a adoção de práticas estruturadas de gestão de riscos representa um avanço importante na modernização da gestão pública, com potencial para aumentar a eficiência, a transparência e a *accountability* na administração federal.

## 2.4 GESTÃO DE RISCOS CIBERNÉTICOS

A crescente digitalização das organizações [90], aliada à sofisticação das ameaças virtuais [91, 92], fez com que os riscos cibernéticos tornassem uma categoria crítica dentro da gestão de riscos contemporânea [93]. Esses riscos referem-se a eventos que comprometem a confidencialidade, a integridade ou a disponibilidade de ativos digitais, com potencial para afetar os objetivos estratégicos, operacionais e de conformidade das organizações [94, 95]. Além disso, eles não se restringem a apenas ataques externos, como *malware*, *phishing*, *ransomware* e negação de serviço (DDoS), mas também vulnerabilidades internas, como o uso de senhas fracas ou configurações inadequadas [96].

Antes de aprofundar a discussão sobre riscos cibernéticos, é importante distinguir os conceitos de segurança da informação e segurança cibernética. De acordo com Von Solms e Van Niekerk [97], a segurança

da informação diz respeito à proteção de ativos informacionais, independentemente de estarem ou não no ciberespaço. Já a segurança cibernética possui um escopo mais amplo, abrangendo tanto ativos informacionais quanto não informacionais (como pessoas e dispositivos físicos conectados) que se encontram dentro do ciberespaço ou que podem ser afetados por ele. Dessa forma, a segurança cibernética lida com ameaças que ultrapassam os limites técnicos da informação e alcançam elementos físicos e humanos.

Dentro desse escopo, os riscos cibernéticos podem ser compreendidos como uma forma específica de risco operacional, diretamente relacionada ao desempenho das atividades no ciberespaço [94]. De acordo com Strupczewski et al. [98], esses riscos ameaçam recursos informacionais, ativos tecnológicos e recursos de TIC, podendo causar danos materiais a bens tangíveis e intangíveis, interrupção de negócios e prejuízos à reputação institucional.

Para lidar com tais riscos, o processo típico de gestão de riscos cibernéticos inclui a identificação de ativos digitais e ameaças potenciais, a avaliação da probabilidade e impacto dos riscos, a implementação de medidas mitigadoras — como *firewalls*, criptografia, autenticação multifator e políticas de segurança — e o monitoramento contínuo da eficácia dessas ações, com capacidade de resposta rápida a incidentes [99].

No contexto do setor público, a gestão de riscos cibernéticos adquire papel ainda mais estratégico, dada a crescente digitalização dos serviços governamentais [30]. O TCU reforça a importância do engajamento da alta administração na liderança desse processo, bem como realça o papel da SGD/MGI, por meio do PPSI, na promoção de medidas que visam reduzir os riscos a níveis aceitáveis e garantir a continuidade dos serviços públicos essenciais [30].

Em síntese, a gestão de riscos cibernéticos constitui um pilar essencial para a segurança da informação em ambientes digitais, sendo determinante para a proteção de dados sensíveis, a conformidade com legislações como a LGPD e o RGPD, a continuidade dos negócios e a confiança dos usuários em serviços digitais.

## 2.5 ATAQUES CIBERNÉTICOS A INSTITUIÇÕES PRIVADAS E PÚBLICAS

O crescimento das ameaças cibernéticas tem imposto desafios significativos tanto ao setor privado quanto ao público, com impactos que extrapolam perdas financeiras, afetando diretamente a continuidade de serviços, a privacidade de milhões de indivíduos e a reputação da organização. Em 2024, o custo médio global de uma violação de dados alcançou US$ 4,88 milhões, um aumento de 10% em relação ao ano anterior, segundo relatório da IBM [100], refletindo o agravamento do cenário de risco cibernético.

Entre os casos mais notórios do setor privado está o da empresa brasileira *JBS S.A.*, uma das maiores processadoras de carne do mundo, que em maio de 2021 sofreu um ataque de *ransomware* [12] que interrompeu suas operações nos Estados Unidos, no Canadá e na Austrália [102]. A empresa optou por pagar o resgate de US$ 11 milhões para recuperar o controle de seus sistemas, ilustrando os altos custos associados à indisponibilidade dos serviços e às medidas de recuperação [103].

Outro exemplo é o da clínica finlandesa *Vastaamo*, especializada em psicoterapia, que sofreu dois

[12] *ransomware* é um ataque caracterizado pelo sequestro de dados e exigência de resgate para liberação [101]

ataques entre 2018 e 2019. Informações sensíveis de aproximadamente 33 mil pacientes foram extraídas e utilizadas para extorsão individual. Diante da negativa da empresa em pagar o resgate, o criminoso divulgou dados terapêuticos de mais de dois mil pacientes. O caso revelou falhas graves de segurança, incluindo ausência de *firewall*, senhas fracas e falta de criptografia nos dados, culminando na declaração de falência da organização em 2021 [104].

No setor público internacional, destaca-se o ataque sofrido pela *Health Service Executive* (HSE) da Irlanda em maio de 2021. O ataque, conduzido com o *ransomware* Conti, levou à paralisação total dos sistemas de TI do serviço público de saúde irlandês, afetando mais de 4 mil unidades de atendimento e 54 hospitais. Apesar da rápida ativação do protocolo de incidente crítico, o processo de recuperação levou mais de quatro meses, demonstrando a vulnerabilidade das infraestruturas críticas de saúde [105].

No contexto brasileiro, o setor público também tem sido alvo recorrente de ataques. Em 3 de novembro de 2020, o Superior Tribunal de Justiça (STJ) sofreu um dos maiores ataques já registrados contra uma instituição pública no país [19]. O ataque do tipo *ransomware* bloqueou o acesso a dados e sistemas da Corte por quase duas semanas, com impacto direto na tramitação de processos judiciais e perda parcial de dados relacionados a atividades internas [19, 106].

Ainda em 2020, o Ministério da Saúde foi protagonista de dois vazamentos de grandes proporções. O primeiro ocorreu devido a uma falha no sistema *e-SUS Notifica*, que expôs informações de aproximadamente 240 milhões de brasileiros, incluindo CPF (Cadastro de Pessoa Física), endereço e dados de saúde. O segundo incidente envolveu a publicação acidental de senhas de acesso ao *E-SUS-VE* e ao *SIVEP-Gripe* por um colaborador de um hospital parceiro, o que comprometeu informações sensíveis, como doenças preexistentes e histórico clínico de milhões de cidadãos [107].

Mais recentemente, em maio de 2024, um ataque cibernético comprometeu o *Sistema Eletrônico de Informações* (SEI) do Ministério da Gestão e Inovação (MGI), afetando oito ministérios e dois órgãos financeiros interligados [108]. O SEI é um sistema fundamental para a tramitação de documentos na administração pública federal [109]. A indisponibilidade do sistema por sete dias impactou severamente os fluxos administrativos, evidenciando a dependência crítica da gestão pública em relação à infraestrutura digital [110].

Esses episódios reforçam a necessidade de adoção de uma cultura de segurança cibernética, tanto no setor público quanto no privado. Mais do que investir em tecnologias, é fundamental aprimorar processos de gestão de risco, governança de TI e resposta a incidentes, sob pena de comprometer não apenas a continuidade operacional, mas também a confiança da sociedade nas instituições.

## 2.6 MODELOS DE SEGURANÇA CIBERNÉTICA

Diferentes *frameworks* de segurança proporcionam abordagens estruturadas para identificar e mitigar ameaças cibernéticas, cada um com foco e aplicação específicos [26]. No contexto deste estudo, destacam-se o CIS Controls v8.1, o MITRE ATT&CK e o Community Defense Model (CDM), que oferecem abordagens complementares para a proteção de servidores web. Enquanto o CIS Controls v8.1 fornece diretrizes práticas para melhorar a postura de segurança de forma geral, o MITRE ATT&CK ajuda a entender o com-

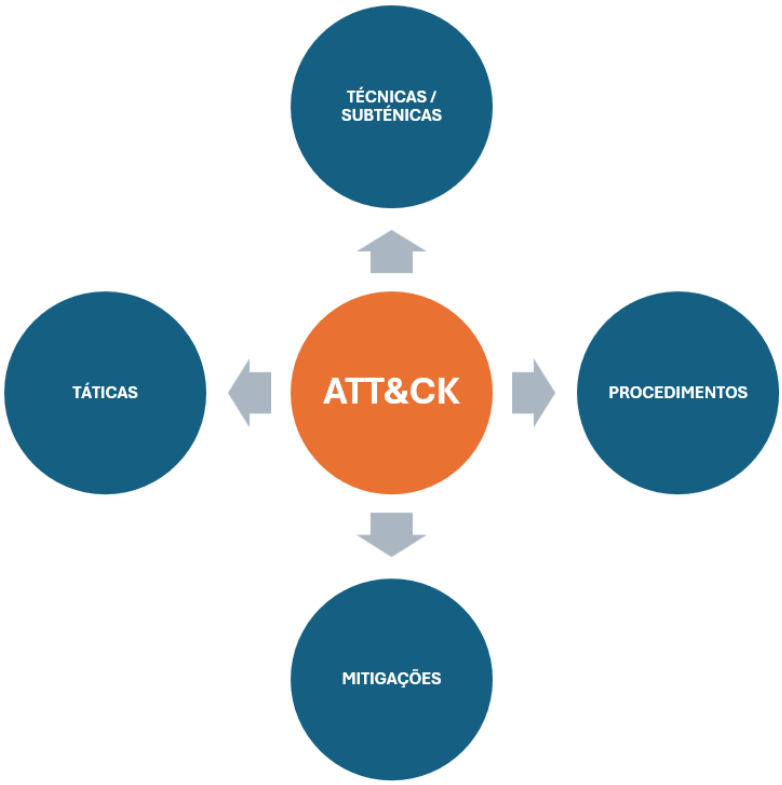


Figura 2.1: Principais Componentes do *framework* MITRE ATT&CK. Fonte: Própria.

portamento dos agentes maliciosos por meio do mapeamento de táticas e técnicas. O CDM, por sua vez, traduz as medidas do CIS Controls em uma estratégia orientada para mitigar ataques cibernéticos comuns, como o *Web Application Hacking*.

### 2.6.1 MITRE

O MITRE ATT&CK (*Adversarial Tactics, Techniques, and Common Knowledge*) é um *framework* aberto, criado em 2013 no âmbito do Fort Meade eXpérience (FMX) da MITRE, que sistematiza o comportamento de agentes maliciosos reais em redes corporativas por meio de táticas, técnicas e procedimentos [111, 112]. Inicialmente, o modelo era voltado ao ambiente Windows, mas a partir de 2017, passou a incorporar cenários para MacOS, Linux e dispositivos móveis (Mobile), evoluindo ainda para ambientes em nuvem (2019) e Sistemas de Controle Industrial (ICS - Industrial Control Systems) (2020) [111]. O MITRE ATT&CK oferece um vocabulário comum e um mapa didático que orienta tanto exercícios de simulação contra um agente malicioso quanto estratégias de detecção e mitigação de ameaças [111, 113].

Embora o MITRE ATT&CK também disponibilize os modelos *Mobile* e ICS, este trabalho foca exclusivamente no MITRE ATT&CK for Enterprise, voltado a redes corporativas e ambientes em nuvem [112], visto que este modelo é o mesmo utilizado como base no CDM v2.0 [4].

O *framework* MITRE ATT&CK for Enterprise é organizado em cinco componentes principais, como ilustrado na Figura 2.1.

As **táticas** representam o objetivo do agente malicioso ao utilizar determinada técnica [111]. Dessa

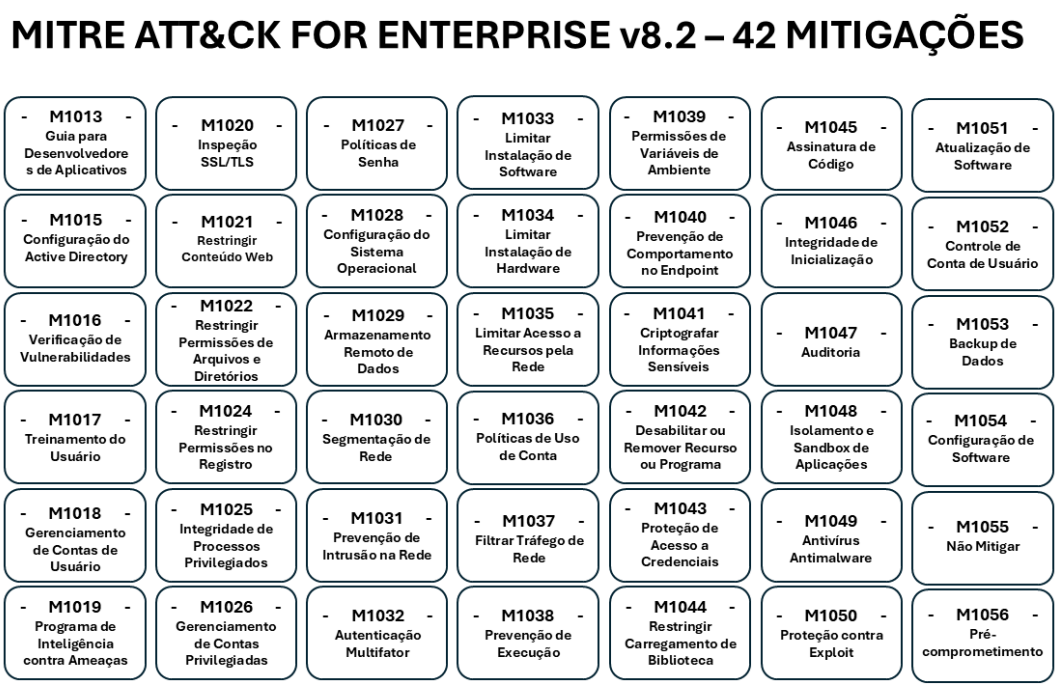


Figura 2.2: Mitigações presente no Framework MITRE ATT&CK versão 8.2. Fonte: Tradução e Adaptação de [1].

forma, elas apontam para o "por que" do seu uso, como descobrir informações, executar arquivos ou exfiltrar dados [114].

Já as **técnicas** podem representar "como" o agente malicioso atinge o objetivo tático. Um exemplo seria a tentativa de várias combinações de usuários e senhas até encontrar credenciais válidas. As técnicas também podem indicar "o que" o agente ganha ao executar uma ação. Por exemplo, por meio da tática Descoberta, o agente malicioso pode usar técnicas para buscar uma informação específica [111].

As **sub-técnicas** são meios mais específicos pelos quais os agentes maliciosos alcançam objetivos táticos em um nível inferior às técnicas. Por exemplo, acessar o /etc/passwd [13] [111]. **Procedimentos** são as implementações específicas que os agentes maliciosos usam para técnicas ou sub-técnicas [111].

Finalmente, **mitigações** representam conceitos de segurança e classes de tecnologias que podem ser usadas para impedir que uma técnica ou sub-técnica seja executada com sucesso [111]. Mitigações endereçam "o que fazer" sobre Táticas, Técnicas e Procedimentos [112].

Apesar do MITRE estar em sua *release* 17.1 (abril de 2025), este trabalho utiliza a versão 8.2 desse *framework*, já que ela consiste na base do mapeamento de mitigações por medidas de segurança do CIS Controls v8 utilizado pelo CDM 2.0 [4]. Detalhes sobre o CDM v2.0 são apresentados na Seção 2.6.2.

Ainda sobre a versão 8.2 do MITRE ATT&CK for Enterprise, ela contém 14 táticas, 177 técnicas, 348 subtécnicas e identifica um total de 42 mitigações voltadas à redução do impacto dessas ações adversas, conforme ilustrado na Figura 2.2. Detalhes das mitigações podem ser encontrados no Apêndice A.

O entendimento dos componentes do MITRE ATT&CK permite não apenas mapear o comportamento

[13] O arquivo passwd é um banco de dados baseado em texto simples, que contém informações sobre todas as contas de usuários encontradas no sistema [115, 116].


Figura 2.3: Os 18 Controles do CIS Controls v8.1. Fonte: CIS [2]

adversário, mas também correlacionar essas ações às medidas de defesa, como será explorado na próxima seção (2.6.2).

### 2.6.2 Framework CIS Controls

O Center for Internet Security® (CIS®) é uma organização que se define sem fins lucrativos voltada para comunidade, responsável, atualmente, pelas publicações CIS Controls e CIS Benchmarks™ [14], sob Licença Pública Internacional Creative Commons Atribuição-Não Comercial-SemDerivações 4.01 [2].

O CIS Controls, na versão 8, é um *framework* de melhores práticas de segurança que reflete o conhecimento combinado de especialistas de vários ecossistemas e atribuições [2]. Esse conhecimento combinado tem gerado uma ampla adoção por organizações ao redor do mundo [26], o que inclui o governo federal do Brasil no PPSI (ver 2.2.2).

O *framework* é organizado em 18 controles, sendo cada um deles contendo um subconjunto de medidas de segurança, que ao todo totalizam 153 Medidas de Segurança (*safeguards*) (ver Figura 2.3). Neste estudo, essas medidas foram avaliadas para práticas de segurança voltadas especificamente para servidores web, permitindo uma comparação estruturada com o ataque Web Application Hacking (WAH) do CDM [4].

**CIS Community Defense Model 2.0**

O CIS Community Defense Model 2.0 (CDM v2.0), também desenvolvido pelo CIS, foi criado com o

[14] As licenças públicas Creative Commons oferecem um conjunto padrão de termos e condições que criadores e outros detentores de direitos podem utilizar para compartilhar obras originais de autor, outros materiais sujeitos a direito de autor e direitos conexos, e certos outros direitos especificados na licença pública [117]

objetivo de demonstrar quão efetivo pode ser o CIS Controls frente aos ataques cibernéticos mais prevalentes. Para tanto, sua estrutura organiza as 153 medidas do CIS Controls v8 para mitigar cinco categorias de ameaças cibernéticas: *Malware, Ransomware, Web Application Hacking, Insider and Privilege Misuse e Targeted Intrusions* [4].

Essas categorias foram definidas com base na análise de dados empíricos extraídos de fontes como o *Verizon Data Breach Investigations Report* (DBIR) [24] e outras estatísticas sobre incidentes reais, visando representar os tipos de ataques mais recorrentes e com maior impacto nos ambientes corporativos. A partir dessas ameaças, o CDM estrutura padrões de ataque que combinam técnicas e subtécnicas do *framework* MITRE ATT&CK for Enterprise v8.2 e os correlaciona diretamente com as medidas de segurança do CIS Controls v8 [4].

Os resultados do CDM v2.0 indicam que a implementação de todas as medidas relacionadas a essas cinco ameaças proporciona uma proteção de 91% frente às subtécnicas descritas no MITRE ATT&CK v8.2 [4]. Esse dado reforça a utilidade do CDM como uma ferramenta de apoio à tomada de decisão estratégica em segurança cibernética.

Para a comparação com o Modelo 3SW, foi selecionado o ataque Web Application Hacking (WAH) do CDM — a partir daqui denominado Modelo WAH ou apenas WAH — por sua relação direta com servidores web, foco desta pesquisa. A Tabela 2.2 apresenta os cinco tipos de ataques do CDM, incluindo suas definições [4], alvos principais e relação com servidores web, justificando a escolha do WAH como base de comparação.

Tabela 2.2: Tipos de Ataques do CDM e Relação com Servidores Web. Retirado e adaptado de [4]

| **Tipo de Ataque** | **Definição** | **Alvo Principal** | **Relação com Servidores Web** |
|---|---|---|---|
| *Malware* | Programas maliciosos, como *crimeware*, que exploram sistemas de forma oportunista e financeiramente motivada, comuns em campanhas de e-mails fraudulentos. | Endpoints, estações de trabalho e servidores de uso geral. | Impacto indireto: pode atingir servidores web caso infecte sistemas conectados, mas não é concebido para explorar vulnerabilidades de aplicações web [118]. |
| *Ransomware* | Criptografa arquivos em sistemas ou redes, exigindo pagamento para restauração, com crescimento acentuado (715,08%) em 2020. | Sistemas de armazenamento e infraestrutura corporativa. | Impacto indireto: embora possa comprometer dados hospedados em servidores web, o vetor primário de ataque é voltado a sistemas de arquivos, não a aplicações web [101]. |
| *Web Application Hacking* (WAH) | Ataques direcionados a aplicações web, representando 80% das violações, como injeções (SQL, NoSQL) e *Cross-Site Scripting* (XSS). | Servidores web e aplicações hospedadas (locais ou em nuvem). | Impacto direto: explora vulnerabilidades típicas de aplicações web expostas à internet, como as presentes nos sistemas avaliados no estudo de caso. |
| *Insider and Privilege Misuse* | Abuso intencional de privilégios ou uso indevido de configurações por usuários internos. | Sistemas internos, bases de dados e infraestrutura restrita. | Relevância limitada: normalmente não envolve exploração remota de aplicações web, mas sim mau uso interno de acessos legítimos. |
| *Targeted Intrusions* | Ataques patrocinados por estados ou grupos avançados, visando ganhos políticos, econômicos ou estratégicos, frequentemente por *phishing* (81%) e *malware* (92%). | Ativos críticos e dados sensíveis de governos ou empresas estratégicas. | Impacto eventual: pode incluir servidores web como parte da infraestrutura comprometida, mas o foco principal está na exfiltração de dados estratégicos e espionagem. |

A escolha do Modelo WAH como base de comparação com o Modelo 3SW fundamenta-se em três fatores principais.

Primeiro, sua **aderência ao escopo**: entre os cinco ataques do CDM, o WAH é o único cujo vetor primário é a exploração de vulnerabilidades em aplicações web e servidores web expostos, coincidindo exatamente com o foco desta pesquisa.

Segundo, sua **magnitude estatística**: o WAH representa mais de 80% das violações reportadas no *Verizon DBIR 2020* [119], superando os demais tipos de ataque do CDM em incidência direta contra aplicações web. Além disso, 73% das violações em ambientes de nuvem envolvem servidores de e-mail ou aplicações web, evidenciando o papel central desses ativos no cenário atual de ameaças [4].

Terceiro, seu **alinhamento com casos reais**: a superfície de ataque dos sistemas públicos expostos, como o e-SUS *Notifica* [107], é compatível com as técnicas associadas ao WAH, incluindo injeções, falhas de autenticação e *Cross-Site Scripting*.

Assim, a comparação com o WAH permite avaliar a eficácia do 3SW em mitigar ameaças diretamente relacionadas ao contexto de servidores web, contribuindo para a segurança cibernética em órgãos públicos e alinhando-se ao objetivo central desta dissertação.

Diante desse contexto, na próxima seção são apresentados os trabalhos relacionados, que abordam modelos, metodologias e práticas voltadas à priorização de medidas de segurança para ativos específicos, como servidores web.

## 2.7 TRABALHOS RELACIONADOS

A adaptação de *frameworks* de segurança cibernética a contextos organizacionais específicos tem sido uma prática recorrente na literatura recente. Essa abordagem busca adequar metodologias generalistas, como o NIST, ISO/IEC 27001 e o CIS Controls, a ambientes técnicos distintos, de forma a enfrentar riscos de maneira mais eficiente e contextualizada [26, 120, 121]. Nesse contexto adaptativo, modelos de maturidade [122], ferramentas de priorização [123] e mecanismos automatizados de apoio à decisão [124] têm sido amplamente propostos.

Dentre os *frameworks* analisados, o CIS Controls tem consolidado-se como uma das metodologias mais adotadas globalmente, conforme identificado por Juma et al. [26] em sua revisão sistemática, de modo que o cenário brasileiro na escolha do CIS Controls para o PPSI, não é uma exceção. Em estudo comparativo, Crotty e Daniel [29] destacaram que, entre os modelos ISO, NIST e CIS Controls v7.1, este último apresenta maior objetividade na orientação sobre sequenciamento e priorização de controles, sendo particularmente útil para pequenas e médias empresas.

Retomando o tema da adaptação de *frameworks* a contextos específicos, destaca-se a definição de controles prioritários como estratégia recorrente para aumentar a efetividade das medidas de segurança [2]. Nesse sentido, Rahman e Williams [125] analisaram o mapeamento entre os controles do NIST SP800-53 e técnicas do MITRE ATT&CK, identificando um subconjunto de 20 controles críticos capazes de mitigar até 72% das técnicas empregadas por 98% dos grupos adversários catalogados. Horta et al. [123], por sua vez, utilizaram métodos de apoio à decisão multicritério (MCDA - *Multi Criteria Decision Analysis*) para ranquear ações com base em simulações de ataques, evidenciando o potencial dessas abordagens na

priorização de medidas de segurança.

Kern et al. [126] propuseram um modelo de maturidade para monitoramento de rede e auditoria de logs, baseado em dois controles do CIS Controls v8, com validação a partir da estrutura MITRE ATT&CK. A proposta contribui com um processo decisório mais alinhado à realidade da organização, levando em conta custo, relevância e conformidade. De forma complementar, Skopik et al. [127] ressaltaram a importância da observância a boas práticas para evitar lacunas no monitoramento de segurança.

Na esfera da automação, Gonzalez-Granadillo et al. [124] desenvolveram o *kit* AMBIENT, que incorpora módulos de avaliação de riscos cibernéticos, privacidade e mitigação. O modelo utiliza como base os *frameworks* NIST 800-53, CIS Controls e ISO 27001, e visa fornecer suporte à decisão com recomendações específicas de salvaguardas.

Cue et al. [128] propuseram um sistema de pontuação baseado no CIS Controls v8, combinando métodos de ranqueamento com ponderação harmônica, visando orientar gestores na priorização de ações e acompanhar a evolução da implementação dos controles ao longo do tempo.

Estudos voltados à avaliação de maturidade organizacional também têm utilizado o CIS Controls como base. Bashofi e Salman [122] propuseram um modelo de maturidade combinando NIST CSF, CIS Controls v8 e ISO/IEC 27002 para avaliação de uma instituição pública. Abohatem e Ba-Alwi [129] conduziram avaliação similar na Yemen Telecoms, resultando em uma estrutura com 14 controles macros. Já AL-Hawamleh [130] e Carías et al. [131] propuseram modelos de progressão para construção de políticas de resiliência cibernética, enfatizando a evolução das capacidades organizacionais.

Um exemplo relevante de contextualização dos CIS Controls é o guia especializado para Sistemas de Controle Industrial (ICS - *Industrial Control Systems*), publicado pelo CIS [132]. O documento reconhece as restrições técnicas, contratuais e operacionais desses ambientes e apresenta uma análise das 153 medidas de segurança do CIS Controls v8.1, indicando sua aplicabilidade e os principais desafios de implementação. Além disso, o guia ressalta aspectos específicos desse contexto, como a segmentação de rede, o uso de protocolos proprietários, a priorização da disponibilidade e as implicações de garantias contratuais de fornecedores, elementos que frequentemente se mostram distintos das práticas tradicionais de TI.

Dentre os estudos que mais se aproximam da proposta deste trabalho, destaca-se a pesquisa de Disanayake et al. [133], que propõe um *framework* racionalizado para aplicações web com base em duas dimensões: criticidade operacional e criticidade de dados. A partir dessas métricas, os autores classificam as aplicações em zonas de segurança, sugerindo *frameworks* adequados a cada nível. O modelo oferece um equilíbrio entre proteção e uso racional de recursos, alinhando-se à realidade de organizações com limitações orçamentárias ou operacionais.

Ainda no contexto de aplicações web, Song e García-Valls [134] propuseram uma abordagem de automonitoramento para servidores de IoT (*Internet of Things*) críticos, com foco em segurança web. Já Fadlil et al. [135] desenvolveram uma metodologia baseada na OWASP (Open Worldwide Application Security Project) para mitigar vulnerabilidades do tipo SQLi em servidores web.

Essas contribuições demonstram que a adaptação e especialização de *frameworks* de segurança cibernética são fundamentais para ampliar sua efetividade. Nesse sentido, o Modelo 3SW proposto nesta dissertação segue essa linha de raciocínio ao selecionar e priorizar medidas específicas do CIS Controls

v8.1 voltadas à proteção de servidores web, considerando critérios operacionais e contextuais definidos na metodologia adotada.

Para concluir, a Tabela 2.3 sintetiza os principais trabalhos relacionados, comparando-os com o Modelo 3SW proposto nesta dissertação. A comparação considera a utilização de *frameworks* como MITRE ATT&CK, CIS Controls e o Community Defense Model (CDM), o foco em ativos específicos e a aplicabilidade a servidores web ou sistemas. Essa análise destaca a singularidade do 3SW, que integra esses elementos para priorizar medidas de segurança específicas para servidores web.

Tabela 2.3: Comparação de Trabalhos Relacionados com o Modelo 3SW

| Autor(es) | MITRE | CIS Controls | CDM | Foco em Ativo | Servidores Web |
|---|---|---|---|---|---|
| Rahman e Williams [125] | ✓ | x | x | x | x |
| Horta et al. [123] | ✓ | ✓ | x | x | x |
| Kern et al. [126] | ✓ | ✓ | x | x | x |
| Gonzalez-Granadillo et al. [124] | x | ✓ | x | x | x |
| Cue et al. [128] | x | ✓ | x | x | x |
| Bashofi e Salman [122] | x | ✓ | x | x | x |
| Abohatem e Ba-Alwi [129] | x | ✓ | x | x | x |
| AL-Hawamleh [130] | x | ✓ | x | x | x |
| Carías et al. [131] | x | x | x | x | x |
| Disanayake et al. [133] | x | ✓ | x | ✓ | ✓ |
| Song e García-Valls [134] | x | x | x | ✓ | ✓ |
| Fadlil et al. [135] | x | x | x | ✓ | ✓ |
| CIS Controls ICS [132] | x | ✓ | x | ✓ | x |
| PPSI [3] | x | ✓ | x | ✓ | x |
| **Este trabalho** | ✓ | ✓ | ✓ | ✓ | ✓ |

**Legenda:** ✓ – Presença do elemento no trabalho; x – Ausência do elemento; MITRE - MITRE ATT&CK; CDM – *Community Defense Model*. A última linha destaca o Modelo 3SW proposto nesta dissertação.

# 3 METODOLOGIA

Para organizar os objetivos metodológicos e os diferentes momentos do estudo, a pesquisa foi dividida em quatro fases macro, sendo duas de apoio (Planejamento de Pesquisa e Fundamentação Teórica) e duas centrais (Desenvolvimento do Modelo 3SW e Validação do Modelo 3SW), como ilustrado na Figura 3.1.

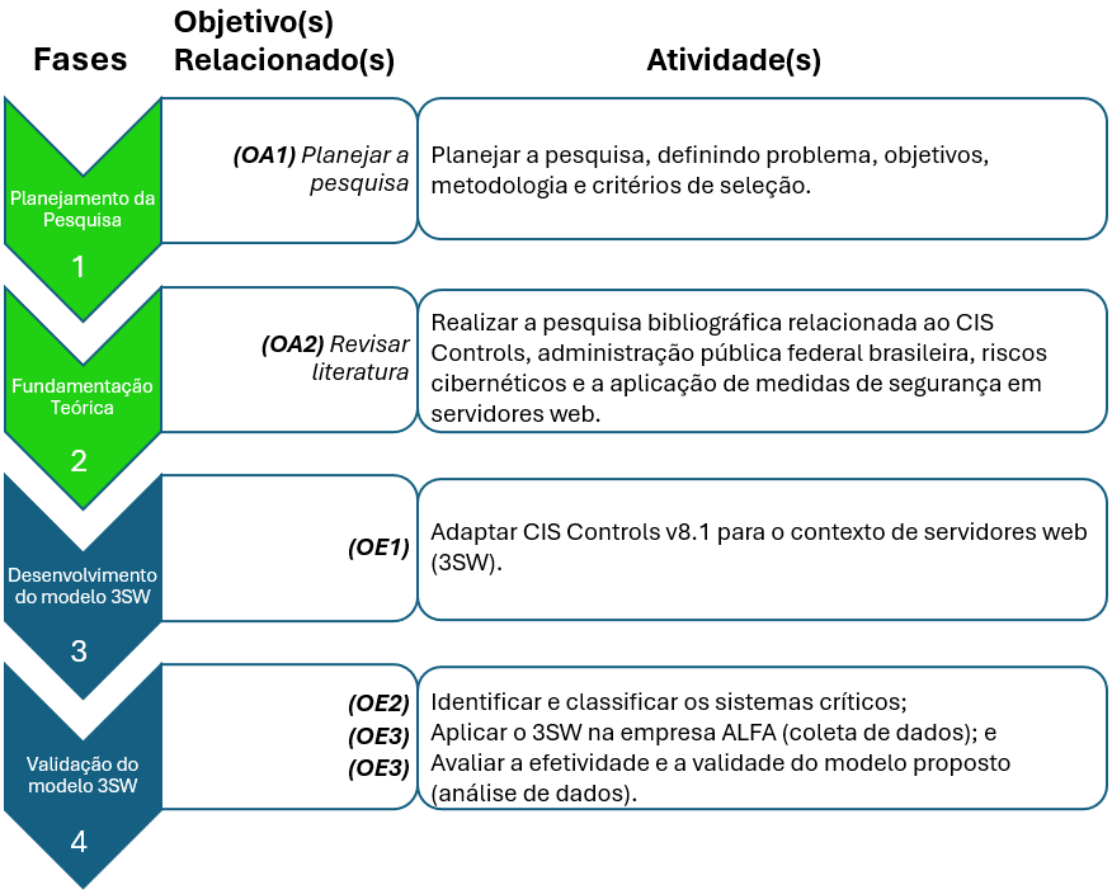


Figura 3.1: Fases, Objetivos e Atividades da Metodologia de Pesquisa. Fonte: Própria

As fases de apoio estão marcadas na Figura 3.1 na cor verde e não estão diretamente vinculadas aos Objetivos Específicos (OE). Entretanto, para garantir a coesão metodológica, foram definidos Objetivos de Apoio (OA) que norteiam suas atividades. Já as fases centrais (marcadas em cor azul) têm como propósito principal verificar a validade da hipótese da pesquisa, sendo, portanto, associadas diretamente aos OE definidos no Capítulo 1 (Introdução). Cabe destacar que o OE3, por tratar da verificação de efetividade do modelo, se desdobra em duas atividades distintas, distribuídas na Fase 4, que será aprofundada nas seções a seguir. A descrição detalhada de cada fase é apresentada na sequência.

**F1 Planejamento da Pesquisa:** Nessa fase foi desenvolvido o **plano de pesquisa** (OA1) contendo a definição do problema, dos objetivos, da hipótese, das questões de pesquisa e da escolha do método (estudo de caso). A fase também abrange a definição dos critérios metodológicos para a seleção de informações e de documentos, bem como a definição de cronograma para a execução e a análise dos

resultados.

**F2 Fundamentação Teórica:** Nessa fase foi realizada uma **revisão de literatura** (OA2) com o objetivo de encontrar artigos relacionados aos temas: Segurança da Informação e Segurança Cibernética, Governo Federal do Brasil e a Segurança da Informação, Gestão de Riscos, *framework* CIS Controls, *framework* MITRE ATT&CK e medidas de segurança para servidores web. Além disso, houve análise documental de arquivos presentes e relacionados aos temas de segurança da informação e gestão de riscos na Empresa ALFA. Essa fase foi essencial para a escrita do Capítulo 2 e apoiou a execução da fase **F3**.

**F3 Desenvolvimento do Modelo 3SW:** Foi realizada a **adaptação do CIS Controls v8.1 para o contexto de servidores web (3SW)** (OE1). Para a adaptação, foi empregada a metodologia de análise de conteúdo (inspirada em Bardin [41]), que envolve três etapas: pré-análise (planejamento da análise), exploração do material e tratamento dos resultados. O resultado dessa fase foi publicado na Revista RISTI [42].

**F4 Validação do Modelo 3SW:** A última fase da metodologia de pesquisa (**F4**) **realiza a análise e a classificação dos sistemas pelo Gestor de TI** (OE2). Em seguida, o Modelo 3SW é, então, **aplicado em um estudo de caso para verificar sua aplicabilidade** (OE3). Por fim, é **verificado a efetividade e a validade desse modelo** (OE3). A validação utiliza-se da comparação de cenários pré e pós-implementação, a utilização de métricas quantitativas e o *feedback* dos participantes sobre o modelo proposto. Mais detalhes podem ser encontrados na Seção 3.2.1.

Como mencionado anteriormente, as Fases 1 e 2 oferecem suporte conceitual e estrutural à pesquisa, não estando diretamente relacionadas à validação da hipótese central. Por essa razão, as próximas seções concentram-se em detalhar as Fases 3 e 4 — consideradas centrais — por reunirem as atividades empíricas e analíticas associadas aos Objetivos Específicos (OE1, OE2 e OE3) e à aplicação prática do Modelo 3SW.

## 3.1 FASE 3: DESENVOLVIMENTO DO 3SW

A Fase 3 consiste na construção do Modelo 3SW (OE1) por meio da adaptação do CIS Controls v8.1 ao contexto dos servidores web. Como resultado, essa etapa gerou um subconjunto de medidas de segurança voltado a esse tipo de ativo, cuja seleção foi orientada pelos critérios definidos na metodologia. O resultado desta fase foi posteriormente aplicado na Fase 4 – Validação do Modelo 3SW (**F4**).

### 3.1.1 Construção do 3SW

A construção do Modelo 3SW foi fundamentada na análise das medidas de segurança presentes no CIS Controls v8.1, com foco em sua aplicação ao contexto de servidores web, conforme previsto no Objetivo Específico OE1. Para tanto, adotou-se uma abordagem exploratória de natureza qualitativa, voltada à redução, categorização e interpretação das informações disponíveis [136].

A análise foi conduzida com base na metodologia de análise de conteúdo proposta por Bardin [41], considerada apropriada para o tratamento e a organização sistemática de dados. Essa metodologia foi estruturada em três etapas principais, conforme ilustrado na Figura 3.2. A primeira delas, denominada **Pré-análise**, compreende as seguintes atividades: **seleção do material a ser analisado**, **definição da estratégia de análise** e **definição dos critérios qualitativos** utilizados na avaliação dos controles.

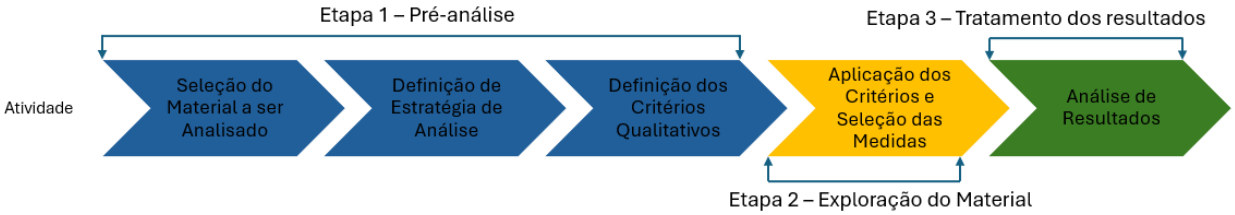


Figura 3.2: Etapas e Atividades da Construção do 3SW. Fonte: Própria

Na atividade **Seleção do Material a ser Analisado** (Etapa 1 - Pré-Análise), foi aplicada a regra de pertinência [41], em que os documentos selecionados devem corresponder ao objetivo da análise. Como resultado da execução desse passo, foram selecionados os *frameworks* CIS Controls v8.1, que guia a implementação de medidas de segurança [2]; o MITRE ATT&CK, que apresenta um conjunto de técnicas e táticas que podem ser utilizadas por agentes maliciosos, bem como formas utilizadas para mitigá-los [113]; e o CDM v2.0, que disponibiliza um mapeamento do CIS Controls v8 com as mitigações presentes no *framework* MITRE ATT&CK [113]. Nesse momento é importante frisar que, embora este estudo utilize o CIS Controls v8.1, essa versão não alterou o propósito das medidas de segurança da versão 8.0, garantindo a validade das análises do CDM v2.0 [2].

Na atividade subsequente, **Definição da Estratégia de Análise** (Etapa 1), foram formuladas três questões de pesquisa (QP) —– sendo duas operacionais e uma comparativa —– com o objetivo de orientar a seleção e a priorização das medidas de segurança no contexto da análise qualitativa, bem como permitir a comparação com abordagem similar:

QP1. É possível selecionar as medidas de segurança do CIS Controls v8.1 para prevenir ou mitigar vulnerabilidades de cibersegurança em Servidores Web?

QP2. As medidas de segurança selecionadas podem ser classificadas por esforço de implementação e manutenção, de modo a serem priorizadas?

QP3. Como o 3SW difere do Web Application Hacking do CDM?

Essas questões foram derivadas das questões mais amplas definidas na Fase 1 (Planejamento da Pesquisa) e serviram de referência direta para a estruturação dos critérios qualitativos (Tabela 3.1).

A atividade **Definição dos Critérios Qualitativos** (Etapa 1) estruturou seis critérios qualitativos, listados na Tabela 3.1, que consideram o escopo das questões de pesquisa QP1 e QP2.

Como pode ser visto na Tabela 3.1, os critérios foram divididos em **Critérios de Seleção (CS)** e **Critérios de Priorização (CP)**. Para compor o 3SW, a medida de segurança precisa receber "Sim" em todos os CS. Essa ação, além de considerar o escopo da hipótese que trata de ataques cibernéticos em

Tabela 3.1: Critérios para seleção e priorização de Medida de Segurança

| Tipo | Critérios | Respostas Possíveis |
|---|---|---|
| Seleção | CS1 - A medida está no escopo do Servidor Web [1]? | Sim/Não |
| Seleção | CS2 - A medida pode ser individualizada? | Sim/Não |
| Seleção | CS3 - A medida pode ser verificada como implementada no servidor web? | Sim/Não |
| Priorização | CP1 - A medida pode ser implementada e gerida diretamente no Servidor Web, sem depender de recursos, softwares ou serviços externos contínuos? | Sim/Não |
| Priorização | CP2 – Qual o esforço para implementar a medida no Servidor Web? | Baixo/Moderado/Alto |
| Priorização | CP3 – Qual o esforço para manter a medida aplicada e atualizada no Servidor Web? | Baixo/Moderado/Alto |

servidores web (CS1), também inclui outros dois aspectos: a possibilidade de individualização das medidas durante a aplicação para fins de priorização das ações (CS2); e a possibilidade da medida ser verificada no intuito de avaliar o êxito de sua aplicação (CS3).

Após a aplicação dos CS, o CP1 avalia as medidas de segurança selecionadas para priorização, distinguindo aquelas que podem ser implementadas diretamente no Servidor Web das que dependem de recursos ou serviços externos contínuos. Em seguida, os CP2 e CP3, avaliam o esforço necessário para implementar e manter as medidas, utilizando uma escala de “Baixo”, “Moderado” ou “Alto”, inspirada no NIST SP 800-55v1 [5]. A Tabela 3.2 apresenta as descrições para as categorias de esforço.

Tabela 3.2: Categorias por Esforço (Baseado no NIST SP 800-55v1 [5])

| Esforço | Implementar a Medida | Manter a Medida |
|---|---|---|
| Baixo | Requer pouco tempo, recursos e esforço para configurar e integrar a medida. Pode envolver a implementação de soluções prontas para uso, seguindo procedimentos simples e diretos. | Requer pouco tempo, recursos e esforço para manter. A manutenção básica pode passar por atualizações de rotina, monitoramento periódico e ajustes mínimos. Geralmente não requer correções frequentes de bugs ou adaptações complexas. |
| Moderado | Requer um esforço significativo, mas gerenciável, para configurar e integrar a medida. | Requer um esforço significativo, mas gerenciável, para manter a medida, bem como pode necessitar de monitoramento regular, atualizações periódicas e ajustes ocasionais para garantir a continuidade da eficácia. |
| Alto | Requer significativo tempo, recursos e esforço, podendo envolver desenvolvimento personalizado, aquisição de hardware/software especializado e treinamento extensivo da equipe. | Requer significativo tempo, recursos e esforço, bem como pode necessitar de atualizações regulares, ajustes complexos e monitoramento contínuo para garantir a eficácia. |

A Etapa 2 - **Exploração do Material**, contém a atividade **Aplicação dos Critérios e Seleção das**

**Medidas**, nela são aplicados os critérios discriminados na Tabela 3.1, permitindo a análise dos documentos para compor o 3SW. Nessa fase, as medidas de segurança são selecionadas e categorizadas conforme seu esforço de implementação e manutenção.

Por fim, a Etapa 3 – **Tratamento dos Resultados**, última etapa da metodologia do 3SW, consiste na análise dos resultados obtidos a partir da aplicação dos critérios na Etapa 2. Nessa etapa, também é respondida a QP3, que compara o 3SW com o WAH, escolhido por ser o único ataque no CDM diretamente relacionado à segurança de servidores web e, assim, alinhado ao escopo dessa etapa.

## 3.2 FASE 4: VALIDAÇÃO DO MODELO 3SW

A Fase 4 consiste na validação do Modelo 3SW por meio da análise de sua aplicação em um estudo de caso conduzido na Empresa ALFA. Esta etapa consolida os dados obtidos durante a aplicação do modelo, utilizando uma abordagem metodológica mista (quantitativa e qualitativa) para verificar sua efetividade e aplicabilidade no contexto da segurança de servidores web (OE3).

Conforme argumentam Yin [136] e Gil [138], o estudo de caso permite uma investigação aprofundada de fenômenos organizacionais reais e favorece a compreensão de suas relações causais, sendo, portanto, adequado à validação de modelos em contextos específicos. A avaliação do 3SW baseou-se em dados empíricos coletados por meio de entrevistas estruturadas e semiestruturadas, análise de documentos institucionais e ferramentas técnicas de verificação de vulnerabilidades.

### 3.2.1 Validação do 3SW

Neste trabalho, o estudo de caso assume natureza exploratória e descritiva, pois busca compreender como o 3SW pode ser aplicado para reduzir ameaças em sistemas expostos à Internet. A partir disso, define-se a seguinte hipótese: **A implementação do 3SW pode contribuir para a redução da probabilidade de ataques bem-sucedidos contra servidores web, aumentando a resiliência desses sistemas frente às ameaças e vulnerabilidades cibernéticas**.

Para essa verificação, o estudo foi conduzido na Empresa ALFA, entidade com relevância no setor econômico brasileiro, que desempenha atividades essenciais relacionadas à prevenção, repressão e educação de diversas outras organizações nesse mesmo setor. A estrutura organizacional da Empresa ALFA está baseada nesses três pilares, os quais orientam sua missão institucional.

Dentro de sua estrutura organizacional, a unidade de Tecnologia da Informação tem como responsabilidade principal a gestão de recursos tecnológicos, que inclui a proteção de sistemas e dados críticos para o funcionamento da organização. Em decorrência da relevância da Empresa ALFA para o setor econômico, o sigilo e a integridade das informações, que por ela são coletadas, processadas ou armazenadas, são fundamentais, pois qualquer comprometimento desses dados pode prejudicar gravemente a imagem e a confiança da instituição.

Nesse contexto, as unidades de análise do Estudo de Caso foram:

1. O **Setor de Tecnologia da Informação (TI)**, que gerencia a infraestrutura de TI e as políticas de segurança da informação;

2. Os **Sistemas Críticos** à missão institucional, que são essenciais para as operações da Empresa ALFA e estão expostos à internet, tornando-se alvos potenciais de ataques.

#### 3.2.1.1 Coleta de Dados

Os procedimentos de coleta de dados neste Estudo de Caso foram realizados por meio de pesquisa documental, entrevistas e a utilização de softwares de análise de vulnerabilidades.

A **pesquisa documental** foi realizada com o objetivo de obter um panorama detalhado sobre as políticas, as diretrizes, os processos de segurança da informação adotados pela Empresa ALFA, bem como os dados computados sobre esses processos e as análises registradas. A fonte principal dessas informações na Empresa ALFA foram os repositórios internos, que possuem um caráter restrito aos membros da equipe de segurança da informação dessa empresa.

Para as **entrevistas**, inicialmente foi analisada a estrutura organizacional para identificar as pessoas mais próximas ao tema tratado nesta dissertação, que relaciona a proteção de sistemas da informação e a criticidade deles diante da missão institucional. Dessa análise, foram identificados dois cargos cujas ações estavam diretamente relacionadas com o tema tratado: o Gestor de TI, responsável por gerir os recursos de TI, e o Chefe de Segurança da Informação, responsável pela gestão de segurança da informação dos ativos institucionais. Frisa-se que, na estrutura da Empresa ALFA, os dois mantêm uma relação hierárquica, o que os aproxima das decisões tomadas sobre a proteção de sistemas da informação.

As duas entrevistas seguiram cenários de atuação diferentes devido à natureza e à necessidade da pesquisa. A entrevista com o Gestor de TI foi do tipo estruturada, sendo apresentada uma lista fechada de sistemas a serem avaliados quanto à criticidade de cada um deles perante a missão institucional [136] (detalhada em 3.2.2.1). Nesse cenário, não foi necessária a gravação de áudio ou de vídeo. Enquanto a entrevista do Chefe de Segurança da Informação (Tabela B.2 no Apêndice B) foi do tipo semiestruturada, com perguntas abertas e visou identificar lacunas no programa PPSI e no CIS Controls, bem como uma avaliação da proposta desta dissertação [136]. Por se tratar de uma entrevista com perguntas abertas, ela foi realizada por meio de videoconferência, de modo que pudessem ser gravadas e revisitadas, pois nem sempre é possível identificar o que foi importante durante uma entrevista [139]. A Tabela 3.3 condensa as características da entrevista para cada um dos participantes.

**Softwares de Análise de Vulnerabilidades.** No que tange à coleta (identificação) de vulnerabilidades, foram utilizadas as ferramentas presentes no processo institucional de gestão de vulnerabilidades da Empresa ALFA. Nesse processo, a organização recorre a ferramentas pagas, gratuitas e de código aberto que auxiliam na detecção direta de vulnerabilidades ou indicam caminhos para sua identificação. Esse trabalho é complementado pela atuação dos analistas, que realizam verificações manuais com o intuito de explorar falhas que eventualmente não tenham sido detectadas pelas ferramentas automatizadas.

Por motivos de segurança da informação e confidencialidade institucional, optou-se por apresentar apenas as categorias das ferramentas utilizadas, de modo a não expor tecnologias específicas ou potenciais

Tabela 3.3: Perfil das Entrevistas

| Participante | Perfil | Tipo da Entrevista | Propósito |
|---|---|---|---|
| Gestor de TI | Mais de 10 anos como Gestor de TI na Empresa ALFA | Estruturada | Identificar a criticidade dos sistemas |
| Chefe de Segurança da Informação | 3 anos na Empresa ALFA e mais de 10 anos de experiência com Segurança da Informação | Semiestruturada | Identificar as lacunas do CIS Controls v8 na estrutura do PPSI |

fragilidades exploráveis por agentes maliciosos. A Tabela 3.4 apresenta essas categorias, juntamente com seus respectivos objetivos, vantagens e limitações.

As vulnerabilidades identificadas pelas ferramentas foram classificadas nos níveis de risco: **Crítico**, **Alto**, **Moderado**, **Baixo** e **Desconhecido**. Destaca-se ainda que as falhas detectadas manualmente pelos analistas não recebem classificação entre "Baixo" e "Crítico" — a fim de evitar subjetividade — e, portanto, são atribuídas ao nível de risco **Desconhecido**, garantindo que continuem sendo contabilizadas como vulnerabilidades identificadas.

Essas ferramentas desempenharam papel essencial na coleta de dados da pesquisa, fornecendo insumos quantitativos sobre vulnerabilidades presentes nos ativos analisados. A combinação entre ferramentas automatizadas e a atuação especializada dos analistas permitiu uma coleta abrangente e consistente, utilizada na comparação entre os cenários anteriores e posteriores à aplicação do Modelo 3SW.

#### 3.2.1.2 Aplicação do Modelo 3SW e Verificação das Medidas

Após a definição dos sistemas críticos da Empresa ALFA para o Estudo de Caso, foi realizada a aplicação do Modelo 3SW, que consiste na avaliação da aderência das medidas de segurança selecionadas para servidores web, segundo os critérios estabelecidos nesta dissertação.

A verificação da implementação das medidas considerou cinco possíveis estados, definidos para refletir a realidade de aderência dos sistemas frente às recomendações propostas:

- **Pré-existente (PR)**: A medida já estava completamente implantada e operacional no ambiente antes do início da aplicação do modelo proposto.
- **Implementada (I)**: A medida de segurança foi implantada durante o período de aplicação do modelo e está plenamente operacional.
- **Parcialmente Implementada (P)**: A medida foi implantada de forma parcial, seja por limitações técnicas, operacionais ou por não abranger todo o escopo necessário.
- **Não Implementada (N)**: A organização não possui nenhuma ação implementada correspondente à medida analisada.

Tabela 3.4: Categorias das Ferramentas Utilizadas na Identificação de Vulnerabilidades

| **Categoria da Ferramenta** | **Objetivo / Uso Principal** | **Vantagens** | **Possíveis Limitações** |
|---|---|---|---|
| Varredura de portas e serviços | Mapear serviços em execução, portas abertas e hosts ativos | Leves, rápidos e úteis na identificação inicial da superfície de ataque | Exige interpretação técnica precisa |
| Varredura de vulnerabilidades em rede | Identificar falhas conhecidas em sistemas operacionais, serviços e redes | Base de vulnerabilidades atualizada e cobertura ampla | Pode gerar falsos positivos; requer maior capacidade computacional |
| Varredura de vulnerabilidades em aplicações web | Detectar falhas em aplicações web, como XSS, SQLi, CSRF, falhas de autenticação e de configuração | Permite automação dos testes | Pode exigir ajustes finos; suscetível a falsos positivos |
| Ferramenta de análise manual de aplicações web (Proxy de interceptação) | Manipular e interceptar requisições HTTP/S para testes manuais e personalizados | Permite análise aprofundada e simulação de ataques reais | Necessita conhecimento técnico; curva de aprendizado elevada |
| Varredura de diretórios e arquivos ocultos | Descobrir caminhos ocultos em aplicações web que podem expor informações sensíveis | Leves, rápidos e fáceis de usar | Detectam apenas padrões conhecidos ou dicionários pré-definidos |
| Ferramentas de varredura passiva | Coletar informações sem interação direta com os alvos (ex.: cabeçalhos, *banners*, DNS) | Baixo impacto no ambiente, úteis para reconhecimento inicial | Resultados limitados sem varredura ativa complementar |

- **Não se Aplica (NA)**: A medida não se aplica ao contexto específico da organização ou ao ambiente dos servidores analisados.

Essa categorização foi adotada como instrumento de coleta de dados, permitindo mapear o grau de aderência das medidas do Modelo 3SW nos sistemas do Estudo de Caso. Posteriormente, os dados coletados foram utilizados na análise dos resultados, que evidencia o panorama de implementação das medidas, bem como as principais lacunas identificadas.

### 3.2.2 Classificação da Criticidade dos Sistemas com Base na Missão Institucional

A fim de aplicar o Modelo 3SW de forma alinhada às prioridades da organização ALFA, faz-se necessário classificar previamente os sistemas computacionais segundo sua criticidade à missão institucional. Essa classificação serve como base para a seleção dos sistemas que serão objeto da análise e aplicação do modelo, garantindo foco nos ativos que mais demandam atenção do ponto de vista da segurança da informação.

A missão da organização está ancorada em três pilares: prevenção, repressão e educação. Assim, considera-se que um sistema é crítico à missão institucional, quando uma falha relacionada à confidencialidade, integridade ou disponibilidade pode comprometer significativamente um desses pilares. A partir dessas informações, torna-se imprescindível a entrevista com o Gestor de TI da instituição para realizar a classificação dos sistemas, essa ação também permite a coleta estruturada de informações sobre os sistemas em uso.

#### 3.2.2.1 Estrutura da coleta para classificação dos Sistemas

O questionário aplicado (Tabela B.1 no Apêndice B) foi estruturado para coletar informações que permitam avaliar a criticidade de cada sistema. Para isso, foram definidos critérios baseados nas diretrizes da NBR ISO/IEC 27005:2023 [140], do NIST SP 800-30 Revision 1 [141], de legislações correlatas e de documentos institucionais da Empresa ALFA, como a metodologia de gestão de riscos e o plano de continuidade de negócios. A Tabela 3.5 apresenta os critérios utilizados na avaliação.

Tabela 3.5: Critérios para Avaliação da Criticidade dos Sistemas

| Critério | Descrição |
|---|---|
| **Confidencialidade (C)** | Avalia o impacto decorrente do acesso não autorizado a dados processados, armazenados ou transmitidos pelo sistema [142]. |
| **Integridade (I)** | Considera o impacto da modificação não autorizada ou não intencional de informações críticas [142]. |
| **Disponibilidade (D)** | Analisa os impactos que a interrupção de funcionamento do sistema pode causar nas atividades operacionais e institucionais [142]. |
| **Contribuição à Missão Institucional (M)** | Verifica se o sistema impacta diretamente ações de repressão, prevenção ou educação, pilares estratégicos da organização. |
| **Tipo de Dado Tratado** | Classifica os dados de acordo com sua natureza [133]:<br>- **Dados públicos**<br>- **Dados pessoais/sensíveis**, nos termos da LGPD [18]<br>- **Dados restritos**, com base em legislação específica da Empresa ALFA |

Com base nos critérios apresentados na Tabela 3.5, foi estruturada uma escala detalhada para representar os impactos potenciais sobre os atributos de segurança da informação: Confidencialidade (C), Integridade (I) e Disponibilidade (D). Os critérios foram desdobrados em cinco níveis graduais de impacto (de 1 – Muito Baixo – a 5 – Muito Alto), considerando três pilares: (i) os parâmetros do processo de gestão de riscos da Empresa ALFA; (ii) as diretrizes das normas NBR ISO/IEC 27005 [140] e NIST SP 800-30 [141]; e (iii) adaptações específicas ao contexto institucional, identificadas por meio das entrevistas e análise de documentos internos.

Na dimensão da Confidencialidade, os tipos de dados tratados — como dados públicos, pessoais, sensíveis ou restritos — foram associados aos níveis de impacto conforme seu potencial de dano, considerando não apenas a LGPD, mas também regulamentações internas específicas da Empresa ALFA. Por exemplo, a exposição de dados de inteligência ou investigações foi classificada como impacto muito alto (nível 5), enquanto dados públicos não estruturados foram classificados como impacto muito baixo (nível 1).

Para a Integridade, além da sensibilidade dos dados, considerou-se a relevância do sistema para os pilares da missão institucional (repressão, prevenção ou educação). Mesmo dados públicos podem representar impacto alto ou muito alto se sua modificação comprometer a transparência institucional ou direitos fundamentais — como no caso de sistemas que publicam decisões administrativas ou judiciais.

Já na Disponibilidade, os níveis de impacto foram diretamente inspirados na estrutura do Plano de Continuidade de Negócios da organização. O Tempo de Inatividade Máximo Tolerável (MTD) foi utilizado como referência: serviços que podem ficar indisponíveis por longos períodos sem afetar a operação foram classificados com impacto baixo ou muito baixo, enquanto sistemas com tempo crítico de resposta — como serviços de denúncia — foram enquadrados nos níveis mais elevados de impacto. Já sistemas de atendimento direto ao cidadão devem iniciar a avaliação de impacto com valor Médio (3). Essa adaptação garante alinhamento entre a escala e os tempos de recuperação operacionais definidos pela organização.

A Tabela 3.7 apresenta a escala detalhada de impacto para cada atributo do CID, segundo os parâmetros descritos anteriormente.

Por fim, a equação que define o *índice de criticidade do sistema* considerou a soma do impacto no

comprometimento do CID:

$$\text{Índice de Criticidade} = (C + I + D) \tag{3.1}$$

O índice de criticidade tem valores resultantes entre 3 e 15 (ver Tabela 3.6), o que permite a ordenação dos sistemas por esse índice, bem como agrupamentos de sistemas por baixa, média e alta criticidade.

Tabela 3.6: Níveis de Criticidade

| Faixa | Classificação | Características |
|---|---|---|
| 3 - 7 | Baixa Criticidade | Sistema com baixo impacto nas operações ou no atendimento ao cidadão |
| 8 - 11 | Média Criticidade | Sistema importante, mas com impacto moderado nas atividades-fim da organização |
| 12 - 15 | Alta Criticidade | Sistema vital para atividades-fim da organização |

Essa avaliação permite não apenas identificar o risco de impacto do CID na segurança do sistema, mas também identificar a criticidade do sistema no cumprimento da missão institucional.

#### 3.2.2.2 Validação com o Gestor de TI

Embora a metodologia permitisse uma avaliação técnica estruturada, a classificação final foi validada junto ao Gestor de TI, que pôde confirmar se a pontuação estava de acordo com a percepção institucional de risco e com os objetivos estratégicos da organização.

#### 3.2.2.3 Estratégia de Análise e Validação dos Dados

No que tange à estratégia de análise e validação dos dados, a pesquisa combinou métodos qualitativos e quantitativos com o objetivo de oferecer uma compreensão abrangente tanto dos impactos mensuráveis quanto das percepções institucionais relacionadas à implementação de medidas de segurança voltadas a servidores web. Além de orientar a análise dos dados, essa estratégia reforçou a validade do estudo, conforme a proposta de Runeson e Höst [139], ao empregar a triangulação metodológica — técnica que envolve a utilização de múltiplas fontes de evidência, como entrevistas, documentos institucionais, ferramentas de varredura e métricas definidas.

Na perspectiva quantitativa, a análise foi centrada na comparação entre os cenários anterior e posterior à aplicação do Modelo 3SW. Para isso, foram utilizadas métricas como a Taxa de Redução de Vulnerabilidades (TRV), obtida por meio de ferramentas de análise de segurança utilizadas pela organização (Tabela 3.4), além da avaliação da cobertura de mitigações com base no *framework* MITRE ATT&CK. A TRV mediu a variação no número de vulnerabilidades identificadas antes e depois da aplicação das medidas de segurança selecionadas, enquanto a análise de cobertura examinou até que ponto as técnicas de ataque previamente mapeadas foram mitigadas por meio da implementação das ações previstas no 3SW. Essa comparação buscou fornecer indícios objetivos da efetividade técnica do modelo em termos de mitigação de riscos.

No eixo qualitativo, foram analisadas as informações obtidas por meio das entrevistas com o Gestor

Tabela 3.7: Escala Detalhada de Impacto para CID

| Nível | Confidencialidade (C) | Integridade (I) | Disponibilidade (D) |
|---|---|---|---|
| **Muito Baixo (1)** | **Dados públicos não estruturados**: Informações sem valor estratégico ou regulatório (ex.: notícias antigas, material de divulgação) | **Alterações inconsequentes**: Dados que podem ser reconstruídos facilmente ou cuja modificação não gera impactos mensuráveis (ex.: notícias antigas) | **Serviço não essencial**: Sistema que pode permanecer offline por tempo indeterminado sem afetar operações (ex.: site de notícias arquivadas) |
| **Baixo (2)** | **Dados públicos estruturados**: Informações organizadas que, se expostas, causam apenas desconforto administrativo (ex.: catálogo de biblioteca, formulários genéricos) | **Alterações com retrabalho controlado**: Dados cuja modificação exige esforço limitado para correção (ex.: agendas internas, metadados de documentos) | **Serviço de apoio**: Sistema cuja indisponibilidade gera inconvenientes operacionais, mas que podem ser contornados por até 7 dias (ex.: sistema de reserva de salas) |
| **Médio (3)** | **Dados pessoais básicos**: Informações cadastrais que, se vazadas, podem gerar desconforto aos titulares, mas sem riscos significativos (ex.: cadastro de visitantes, e-mails institucionais) | **Alterações com impacto operacional**: Dados cuja modificação distorce processos internos ou tomadas de decisão (ex.: relatórios de gestão, indicadores de desempenho) | **Serviço importante**: Sistema essencial para operações rotineiras, com tolerância máxima de 48h de indisponibilidade (ex.: portal de serviços ao cidadão) |
| **Alto (4)** | **Dados sensíveis**: Informações cujo acesso não autorizado pode causar danos aos titulares ou à instituição (ex.: registros de saúde, localização de servidores em operação) | **Alterações com dano institucional**: Dados cuja modificação compromete a transparência, direitos ou gera perda de confiança pública (ex.: processos julgados, dados de licitações) | **Serviço essencial**: Sistema crítico para atendimento à população ou operações-fim, com tolerância máxima de 4h de indisponibilidade (ex.: sistema de pagamento de multas) |
| **Muito Alto (5)** | **Dados restritos/confidenciais**: Informações cujo comprometimento pode colocar vidas em risco ou causar danos estratégicos irreparáveis (ex.: dados de inteligência, investigações em andamento) | **Alterações catastróficas**: Dados cuja modificação inviabiliza a missão institucional ou causa danos irreversíveis (ex.: provas digitais, registros de operações) | **Serviço vital**: Sistema cuja indisponibilidade paralisa imediatamente as atividades-fim da organização (ex.: central de emergências, sistema de denúncias em tempo real) |

de TI e o Chefe de Segurança da Informação da organização, juntamente com os documentos institucionais relacionados às políticas de segurança da informação, planos de continuidade e diretrizes técnicas. As entrevistas foram conduzidas nos formatos estruturado e semiestruturado, de acordo com o perfil e os objetivos de cada interlocutor, e foram examinadas a partir de técnicas de codificação e categorização. A análise qualitativa buscou compreender as percepções dos profissionais sobre lacunas no modelo atual de segurança, os potenciais benefícios da proposta 3SW e sua adequação ao contexto organizacional, ampliando o alcance interpretativo da pesquisa além dos dados técnicos.

Além da análise em si, esta fase incorpora estratégias explícitas de validação dos resultados, baseadas nas quatro dimensões clássicas da validade científica em estudos de caso: validade de construto, validade interna, validade externa e confiabilidade.

A *validade de construto* foi assegurada por meio da formulação de critérios estruturados para a seleção (CS1, CS2, CS3) e priorização (CP1, CP2, CP3) das medidas de segurança, fundamentados em *frameworks* amplamente reconhecidos (CIS Controls v8.1, MITRE ATT&CK e CDM v2.0). Embora tais critérios envolvam certa dose de julgamento qualitativo, seu desenvolvimento foi pautado nas perguntas de pesquisa (QP1, QP2 e QP3) e sua aplicação ocorreu de forma sistemática, de modo a assegurar coerência entre os conceitos investigados e as decisões analíticas. A realização de entrevistas com profissionais diretamente envolvidos na gestão da segurança institucional reforça essa dimensão, permitindo validar os construtos com base na experiência prática dos participantes.

A *validade interna* foi sustentada pela comparação dos dados coletados em dois momentos distintos —– antes e depois da aplicação do modelo —–, pelo uso de indicadores mensuráveis e pelo controle de variáveis contextuais por meio da triangulação de dados. Essa triangulação contempla a integração de documentos institucionais, resultados técnicos e percepções extraídas das entrevistas, contribuindo para reduzir o risco de que os resultados sejam influenciados por fatores externos não controlados.

A *validade externa*, embora limitada pelo fato de tratar-se de um único estudo de caso, foi considerada a partir da possibilidade de replicação do modelo em organizações públicas com características semelhantes. A descrição detalhada dos critérios, procedimentos de aplicação e instrumentos utilizados (inclusive os roteiros de entrevista presentes nos apêndices) permite que a metodologia adotada seja adaptada a outros contextos. Assim, mais do que buscar generalização estatística, o estudo visa promover uma generalização analítica, segundo preconizado por Yin [136], em que os resultados são transferíveis para casos que compartilham elementos estruturais e operacionais similares ao da organização analisada.

Por fim, a *confiabilidade* foi garantida por meio da documentação sistemática de todas as etapas metodológicas, incluindo o registro dos critérios utilizados, a gravação e transcrição das entrevistas (mediante consentimento), e o uso de ferramentas amplamente reconhecidas na área de segurança da informação para a coleta dos dados técnicos. A padronização dos instrumentos de coleta e a descrição detalhada dos procedimentos metodológicos asseguram que o estudo possa ser reproduzido por outros pesquisadores em contextos comparáveis.

Com essa abordagem integrada, a Fase 4 buscou assegurar não apenas a qualidade técnica e interpretativa dos dados, mas também a coerência entre os objetivos da pesquisa, os métodos adotados e as conclusões que foram apresentadas. Essa consistência metodológica oferece uma base sólida para a avaliação da eficácia do Modelo 3SW na mitigação de vulnerabilidades em servidores web em contextos institucionais

reais.

## 3.3 CONSIDERAÇÕES ÉTICAS

A condução deste estudo seguiu princípios éticos fundamentais para garantir a integridade, a transparência e a proteção das informações envolvidas. Dado o caráter sensível dos dados analisados e a participação de profissionais da organização, medidas específicas foram adotadas para assegurar o respeito aos direitos dos envolvidos e à confidencialidade das informações.

### 3.3.1 Consentimento Informado

A participação no estudo foi voluntária e com o consentimento informado dos envolvidos, incluindo o Chefe de Segurança da Informação e o Gestor de TI da organização. Esses profissionais foram devidamente informados sobre os objetivos da pesquisa, os procedimentos adotados, os potenciais benefícios e os riscos, além do uso das informações coletadas. O consentimento foi documentado por meio da assinatura do termo de consentimento, garantindo a transparência do processo.

### 3.3.2 Confidencialidade e Proteção de Dados

Para preservar a confidencialidade das informações institucionais e individuais, foram adotadas medidas como:

1. **Anonimização de dados:** Nenhum nome ou detalhe sensível da Empresa ALFA deve ser mencionado na descrição de processos ou nos resultados da pesquisa relatados;
2. **Restrição de acesso:** Os dados coletados devem ser acessíveis apenas ao pesquisador responsável e aos indicados da Empresa ALFA que participam da pesquisa, bem como devem ser armazenados de forma segura e protegidos contra acessos não autorizados;
3. **Uso exclusivo para fins acadêmicos:** As informações obtidas devem ser utilizadas apenas no contexto desta pesquisa e não devem ser compartilhadas com terceiros sem autorização expressa da Empresa ALFA.

Os próximos capítulos apresentam os resultados desta pesquisa, detalhando o desenvolvimento, a validação e a análise do Modelo 3SW. O Capítulo 4 descreve a construção do 3SW, incluindo os critérios de seleção e priorização (3.1.1). O Capítulo 5 aplica o modelo na Empresa ALFA, utilizando estudo de caso e triangulação de dados (3.2.2.3). O Capítulo 6 avalia a eficácia do 3SW, comparando-o ao Modelo WAH (4.3), contribuindo para a segurança de servidores web na transformação digital [14].

# 4 DESENVOLVIMENTO DO MODELO 3SW

O principal resultado produzido neste mestrado é o Modelo 3SW (Subconjunto de Salvaguardas para Servidores Web), o qual é composto por um conjunto de medidas selecionadas para o contexto de servidores web. Estas medidas podem ser utilizadas para auxiliar na mitigação de ameaças de segurança, como ilustrado na Figura 4.1.

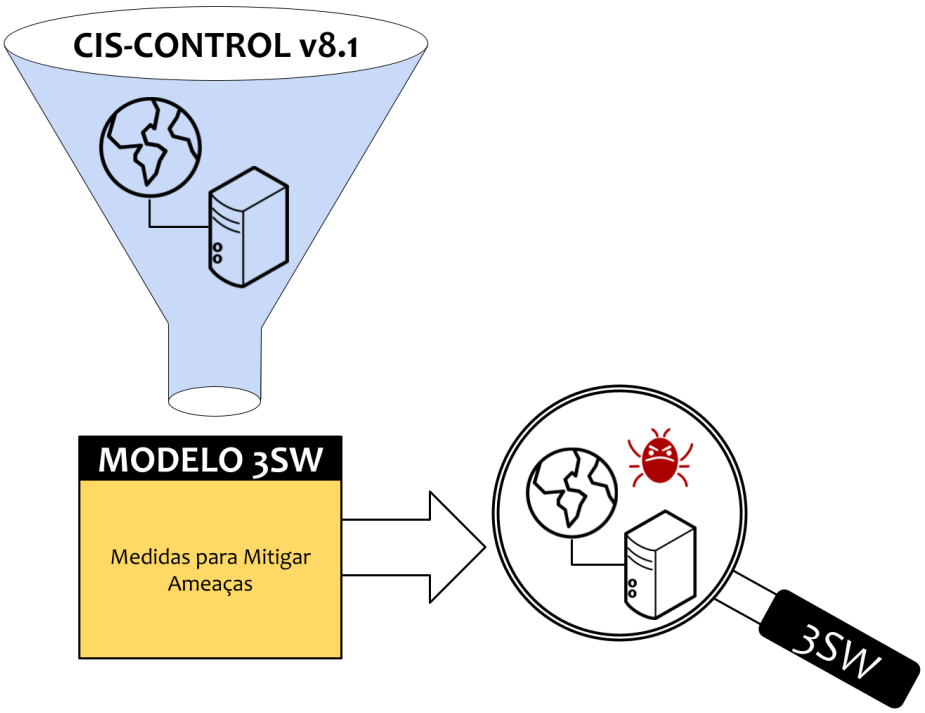


Figura 4.1: Modelo 3SW. Fonte: Própria

Além de facilitar a detecção de lacunas, o 3SW aborda um olhar direcionado para o ativo, uma ação que permite ao técnico atuar e desenhar soluções para as particularidades desse objeto. Portanto, para empresas, o Modelo 3SW pode integrar-se a processos de gestão de riscos e atuar na mitigação de lacunas de segurança da informação.

O desenvolvimento do Modelo 3SW foi realizado na terceira fase da pesquisa, conforme descrito no Capítulo 3. Para atingir essa finalidade, foi realizada a adaptação do CIS Controls v8.1 para o contexto de servidores web (OE1), empregando-se uma metodologia de análise de conteúdo estruturada em três etapas: pré-análise (planejamento da análise), exploração do material e tratamento dos resultados. A seguir, são apresentados os resultados da execução desta fase. Detalhes da análise desenvolvida estão disponíveis em [143].

## 4.1 SELEÇÃO DAS MEDIDAS DE SEGURANÇA DO 3SW (QP1)

A seleção das medidas de segurança a serem incluídas no 3SW foi guiada por três critérios (vide Seção 3.1.1). Esses critérios foram aplicados às 153 medidas definidas no *framework* CIS Controls v8.1, com o objetivo de selecionar aquelas mais adequadas para compor o 3SW. Uma medida só poderia ser incluída caso todos os critérios fossem atendidos —— ou seja, fosse relevante, individualizável e verificável para o contexto de servidores web. A Tabela 4.1 apresenta uma visão geral das medidas de segurança selecionadas com base nesses critérios.

Tabela 4.1: Resultado da seleção das medidas de segurança

| IDC | Descrição | QMS | %MS |
|---|---|---|---|
| C1 | Inventário e Controle de Ativos Corporativos | 1 | 20% (1/5) |
| C2 | Inventário e Controle de Ativos de Software | 7 | 100% (7/7) |
| C3 | Proteção de Dados | 10 | 71% (10/14) |
| C4 | Configuração Segura de Ativos Corporativos e Software | 8 | 67% (8/12) |
| C5 | Gestão de Contas | 6 | 100% (6/6) |
| C6 | Gestão do Controle de Acesso | 5 | 63% (5/8) |
| C7 | Gestão Contínua de Vulnerabilidades | 5 | 71% (5/7) |
| C8 | Gestão de Registros de Auditoria | 10 | 83% (10/12) |
| C9 | Proteções de E-mail e Navegador Web | 4 | 57% (4/7) |
| C10 | Defesas Contra Malware | 7 | 100% (7/7) |
| C11 | Recuperação de Dados | 5 | 100% (5/5) |
| C12 | Gestão da Infraestrutura de Rede | 4 | 50% (4/8) |
| C13 | Monitoramento e Defesa da Rede | 4 | 36% (4/11) |
| C14 | Conscientização sobre Segurança e Treinamento de Competências | 0 | 0% (0/9) |
| C15 | Gestão de Provedor de Serviços | 1 | 14% (1/7) |
| C16 | Segurança de Aplicações | 10 | 71% (10/14) |
| C17 | Gestão de Respostas a Incidentes | 1 | 11% (1/9) |
| C18 | Testes de Invasão | 5 | 100% (5/5) |
| **Total de Medidas de Segurança Selecionadas** | | **93** | **61% (93/153)** |

**Legenda:** IDC – Identificador do Controle; QMS – Quantidade de Medidas Selecionadas; %MS – Porcentagem de Medidas de Segurança (Total de medidas selecionadas / Total de Medidas Possíveis do Controle).

A Tabela 4.1 apresenta os 18 controles do CIS Controls v8.1, o número de medidas de segurança que atenderam aos critérios em cada um dos controles (QMS) e a porcentagem de medidas selecionadas em relação ao total de medidas de segurança disponíveis para cada controle (%MS).

Como resultado, das 153 medidas de segurança disponibilizadas no *framework* CIS v8.1, 93 (61%) atenderam aos três critérios de seleção (vide Seção 3.1.1). Em relação aos controles, que agrupam as medidas por temas específicos, destaca-se que, dos 18 controles, cinco tiveram todas as medidas identificadas como aplicáveis e verificáveis no servidor web, sendo completamente aderentes: C2, C5, C10, C11 e C18. Em contraste, apenas o controle C14, conscientização sobre segurança e treinamento de competências, não teve nenhuma medida que atendesse aos três critérios de seleção, refletindo a dificuldade de aplicabilidade dessas medidas no contexto de servidores web.

Os demais controles dividem-se em outros dois grupos: (1) controles com baixa aderência ao 3SW (entre 1% e 49%), no qual incluem-se os controles C1, C13, C15 e C17; e (2) controles com alta aderência

ao 3SW (entre 50% e 99%), em que estão presentes os controles C3, C4, C6, C7, C8, C9, C12 e C16. Esses agrupamentos propiciam uma orientação valiosa para as equipes técnicas, permitindo a priorização de áreas com maior impacto na mitigação de riscos cibernéticos por meio do 3SW.

## 4.2 CLASSIFICAÇÃO E PRIORIZAÇÃO DAS MEDIDAS DE SEGURANÇA DO 3SW (QP2)

A partir da análise das 93 medidas de segurança selecionadas para o 3SW, foi realizada a classificação com base em três critérios de priorização: ausência da necessidade de software ou atividades externas para implementação (CP1), dificuldade de implementação (CP2) e esforço de manutenção (CP3). Os critérios utilizaram as definições Baixo, Moderado e Alto presentes na Tabela 3.2. A consolidação desses resultados está disposta na Tabela 4.2, que oferece uma visão abrangente do esforço requerido para aplicação e sustentação das medidas no contexto dos servidores web.

Tabela 4.2: Consolidação da análise dos critérios de priorização sobre as medidas do 3SW

| **Viabilidade de Implementação (CP1)** | **Esforço de Implementação (CP2)** | **Esforço de Manutenção (CP3)** | | | **Total CP2 (%)** |
|---|---|---|---|---|---|
| | | *Baixo* | *Moderado* | *Alto* | |
| Sim - 53 (57%) | Baixo | 11 | 5 | 0 | 16 (30%) |
| | Moderado | 12 | 21 | 0 | 33 (62%) |
| | Alto | 0 | 3 | 1 | 4 (8%) |
| | **Total CP3** (%) | 23 (43%) | 29 (55%) | 1 (2%) | |
| Não - 40 (43%) | Baixo | 6 | 1 | 0 | 7 (17%) |
| | Moderado | 7 | 14 | 2 | 23 (58%) |
| | Alto | 0 | 5 | 5 | 10 (25%) |
| | **Total CP3** (%) | 13 (33%) | 20 (50%) | 7 (17%) | |
| | | | | **Total de Medidas** | **93** |

**Legenda:** CP1 – A medida pode ser implementada e gerida diretamente no servidor web, sem depender de recursos, softwares ou serviços externos contínuos? CP2 – Qual o esforço para implementar a medida no servidor web? CP3 – Qual o esforço para manter a medida aplicada e atualizada no servidor web?

Das 93 medidas analisadas, 53 (57%) podem ser implementadas e geridas diretamente no servidor web, sem a necessidade de recursos externos, enquanto 40 (43%) dependem de algum tipo de software ou atividade externa. Isso indica que a maioria das medidas pode ser gerida no próprio servidor web, facilitando a implementação, mas uma parcela significativa ainda requer integração com componentes externos, o que pode aumentar a complexidade de sua aplicação e manutenção.

Em relação ao esforço de implementação (CP2) para as medidas que podem ser geridas diretamente no servidor web (“Sim” para CP1), 62% delas exigem um esforço moderado de implementação, 30% apresentam um esforço baixo, e 8% possuem um esforço alto. Esses números demonstram que, mesmo entre as medidas que não dependem de recursos externos, a implementação moderada é predominante.

Por outro lado, entre as medidas que dependem de recursos externos (“Não” para CP1), 58% apresentam um esforço moderado para implementação, 25% requerem um esforço alto, e 17% um esforço baixo. Esse padrão sugere que, embora a maioria das medidas externas também exija um esforço moderado, o esforço alto é mais frequente nessa categoria em comparação com as medidas geridas no próprio servidor

web.

Ao analisar o esforço para manter as medidas após a implementação (CP3), observa-se uma distribuição distinta entre as categorias de CP1. Para as medidas que não dependem de recursos externos, 55% exigem moderado esforço de manutenção, 43% baixo, e 2% alto. Já para as medidas que necessitam de recursos externos, 50% requerem esforço moderado, 33% baixo, e 17% esforço alto. Isso evidencia que medidas aplicadas diretamente no servidor web tendem a ser menos complexas em termos de manutenção, com uma prevalência de esforço moderado ou baixo, o que contribui para uma gestão mais eficiente a longo prazo. Por outro lado, as medidas que utilizam recursos externos, embora possam ser mais gerenciáveis, apresentam um maior esforço de manutenção, o que pode exigir mais tempo e recursos da equipe técnica.

A priorização das medidas que podem ser implementadas diretamente no servidor web tem como objetivo a otimização do uso de recursos e a liberação de tempo para a equipe se concentrar em outras estratégias de mitigação de riscos cibernéticos.

## 4.3 COMPARAÇÃO DO 3SW COM WEB APPLICATION HACKING (QP3)

O último passo da construção do 3SW consistiu em compará-lo ao modelo que mais se aproxima de sua proposta, o Web Application Hacking (WAH), ambos baseados no CIS Controls v8. Essa comparação buscou identificar semelhanças e diferenças na quantidade e distribuição das medidas de segurança selecionadas em cada modelo.

No contexto geral, de acordo com os dados expostos na Tabela 4.3, o 3SW abrange 93 medidas (61% das 153 do CIS Controls v8.1) e o WAH, 90 medidas (59%). Para facilitar a visualização dessa distribuição, elaborou-se o mapa de calor apresentado na Tabela 4.4, que evidencia a concentração de medidas por controle em cada modelo. Quanto maior a quantidade de medidas, mais escura é a tonalidade do vermelho.

No tocante ao total de medidas, 61 medidas são comuns aos dois modelos (40% do total), enquanto 32 são exclusivas do 3SW (21%) e 29 do WAH (19%), resultando em uma cobertura combinada de 122 medidas (80%).

Tabela 4.3: Distribuição das medidas de segurança entre os modelos 3SW e WAH em relação ao CIS Controls v8.1

| **Categoria** | **Modelos** | | **% sobre as 153** | |
|---|---|---|---|---|
| | **3SW** | **WAH** | **3SW** | **WAH** |
| Total de medidas no modelo | 93 | 90 | 61% | 59% |
| Medidas comuns aos dois modelos | 61 | | 40% | |
| Medidas exclusivas | 32 | 29 | 21% | 19% |
| Cobertura total combinada dos modelos | 122 (61+32+29) | | 80% | |

**Nota:** Os valores percentuais foram arredondados para o número inteiro mais próximo com base no total de 153 medidas de segurança descritas no CIS Controls v8.1.

A Tabela 4.5 aborda a Diferença Percentual (DP) que cada modelo possui, a partir de medidas exclusivas distribuídas por cada um dos 18 controles.

Tabela 4.4: Mapa de Calor das Medidas Totais nos modelos 3SW e WAH por Controle

| IDC | TM-3SW | TM-WAH |
|---|---|---|
| C1 | 1 | 0 |
| C2 | 7 | 7 |
| C3 | 10 | 7 |
| C4 | 8 | 8 |
| C5 | 6 | 5 |
| C6 | 5 | 6 |
| C7 | 5 | 7 |
| C8 | 10 | 5 |
| C9 | 4 | 5 |
| C10 | 7 | 5 |
| C11 | 5 | 2 |
| C12 | 4 | 4 |
| C13 | 4 | 7 |
| C14 | 0 | 6 |
| C15 | 1 | 1 |
| C16 | 10 | 11 |
| C17 | 1 | 0 |
| C18 | 5 | 4 |
| **Totais** | **93** | **90** |

**Legenda: IDC**: Identificação do Controle; **TM-3SW**: Total de Medidas no Modelo 3SW; **TM-WAH**: Total de Medidas no Modelo WAH. *Escala de cores*: branco (0 medidas), vermelho claro (1–2 medidas), vermelho médio (3–6 medidas), vermelho escuro (7–11 medidas). Células escuras (vermelho escuro) usam fonte branca para legibilidade.

A análise da DP entre os modelos permite compreender quão diferentes são o 3SW e o WAH. Nesse contexto, DP igual a zero indica que ambos os modelos cobrem igualmente o contexto de servidores web, estes casos estão marcados de amarelo na Tabela 4.5. Enquanto DP negativo (marcado de vermelho), indica maior cobertura do WAH ao controle observado e DP positivo (marcado de verde) aponta para maior cobertura do 3SW. Apenas quatro controles apresentam a mesma cobertura em ambos os modelos; em cinco, o WAH obteve melhor cobertura, e nos demais nove controles, o 3SW possui maior quantidade de medidas. Conclui-se, portanto, que o Modelo 3SW possui uma distribuição mais ampla de medidas de segurança entre os controles da metodologia CIS Controls.

Também foi realizada uma análise dos controles com variações maior que 25% e menor que –25%, mostrada na Tabela 4.6.

A análise comparativa destaca que o impacto prático do 3SW se dá pela priorização de medidas voltadas diretamente à proteção do servidor web, garantindo maior controle sobre aspectos críticos como integridade dos registros de auditoria (C8), defesas contra malwares (C10) e recuperação de dados (C11). Na prática, isso significa que a aplicação do 3SW pode fortalecer a resposta a incidentes e a resiliência operacional do servidor.

Em contrapartida, o WAH apresenta um escopo mais amplo, incluindo medidas relacionadas aos processos de gestão contínua de vulnerabilidades (C7), monitoramento e defesa da rede (C13) e treinamento de usuários (C14), que possuem um impacto mais abrangente na postura de segurança da organização,

Tabela 4.5: Medidas de Segurança únicas em 3SW e WAH

| IDC | QTD 3SW | QTD WAH | Dif% | IDC | QTD 3SW | QTD WAH | Dif% |
|---|---|---|---|---|---|---|---|
| C1 | 1 | 0 | 20% (1/5) | C10 | 2 | 0 | 29% (2/7) |
| C2 | 0 | 0 | 0% (0/7) | C11 | 3 | 0 | 60% (3/5) |
| C3 | 4 | 1 | 21% (3/14) | C12 | 2 | 2 | 0% (0/8) |
| C4 | 2 | 2 | 0% (0/12) | C13 | 1 | 4 | -27% (3/11) |
| C5 | 1 | 0 | 17% (1/6) | C14 | 0 | 6 | -67% (6/9) |
| C6 | 2 | 3 | -13% (1/8) | C15 | 0 | 0 | 0% (0/7) |
| C7 | 0 | 2 | -29% (2/7) | C16 | 3 | 0 | 21% (3/14) |
| C8 | 7 | 2 | 42% (5/12) | C17 | 1 | 0 | 11% (1/9) |
| C9 | 2 | 3 | -14% (1/7) | C18 | 1 | 0 | 20% (1/5) |

**Legenda:** QTD 3SW – Quantidade de medidas apenas no 3SW; QTD WAH – Quantidade de medidas apenas no WAH; Dif% – Diferença Percentual: (Total de medidas exclusivas do 3SW – Total de medidas exclusivas do WAH) / Total de Medidas do Controle.

Tabela 4.6: Análise dos controles com diferença percentual > 25% e < -25%.

| Controle | Dif% | Destaque comparativo |
|---|---|---|
| C7 - Gestão contínua de vulnerabilidades | -29% | As medidas tratam de estabelecer processos, fogem do escopo de aplicabilidade no contexto de servidores web. |
| C8 - Gestão de registros de auditoria | 42% | Reforça a ênfase na gestão e monitoramento de registros de auditoria, essencial para a visibilidade e a resposta a incidentes em servidores web. |
| C10 - Defesas contra malware | 29% | Crucial para proteger servidores web contra ameaças externas. |
| C11 - Recuperação de dados | 60% | Preocupação com a recuperação de dados, alinhando-se à necessidade crítica de resiliência e continuidade operacional em servidores web. |
| C13 - Monitoramento e defesa da Rede | -27% | Apresenta medidas cuja verificação encontra-se em componentes periféricos ao servidor web. |
| C14 - Conscientização sobre segurança e treinamento de competências | -67% | Conforme tratados em 4.1, as medidas não são diretamente verificáveis em servidores web. |

mas podem ter aplicabilidade direta reduzida na administração técnica dos servidores web. Essa distinção sugere que, **enquanto o WAH busca um fortalecimento global da segurança da aplicação e do ambiente ao redor, o 3SW foca na implementação de proteções diretamente sobre o ativo, facilitando sua aplicação em cenários onde a segurança do servidor web é a prioridade**.

Ainda como parte da análise comparativa, foi avaliada a aderência de cada modelo às mitigações do MITRE ATT&CK. O CIS Controls v8.1 abrange 39 das 42 mitigações catalogadas pelo MITRE ATT&CK v8.2, das quais o 3SW cobre 36 (92%) e o WAH, 38 (97%). As mitigações ausentes no 3SW, como M1013 (Guia para Desenvolvedores de Aplicativos) e M1017 (Treinamento do Usuário), estão relacionadas ao controle C14, Conscientização sobre Segurança e Treinamento de Competências. Conforme discutido na Seção 4.1, as medidas desse controle não se enquadram nos critérios de seleção deste estudo (CS1, CS2 e CS3) para servidores web. Essa diferença ilustra que, **enquanto o WAH incorpora medidas que visam mudança de cultura e treinamento de usuários, o 3SW prioriza a proteção dos ativos mais expostos a ataques cibernéticos**.

Os resultados reforçam que, embora ambos os modelos compartilhem o objetivo de mitigar riscos cibernéticos, suas abordagens divergem para atender aos desafios específicos de seus respectivos ambientes. O Modelo 3SW, ao concentrar-se em medidas mais aplicáveis a servidores web, promove a adaptação e simplificação das recomendações do CIS Controls v8.1, com ênfase em aspectos como recuperação de dados [144], gestão de registros de auditoria [126] e defesa contra malwares [118]. Isso evidencia a relevância das medidas selecionadas frente às demandas típicas desse tipo de ativo.

Ademais, por ser direcionado especificamente a servidores web, o 3SW mostra-se especialmente útil para a proteção de sistemas com alta exposição a ameaças cibernéticas, ao oferecer uma abordagem prática e orientada ao ativo, servindo também como complemento a estratégias de segurança mais amplas, quando necessário.

## 4.4 RESUMO DO CAPÍTULO

Este capítulo descreve o processo de construção do Modelo 3SW, abordando a seleção, a classificação e a priorização de medidas de segurança do CIS Controls v8.1, além de sua comparação com o Modelo Web Application Hacking (WAH). Inicialmente, foram selecionadas 93 (61%) das 153 medidas do CIS Controls v8.1, com base em três critérios: relevância, individualização e verificabilidade no contexto de servidores web (Seção 4.1). Cinco controles (C2, C5, C10, C11 e C18) tiveram todas as medidas selecionadas, enquanto o controle C14 não apresentou medidas aplicáveis, evidenciando a dificuldade de aplicação de treinamentos no contexto de servidores web (Tabela 4.1).

Na etapa de classificação e priorização (Seção 4.2), as 93 medidas foram analisadas com base em três critérios: ausência de dependência de recursos externos (CP1), esforço de implementação (CP2) e esforço de manutenção (CP3). Resultados indicam que 57% das medidas podem ser implementadas diretamente no servidor web, com predominância de esforço moderado (62%) para implementação e manutenção (55%) nessas medidas, enquanto as dependentes de recursos externos apresentam maior esforço de manutenção (17% alto, ver Tabela 4.2).

A comparação com o WAH (Seção 4.3) revelou que, das 93 medidas do 3SW e 90 do WAH, 61 são comuns, com 32 exclusivas do 3SW e 29 do WAH. O 3SW destaca-se em controles como C8 (gestão de registros de auditoria), C10 (defesas contra malware) e C11 (recuperação de dados), com maior cobertura (Tabela 4.5), enquanto o WAH abrange mais medidas em C7, C13 e C14, focando em processos organizacionais e treinamento (Tabela 4.6). Em relação às mitigações do MITRE ATT&CK v8.2, o 3SW cobre 36 (92%) e o WAH 38 (97%), com ausências no 3SW ligadas ao controle C14 [144, 126, 118]. Assim, o 3SW prioriza a proteção direta de servidores web, enquanto o WAH adota uma abordagem mais ampla, complementando estratégias organizacionais.

# 5 VALIDAÇÃO DO MODELO 3SW

Este capítulo apresenta a validação do Modelo 3SW, desenvolvido para adaptar as medidas do CIS Controls v8.1 ao contexto de servidores web, com foco em sua aplicabilidade, efetividade e validade (OE3). A estrutura do capítulo acompanha as etapas do processo de validação, iniciando com o diagnóstico institucional da Empresa ALFA (Seção 5.1), seguido pela seleção dos sistemas a serem avaliados (Seção 5.2). Logo após, são apresentados os casos de aplicação prática e realizado o registro pré-implementação dos modelos (Seção 5.3). Essa organização busca alinhar o processo de validação aos objetivos específicos da pesquisa (OE2 e OE3), partindo da compreensão do ambiente organizacional até o registro do estado antes da implementação dos modelos.

## 5.1 DIAGNÓSTICO: ANÁLISE DOCUMENTAL E ENTREVISTA COM CHEFE DE SEGURANÇA DA INFORMAÇÃO

A aplicação do Modelo 3SW em ambiente real teve início com a necessidade de compreender como a instituição lida com os temas de segurança da informação e de proteção de sistemas nos seus processos institucionais. Para alcançar esse objetivo, foi realizada a análise dos documentos relacionados ao Programa de Privacidade e Segurança da Informação (PPSI) da organização e dos documentos relacionados à Gestão de Riscos Organizacionais. Ademais, foi conduzida uma entrevista com o Chefe de Segurança da Informação. Detalhes de como e quais documentos foram analisados são apresentados na Seção 3.2 juntamente com os detalhes de como a entrevista foi conduzida. O conjunto de perguntas utilizadas na entrevista pode ser visto no Apêndice B.

### 5.1.1 Análise dos documentos do PPSI

A análise dos documentos revelou que a organização desenvolvia iniciativas relacionadas ao CIS Controls desde 2022, antes da criação formal do PPSI, que data de 28 de março de 2023 [66]. Por outro lado, a exigência oficial de implementação das medidas previstas no Guia do Framework de Privacidade e Segurança da Informação teve início apenas em 2 de outubro de 2023 [79], cerca de sete meses após a publicação da portaria que instituiu o programa. Esses dados indicam que a Empresa ALFA, por meio de seus colaboradores, adotava o CIS Controls na qualidade de referência mesmo antes de sua formalização como diretriz institucional. Essa percepção foi confirmada na entrevista com o Chefe de Segurança da Informação (ver 5.1.3).

Dado que o 3SW é um modelo que também utiliza o CIS Controls como base de sua análise em servidores web, o levantamento das ações realizadas nesse programa torna-se importante para mapear possíveis implementações de medidas de segurança de forma paralela, o que poderia impactar a análise final da aplicação do 3SW e do WAH em curso.

Diante da análise documental, foi observado que a implantação do PPSI dá-se por agrupamentos de medidas em ciclos de seis em seis meses, com exceção do Ciclo 1, com três meses. A Tabela 5.1 exibe a distribuição dessas medidas ao longo dos ciclos e quais medidas do 3SW e do WAH poderiam ser afetadas.

Tabela 5.1: Interseção das medidas do PPSI com os modelos 3SW e WAH

| **Ciclo** | **Prazo** | **Medidas** | | | |
|---|---|---|---|---|---|
| | | **Total** | **PPSI** | **3SW** | **WAH** |
| 1 | 02/10/2023 a 31/01/2024 | 19 | 1.1, 1.2, 2.1, 2.2, 2.3, 6.1, 6.2, 6.3, 6.5, 7.7, 8.1, 8.3, 11.1, 11.2, 11.4, 11.5, 17.1, 17.2, 17.3 | 1.1, 2.1, 2.2, 2.3, 6.3, 6.5, 7.7, 11.1, 11.2, 11.4, 11.5, 17.2 | 2.1, 2.2, 2.3, 6.1, 6.2, 6.3, 6.5, 7.7, 8.1, 8.3, 11.4 |
| 2 | 01/01/2024 a 30/06/2024 | 8 | 3.1, 3.2, 8.4, 8.10, 10.1, 10.2, 14.1, 15.1 | 3.2, 8.4, 8.10, 10.1, 10.2 | 3.1, 3.2, 8.4, 8.10, 10.1, 10.2, 14.1 |
| 3 | 01/07/2024 a 31/12/2024 | 13 | 2.4, 3.3, 3.10, 3.14, 6.4, 7.3, 8.2, 8.6, 11.3, 12.4, 14.8, 16.8, 17.4 | 2.4, 3.3, 3.10, 3.14, 7.3, 8.2, 8.6, 11.3, 16.8 | 2.4, 3.3, 3.10, 6.4, 7.3, 8.2, 8.6, 11.3, 16.8 |
| 4 | 01/01/2025 a 30/06/2025 | 17 | 4.1, 4.2, 4.3, 4.4, 4.5, 4.7, 5.1, 5.2, 5.3, 5.4, 7.2, 9.1, 9.2, 10.3, 14.2, 14.4, 14.5 | 4.1, 4.3, 4.4, 4.7, 5.1, 5.2, 5.3, 5.4, 10.3 | 4.1, 4.2, 4.4, 4.5, 4.7, 5.1, 5.2, 5.3, 5.4, 7.2, 9.1, 10.3, 14.2, 14.4 |

Para o Estudo de Caso, que teve iniciada a implementação de suas medidas no início do Ciclo 4, os sistemas escolhidos foram clonados e isolados. Como ação seguinte, foi registrado o estado, naquele momento, da implementação das medidas de segurança dos modelos 3SW e WAH, de modo que ao final houvesse a medição de progressão em ambos os modelos, ver Tabela 5.5.

### 5.1.2 Análise dos documentos da Gestão de Riscos da Organização

A análise documental, além de permitir compreender o contexto da organização em relação à segurança da informação e à proteção de dados, apoiou a identificação de como o Modelo 3SW poderia ser incorporado aos processos internos da Empresa ALFA. Neste contexto, o principal instrumento encontrado foi a gestão de riscos utilizada como ferramenta para a proteção dos ativos de TIC.

Esse processo adotado para gestão de riscos baseia-se nas normas ABNT ISO/IEC 31000 [87] e COSO ERM [86], ilustrado na Figura 5.1, permitindo identificar, analisar e tratar riscos de forma sistemática. Na Empresa ALFA, esse processo foi organizado em sete etapas 5.1.2:

1. **Estabelecimento do Contexto:** envolve a definição do escopo de ativos, compreensão sobre o ambiente organizacional, mapeamento de normas e políticas aplicadas ao escopo identificado, bem como conhecer os principais fatores podem impactar o alcance dos objetivos institucionais;

2. **Identificação dos Riscos:** essa etapa tem por finalidade identificar os ativos de TIC, mapear as causas e as vulnerabilidades associadas a cada ativo de TIC, assim como registrar as consequências de cada uma delas. A etapa utiliza na qualidade de principal componente ferramentas de varredura e análise de vulnerabilidades.

3. **Análise de Riscos:** nessa etapa são calculados os níveis dos riscos identificados pelas ferramentas de análise;

4. **Avaliação de Riscos:** compara-se os resultados da análise com os níveis de riscos para determinar se o risco da ocorrência do evento é aceitável;

5. **Priorização de Riscos:** compreende a seleção dos ativos de TIC para aplicar correções e quais riscos terão prioridade (criticidade e urgência) na implementação das medidas de tratamento ou definição de respostas aos riscos;

6. **Definição de Respostas aos Riscos:** engloba a proposição de uma ou mais alternativas para evitar, reduzir, compartilhar ou aceitar os riscos; e

7. **Comunicação e Monitoramento:** a comunicação ocorre pelo envio do relatório aos responsáveis pelo ativo de TIC. O monitoramento é uma atividade contínua, de forma a obter informações adicionais, detectar mudanças, analisar mudanças e aprender com elas, assim como acompanhar a evolução dos níveis de riscos e as respostas aos riscos.

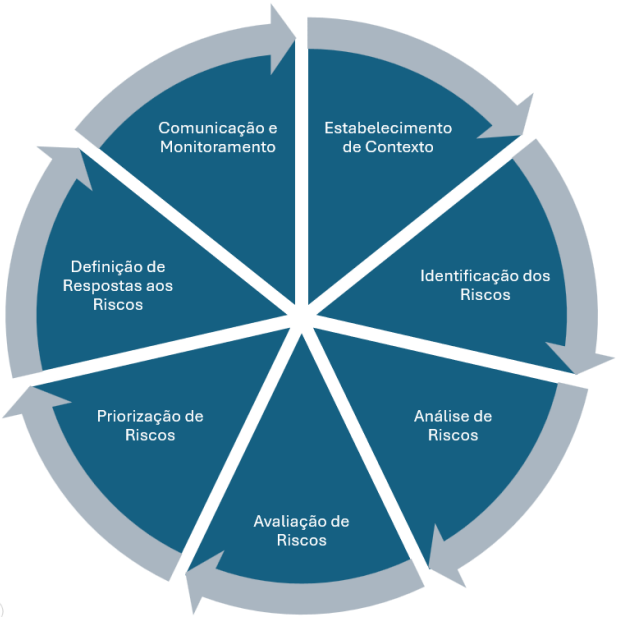


Figura 5.1: Processo de Gestão de Riscos da Empresa ALFA. Fonte: Adaptado de Documento Interno da Empresa ALFA

Após a compreensão do processo de gestão de riscos utilizado pela Empresa ALFA, buscou-se identificar como o 3SW poderia ser integrado de maneira prática e estratégica a esse ciclo. Essa adaptação ao processo de gestão de riscos da organização considerou dois critérios principais:

1. **Alinhamento aos objetivos do estudo:** aplicação do 3SW para avaliar sua efetividade como resposta aos riscos identificados nos servidores web; e

2. **Viabilidade operacional:** identificação das etapas do processo onde o 3SW agrega valor sem sobrepor atividades consolidadas.

Com base nesses critérios, o 3SW foi incorporado a partir da **Etapa 6 (Definição de Respostas aos Riscos)**, sendo direcionado apenas aos sistemas selecionados pelo Gestor de TI. A Tabela 5.2 apresenta a correspondência entre as atividades previstas no 3SW e as etapas da metodologia de gestão de riscos da Empresa ALFA.

Tabela 5.2: Correspondência entre atividades do 3SW e etapas do processo de gestão de riscos da ALFA

| **Atividades do 3SW** | **Etapas da Gestão de Riscos da ALFA** |
|---|---|
| Aplicação do 3SW para identificar lacunas e riscos nos sistemas selecionados | Etapa 6 – Definição de Respostas aos Riscos |
| Elaboração de cronograma para implantação das medidas não implementadas | Etapa 6 – Definição de Respostas aos Riscos |
| Definição da forma de implementação das medidas de segurança | Etapa 6 – Definição de Respostas aos Riscos |
| Avaliação periódica da efetividade das medidas adotadas | Etapa 7 – Comunicação e Monitoramento |

Concluída a adaptação do Modelo 3SW ao processo de gestão de riscos de TIC da organização ALFA, iniciou-se a etapa de entrevistas. A entrevista com o Chefe de Segurança da Informação teve como objetivo identificar lacunas no PPSI, avaliar o estado atual da segurança institucional e coletar impressões sobre a proposta do Modelo 3SW. Detalhes dessa entrevista são apresentados a seguir.

### 5.1.3 Percepções do Chefe de Segurança da Informação sobre o Modelo 3SW e o PPSI

Esta seção apresenta as percepções do Chefe de Segurança da Informação da Empresa ALFA, obtidas por meio de entrevista semiestruturada (ver Perguntas na Tabela B.2), com foco na avaliação da maturidade institucional, aplicação do PPSI, lacunas de proteção em sistemas críticos e expectativas em relação ao Modelo 3SW. As respostas complementam a validação do modelo proposto, oferecendo uma perspectiva institucional sobre sua aplicabilidade e seu valor prático.

**Experiência e o PPSI**. O entrevistado atua há três anos na Empresa ALFA e possui 18 anos de experiência na área de segurança da informação. Segundo ele, o *framework* CIS Controls v8 era de conhecimento do seu setor e havia atividades iniciais de adoção na organização antes da implementação do PPSI. No entanto, com a chegada desse programa, sua adoção passou a ser obrigatória e sistematizada por meio de ciclos com prazos definidos.

As medidas de cada um dos ciclos do PPSI são encaminhadas a instâncias superiores dentro da Empresa ALFA e distribuídas entre os setores responsáveis, que devem registrar sua evolução segundo os prazos estabelecidos. Essa estrutura tem contribuído para que áreas menos envolvidas com segurança comprometam-se com as ações propostas, embora os resultados práticos ainda estejam aquém do esperado. Destaca-se a importância do apoio institucional, uma vez que o direcionamento de instâncias superiores reforça e legitima demandas anteriormente levantadas pela equipe de segurança. Entre os principais desafios enfrentados, foi destacada a dificuldade de engajar as áreas que não eram de segurança e promover uma cultura de corresponsabilidade em segurança da informação. O nível de adesão da organização ao componente de segurança do PPSI foi classificado como Moderado (entre 50% e 84%), ou Alto, caso os níveis de escolha abrangessem cinco categorias. Na sua visão, há sempre espaço para melhoria.

**Limitações do PPSI para Sistemas Críticos**. Embora o PPSI e o CIS Controls v8 forneçam diretrizes importantes, o entrevistado considera que seu foco é genérico, não atendendo de forma suficiente às necessidades específicas dos sistemas críticos. Assim, esses *frameworks* atuam como norteadores ou orientações gerais, mas carecem de direcionamentos técnicos mais específicos. Em particular, são limitados na abordagem de sistemas expostos à Internet ou que exijam proteções aprofundadas em nível de aplicação.

Com relação à proteção atual dos sistemas críticos, o entrevistado avalia que há uma perspectiva de melhoria, mas que avanços mais significativos exigem tempo e estabelecimento de processos. Os riscos mais relevantes mencionados incluem ataques de negação de serviço, comprometimento da imagem institucional, exploração de vulnerabilidades e perda de licenciamento de software.

**Recursos, Capacitação e Maturidade Institucional**. O entrevistado afirmou que, excetuando os momentos de restrição orçamentária, como os vividos, principalmente, nos últimos dois anos, a organização dispõe de recursos humanos e financeiros suficientes para implementar a maioria das medidas do PPSI e os controles do CIS Controls v8. Entretanto, destacou que o principal desafio reside na qualificação dos profissionais, especialmente nas áreas de governança de TI. A equipe de segurança é considerada capacitada e compreende bem o funcionamento dos controles propostos.

Apesar disso, há lacunas na formação de outros setores envolvidos na implementação das medidas. Embora a organização forneça acesso a plataformas de capacitação, não há treinamentos específicos voltados para o PPSI. A necessidade contínua de capacitação foi apontada como um fator crucial, dado o dinamismo da área de tecnologia.

Em termos de maturidade institucional, a organização foi classificada como tendo um nível moderado, com potencial de evolução para níveis mais elevados. Entre os indicadores utilizados para mensurar essa maturidade, o entrevistado citou a proporção de processos automatizados, a taxa de incidentes tratados e a frequência de capacitações oferecidas.

**Incidentes de Segurança e a Efetividade do PPSI**. De acordo com o entrevistado, a organização não enfrentou incidentes de segurança cibernética relevantes em sistemas críticos até o momento da entrevista. Consequentemente, não houve necessidade de aplicar os processos de resposta estabelecidos, tampouco foi possível avaliar diretamente a efetividade do PPSI e dos controles do CIS Controls v8 em situações de crise.

Mesmo assim, foi reconhecido que, por serem medidas genéricas, esses *frameworks* podem oferecer diretrizes iniciais em contextos de incidentes. O entrevistado, entretanto, destacou que modelos mais especializados, a exemplo do NIST SP 800-61r3 [145], são mais apropriados para lidar com respostas a incidentes de forma estruturada e eficiente.

**Avaliação do Modelo 3SW**. O entrevistado avaliou de forma positiva a proposta do Modelo 3SW, reconhecendo seu potencial de aprofundar as diretrizes do CIS Controls para contextos mais específicos, como servidores web e sistemas expostos à Internet. Considerou que o modelo atua na qualidade de uma "segunda camada" de proteção, ao detalhar ações específicas dentro de um escopo mais restrito e técnico.

Entre os benefícios identificados, estão a possibilidade de desenvolver medidas mais direcionadas às vulnerabilidades de ambientes específicos, o que aumenta o potencial de mitigação de riscos reais. Como desafio, foi mencionada a complexidade de expandir essa abordagem para múltiplos tipos de ambientes, o

que exigiria adaptações.

Para implementação do Modelo 3SW, recomendou-se iniciar com a identificação dos ativos mais relevantes e aplicar as medidas de acordo com as tecnologias e contextos de cada sistema. Quanto às métricas para avaliar sua eficácia, sugeriu-se monitorar a redução de eventos de segurança, a exemplo de ataques de força bruta, bem como comparações baseadas em análises antes e depois da aplicação das medidas.

**Relevância do Estudo e Alinhamento com os Problemas da Instituição**. O entrevistado considerou que o estudo está alinhado com as necessidades institucionais, especialmente no que diz respeito à proteção de sistemas expostos à Internet. Foi destacado que um dos principais problemas da organização é a ausência de processos que sustentem a operação e a proteção de sistemas críticos de forma sistemática.

Nesse sentido, o Modelo 3SW pode contribuir para preencher essa lacuna, desde que demonstre resultados concretos, como a redução de exposição a riscos. A expectativa é que, em curto prazo, sejam aplicadas as medidas selecionadas; em médio prazo, seja possível documentar sua aplicação por ambiente; e, em longo prazo, utilizar os resultados para promover ciclos de melhoria contínua, por meio de um processo estruturado de avaliação e ajuste (PDCA — *Plan-Do-Check-Act* — Planejar-Fazer-Verificar-Agir).

Por fim, foi reforçada a importância de tratar a segurança cibernética em nível estratégico, e não apenas operacional, visando garantir a sustentabilidade das ações implementadas.

## 5.2 SELEÇÃO DE SISTEMAS

A seleção dos sistemas utilizados no estudo de caso foi realizada por meio de entrevista com o Gestor de TI, utilizando a metodologia de classificação de sistemas externos descrita na Seção 3.2.2.1. Essa metodologia foi guiada pelas perguntas da Tabela B.1 e avaliou o tipo de dado processado (pessoais, sensíveis, restritos ou públicos), bem como os impactos potenciais para a Empresa ALFA em caso de comprometimento ou indisponibilidade.

Importante ressaltar que, por motivos de confidencialidade, os nomes e quantidades dos sistemas analisados não podem ser divulgados. No entanto, os resultados são mostrados em termos percentuais. A Tabela 5.3 resume a distribuição final dos sistemas conforme a criticidade, assim como a taxa de reclassificação feita pelo Gestor de TI.

Durante a entrevista, o Gestor de TI foi convidado a avaliar a classificação automática proposta pelo modelo. Quando discordava da criticidade atribuída, ele pôde realizar ajustes, justificando cada reclassificação. Os motivos mais recorrentes envolviam a alta demanda de uso por públicos externos ou a relevância crítica dos sistemas para o fornecimento de dados essenciais — fatores não contemplados diretamente pelo modelo de avaliação desta dissertação.

Com base nessas observações, analisou-se o impacto de uma possível reconfiguração nas faixas de classificação de criticidade. A Tabela 5.4 compara as faixas originais e as ajustadas de pontuação. Um simples ajuste de 1 ponto nos limites das faixas poderia reduzir o índice de erro da classificação automática de 21% para 13%.

Apesar da melhoria estatística com esse pequeno ajuste, a participação ativa do Gestor de TI permanece

Tabela 5.3: Distribuição percentual da criticidade dos sistemas e reclassificações realizadas

| Nível de Criticidade | Classificação Automática (%) | Classificação Final (%) |
|---|---|---|
| Baixa | 21% | 17% |
| Média | 38% | 25% |
| Alta | 41% | 58% |
| **Total de reclassificações** | 21% dos sistemas foram ajustados pelo Gestor de TI | |

Tabela 5.4: Comparativo entre as faixas originais e ajustadas de classificação de criticidade

| Nível de Criticidade | Faixa Original (Pontos) | Faixa Ajustada (Pontos) | Observação |
|---|---|---|---|
| Baixa | 3 a 7 (<8) | 3 a 6 (<7) | Redução no limite superior da faixa |
| Média | 8 a 11 (>7 e <12) | 7 a 10 (>6 e <11) | Reposicionamento da faixa intermediária |
| Alta | 12 a 15 (>11) | 11 a 15 (>10) | Redução no limite inferior da faixa |

essencial para alinhar a avaliação à missão crítica institucional e aos aspectos operacionais dos sistemas.

Com a etapa de classificação concluída, dois sistemas externos com classificação final de Alta Criticidade foram selecionados para compor o Estudo de Caso. Por confidencialidade, seus nomes foram substituídos por identificadores fictícios: **Sistema Alpaca** e **Sistema Lhama**. Ambos apresentam arquiteturas similares, utilizando o mesmo sistema operacional, com separação entre servidor de aplicação e servidor de banco de dados.

## 5.3 APLICAÇÃO DO 3SW

Uma vez que os sistemas foram definidos para o Estudo de Caso, foi aplicado o Modelo 3SW ao Sistema Alpaca e o Modelo WAH ao Sistema Lhama. A aplicação foi feita de forma sequencial, de acordo com a seguinte janela:

- **Sistema Alpaca (3SW):** 17 de fevereiro a 11 de abril de 2025 — 39 dias úteis (54 dias corridos); e
- **Sistema Lhama (WAH):** 14 de abril a 10 de junho de 2025 — 39 dias úteis (58 dias corridos).

Como explicado na Seção 5.1.1, os sistemas de produção foram clonados e isolados no início do Ciclo 4 do PPSI para evitar interferência no estudo. No entanto, até o final do Ciclo 3, diversas medidas do CIS Controls v8 já haviam sido implementadas pela Empresa ALFA. Assim, para avaliar o estado "antes" da intervenção dos modelos, foi necessário revalidar as medidas de segurança que possuem interseção entre os ciclos do PPSI e os modelos 3SW e WAH.

A Tabela 5.5 exibe: as 33 medidas de segurança que fazem parte dessa interseção entre os ciclos 1 a 3 do PPSI e os modelos 3SW e WAH; o ciclo em que cada uma dessas medidas foi incluída no PPSI; o modelo em que está presente; o *status* do nível AMT ("Adota em Maior parte ou Totalmente") na Empresa ALFA; e se a medida estava previamente implementada em algum dos sistemas antes da aplicação do modelo.

Complementarmente, foram utilizados os seguintes destaques nas cores **Vermelho**, **Verde** e **Branco** na Tabela 5.5 para facilitar a análise do estado de implementação das medidas de segurança:

- **Vermelho:** medida declarada como AMT pelo PPSI, mas não implementada em nenhum dos sistemas;
- **Verde:** medida não declarada como AMT pelo PPSI, mas implementada em pelo menos um dos sistemas; e
- **Branco:** concordância entre o estado do PPSI e o estado real nos sistemas.

Tabela 5.5: Status das medidas comuns entre PPSI, 3SW e WAH após o fim do Ciclo 3

| Medida | Ciclo PPSI | Presente em | PPSI (AMT) | Alpaca (I) | Lhama (I) | Pré-existente |
|---|---|---|---|---|---|---|
| 1.1 | 1 | 3SW | Sim | Não | N/A | Nenhum |
| 2.1 | 1 | Ambos | Sim | Não | Não | Nenhum |
| 2.2 | 1 | Ambos | Sim | Não | Não | Nenhum |
| 2.3 | 1 | Ambos | Sim | Não | Não | Nenhum |
| 2.4 | 3 | Ambos | Não | Sim | Sim | Ambos |
| 3.1 | 2 | WAH | Não | N/A | Não | Nenhum |
| 3.2 | 2 | Ambos | Não | Não | Não | Nenhum |
| 3.3 | 3 | Ambos | Não | Não | Não | Nenhum |
| 3.10 | 3 | Ambos | Não | Sim | Sim | Ambos |
| 3.14 | 3 | 3SW | Não | Não | N/A | Nenhum |
| 6.1 | 1 | WAH | Não | N/A | Sim | Lhama |
| 6.2 | 1 | WAH | Não | N/A | Sim | Lhama |
| 6.3 | 1 | Ambos | Não | Não | Não | Nenhum |
| 6.4 | 3 | WAH | Não | N/A | Sim | Lhama |
| 6.5 | 1 | Ambos | Sim | Não | Não | Nenhum |
| 7.3 | 3 | Ambos | Sim | Não | Não | Nenhum |
| 7.7 | 1 | Ambos | Sim | Não | Não | Nenhum |
| 8.1 | 1 | WAH | Não | N/A | Sim | Lhama |
| 8.2 | 3 | Ambos | Não | Não | Não | Nenhum |
| 8.3 | 1 | WAH | Sim | Não | Não | Nenhum |
| 8.4 | 2 | Ambos | Sim | Não | Não | Nenhum |
| 8.6 | 3 | Ambos | Não | Sim | Sim | Ambos |
| 8.10 | 2 | Ambos | Não | Não | Não | Nenhum |
| 10.1 | 2 | Ambos | Sim | Não | Não | Nenhum |
| 10.2 | 2 | Ambos | Sim | Não | Não | Nenhum |
| 11.1 | 1 | 3SW | Sim | Não | N/A | Nenhum |
| 11.2 | 1 | 3SW | Não | Sim | N/A | Alpaca |
| 11.3 | 3 | Ambos | Sim | Não | Não | Nenhum |
| 11.4 | 1 | Ambos | Não | Sim | Sim | Ambos |
| 11.5 | 1 | 3SW | Não | Não | N/A | Nenhum |
| 14.1 | 2 | WAH | Não | N/A | Não | Nenhum |
| 16.8 | 3 | Ambos | Não | Sim | Sim | Ambos |
| 17.2 | 1 | Ambos | Sim | Não | Não | Nenhum |

**Legenda:** AMT = Adota em Maior Parte ou Totalmente; I = Implementada; N/A = Não se APlica ao Modelo.
Linhas vermelhas claras: medidas com "Adota em Maior Parte ou Totalmente" no PPSI, mas não implementadas em todos os sistemas.
Linhas verdes claras: medidas implementadas em pelo menos um dos sistemas analisados, mas não declaradas como "Adota em Maior Parte ou Totalmente" no PPSI.

O objetivo foi verificar se o *status* AMT registrado no *framework* PPSI corresponde ao estado real de implementação nos sistemas selecionados para o estudo de caso. Essa verificação permitiu identificar eventuais divergências entre o que está documentado institucionalmente e a aplicação prática das medidas de segurança na organização ALFA, considerando o conjunto específico de sistemas avaliados. Os resultados da análise das 33 medidas para os sistemas Alpaca e Lhama, comparados ao status institucional do PPSI, são apresentados a seguir (ver Tabela 5.5):

- 14 medidas (42%) foram marcadas como AMT pelo PPSI, mas não estavam implementadas em nenhum dos sistemas (linha vermelha);
- 10 medidas (30%) estavam implementadas nos sistemas, mas essas medidas não foram assinadas com nível "AMT" institucionalmente (linha verde); e
- 9 medidas (27%) apresentaram correspondência entre a avaliação institucional AMT e o estado nos sistemas (linha branca).

Esses resultados revelam dados importantes das medidas classificadas com AMT, em que 100% (14/14) dessas medidas não foram identificadas como implementadas em nenhum dos dois sistemas analisados no estudo. Isso evidencia limitações relevantes na escala de avaliação utilizada pelo PPSI. Segundo o Guia do PPSI [79], o nível AMT é atingido quando a medida está implementada integralmente em mais de 50% ou em todos os ativos, o que pode ocultar a ausência de implementação em sistemas críticos. Ademais, uma vez alcançado esse nível, a medida deixa de ser monitorada pela SGD/MGI, o que pode comprometer a visibilidade sobre falhas, visto que elas podem não ter sido corrigidas em sua totalidade. As demais situações, linhas verdes e brancas, ainda estão no escopo de evolução de análise do PPSI, ou seja, não evidenciam destaque negativo. A Tabela 5.6 resume a distribuição quantitativa das medidas segundo o *status* identificado.

Tabela 5.6: Resumo da análise das medidas do PPSI comparadas ao estado real dos sistemas selecionados

| **Categoria de Análise** | **Quantidade** | **Porcentagem** |
|---|---|---|
| Medidas AMT não implementadas nos sistemas selecionados (vermelho) | 14 | 42% (14/33) |
| Medidas não-AMT, mas implementadas nos sistemas selecionados (verde) | 10 | 30% (10/33) |
| Medidas com correspondência PPSI x sistemas selecionados (branco) | 9 | 27% (9/33) |
| **Total de Medidas Analisadas** | **33** | **100%** |

**Nota:** As porcentagens foram arredondadas para facilitar a leitura. Dessa forma, a soma total pode não resultar exatamente em 100%.

Essa disparidade entre avaliação centralizada e realidade local reforça a importância de avaliações específicas por sistema, especialmente quando se trata de ativos classificados como críticos.

## 5.4 RESUMO DO CAPÍTULO

Este capítulo apresenta as etapas iniciais do processo de validação do Modelo 3SW, desenvolvido para adaptar as medidas do CIS Controls v8.1 ao contexto de servidores web, com foco em aplicabilidade, efetividade e validade (OE3). A validação começou com o diagnóstico institucional da Empresa ALFA, realizado por meio da análise documental de diversos instrumentos, incluindo o Programa de Privacidade e Segurança da Informação (PPSI) (ver Seção 5.1.1) e o processo de Gestão de Riscos Organizacional (ver Seção 5.1.2). Essa análise permitiu identificar o ponto de integração do 3SW no processo de gestão de riscos, especificamente na etapa de definição de respostas aos riscos, em alinhamento com os objetivos do estudo e a viabilidade operacional (Tabela 5.2).

A validação também incluiu duas entrevistas. Na primeira, o Chefe de Segurança da Informação destacou que a organização já adotava o CIS Controls antes da formalização do PPSI, em 28 de março de 2023 [66]. Embora considere o CIS Controls um *framework* genérico, o entrevistado avaliou positivamente o direcionamento do 3SW a servidores web, reconhecendo seu potencial como segunda camada de proteção. Na segunda entrevista, o Gestor de TI aplicou a metodologia de classificação de criticidade de sistemas externos (ver Seção 5.2), resultando na escolha de dois sistemas de alta criticidade para o estudo de caso: Sistema Alpaca (3SW) e Sistema Lhama (WAH).

Antes da aplicação dos modelos, foi realizado o registro do estado atual das medidas de segurança nesses sistemas, considerando o andamento do PPSI. Essa verificação revelou discrepâncias entre o *status* "Adota em Maior Parte ou Totalmente" (AMT) declarado no PPSI e a realidade de implementação: 42% das medidas AMT não estavam implementadas, 30% estavam implementadas sem registro e apenas 27% apresentavam alinhamento entre registro e prática (Tabela 5.5). Esses resultados expõem limitações na avaliação centralizada do PPSI e reforçam a importância de análises específicas por sistema.

A análise pré-implementação demonstrou que, por propor medidas direcionadas, o 3SW pode contribuir para uma gestão de segurança mais robusta em servidores web — percepção reforçada pela entrevista com o Chefe de Segurança da Informação.

# 6 ANÁLISE DOS RESULTADOS DO ESTUDO DE CASO

Este capítulo apresenta a análise dos resultados do estudo de caso conduzido para validar o Modelo 3SW, desenvolvido para adaptar as medidas do CIS Controls v8.1 ao contexto de servidores web, com foco em sua aplicabilidade, efetividade e validade (OE3). A estrutura do capítulo segue as etapas descritas no Capítulo 3, iniciando com a análise comparativa da efetividade global dos modelos 3SW e WAH em um ambiente real (Seção 6.1), seguida pela análise detalhada das medidas comuns e exclusivas de cada modelo aplicadas aos sistemas Alpaca e Lhama (Seções 6.1 a 6.2). Por fim, discutem-se as lições aprendidas sobre a efetividade do PPSI (Seção 5.1.3), a avaliação institucional e as melhorias propostas para o 3SW (Seção 6.3), e as ameaças à validade do estudo (Seção 6.4). A triangulação de dados, combinando entrevistas, análise documental e métricas técnicas, sustenta a robustez dos resultados, alinhando-se aos objetivos da pesquisa.

## 6.1 COMPARATIVO DA EFETIVIDADE GLOBAL

Após a construção do Modelo 3SW e sua comparação teórica com o Modelo WAH na Seção 4.3, faz-se necessária a análise, de forma prática, da efetividade de ambos os modelos a partir da implementação das medidas de segurança em um ambiente real. A Tabela 6.1 apresenta os dados consolidados da implementação das medidas dos modelos 3SW e WAH.

Essa tabela sintetiza a quantidade total de medidas possíveis por controle em cada um dos modelos, destacando aquelas que não se aplicam ao ambiente estudado, as que já estavam previamente implementadas, as efetivamente aplicadas no Estudo de Caso e, por fim, o percentual de cobertura real alcançado. Também são indicadas as mitigações do MITRE ATT&CK cobertas por cada controle de acordo com as medidas implementadas em cada modelo.

A análise da Tabela 6.1 permite relacionar a resposta obtida na análise comparativa (QP3) realizada na Seção 4.3 e a aplicação prática obtida pelo Estudo de Caso, revelando se a priorização adotada no 3SW se traduz em maior viabilidade técnica no cenário proposto.

Como pode ser visto na Tabela 6.1, no que tange às medidas de segurança, o Modelo 3SW resultou em **76 medidas implementadas**, o que representa uma **efetividade de 82%** (76/93). Por sua vez, o Modelo WAH obteve **67 medidas implementadas**, correspondendo a **74% de efetividade** (67/90). Essa diferença quantitativa reforça a hipótese de que o 3SW apresenta maior viabilidade técnica no contexto específico de servidores web, conforme proposto nesta dissertação. Como complemento informacional, no que tange às mitigações ativas após o Estudo de Caso, observa-se que o Sistema Alpaca implementou 35 das 36 mitigações possíveis (97%), ao passo que o Sistema Lhama alcançou 36 das 38 mitigações possíveis (95%). Assim, em termos de mitigações totais únicas, os dois modelos ficam próximos ao que se propõem.

No que concerne ao agrupamento de medidas por controle, destaca-se o C4 (Configuração Segura) e o C12 (Infraestrutura de Rede) que já contavam com quase a totalidade de **medidas pré-existentes** nos

Tabela 6.1: Estado da Implementação das medidas de segurança nos Sistemas Alpaca (3SW) e Lhama (WAH) pós Estudo de Caso

| **Sistema Alpaca - Modelo 3SW** | | | | | | | |
|---|---|---|---|---|---|---|---|
| **IDC** | **TM** | **N/A** | **PE** | **IEC** | **Total (%)** | **PI** | **Mitigações (Ativas)** |
| C1 | 1 | 0 | 0 | 1 | 100% (1/1) | 0 | M1035 |
| C2 | 7 | 0 | 1 | 6 | 100% (7/7) | 0 | M1021, M1022, M1025, M1026, M1033, M1038, M1042, M1044, M1045, M1047, M1054 |
| C3 | 10 | 0 | 3 | 4 | 70% (7/10) | 0 | M1029, M1030, M1041, M1047 |
| C4 | 8 | 0 | 8 | 0 | 100% (8/8) | 0 | M1015, M1018, M1022, M1024, M1025, M1026, M1027, M1028, M1030, M1033, M1035, M1036, M1037, M1039, M1040, M1041, M1042, M1043, M1044, M1045, M1046, M1047, M1048, M1052, M1054 |
| C5 | 6 | 0 | 1 | 5 | 100% (6/6) | 0 | M1018, M1022, M1026, M1027, M1047 |
| C6 | 5 | 1 | 1 | 2 | 60% (3/5) | 0 | M1018, M1022, M1026, M1047 |
| C7 | 5 | 0 | 2 | 3 | 100% (5/5) | 0 | M1016, M1037, M1042, M1051 |
| C8 | 10 | 0 | 2 | 8 | 100% (10/10) | 0 | M1018, M1028, M1029, M1047 |
| C9 | 4 | 2 | 0 | 2 | 50% (2/4) | 0 | M1021, M1031, M1037 |
| C10 | 7 | 2 | 0 | 3 | 43% (3/7) | 0 | M1049 |
| C11 | 5 | 0 | 2 | 2 | 80% (4/5) | 0 | M1029, M1030, M1041, M1053 |
| C12 | 4 | 0 | 4 | 0 | 100% (4/4) | 0 | M1018, M1026, M1029, M1030, M1035 |
| C13 | 4 | 0 | 1 | 3 | 100% (4/4) | 0 | M1030, M1035, M1037, M1040, M1049, M1050 |
| C14 | 0 | 0 | 0 | 0 | - | 0 | |
| C15 | 1 | 0 | 1 | 0 | 100% (1/1) | 0 | M1018, M1052 |
| C16 | 10 | 0 | 2 | 4 | 60% (6/10) | 1 | M1016, M1026, M1030, M1042, M1048, M1047 |
| C17 | 1 | 0 | 0 | 1 | 100% (1/1) | 0 | Não há mitigações |
| C18 | 5 | 0 | 0 | 4 | 80% (4/5) | 1 | M1015, M1016, M1028, M1037, M1042, M1047, M1051, M1054, M1056 |
| **Totais** | **93** | **5** | **28** | **48** | **82% (76/93)** | | **TMU = 97% (35/36)** |

| **Sistema Lhama - Modelo WAH** | | | | | | | |
|---|---|---|---|---|---|---|---|
| **IDC** | **TM** | **N/A** | **PE** | **IEC** | **Total (%)** | **PI** | **Mitigações (Ativas)** |
| C1 | 0 | 0 | 0 | 0 | - | 0 | - |
| C2 | 7 | 0 | 1 | 6 | 100% (7/7) | 0 | M1021, M1022, M1025, M1026, M1033, M1038, M1042, M1044, M1045, M1047, M1054 |
| C3 | 7 | 0 | 2 | 4 | 86% (6/7) | 0 | M1018, M1022, M1026, M1029, M1030, M1041, M1047 |
| C4 | 8 | 0 | 7 | 0 | 88% (7/8) | 0 | M1015, M1018, M1022, M1024, M1025, M1026, M1027, M1028, M1030, M1033, M1035, M1036, M1037, M1039, M1040, M1041, M1042, M1043, M1044, M1045, M1046, M1047, M1048, M1052, M1054 |
| C5 | 5 | 0 | 1 | 4 | 100% (5/5) | 0 | M1018, M1022, M1026, M1027, M1047 |
| C6 | 6 | 0 | 4 | 0 | 67% (4/6) | 0 | M1018, M1022, M1026, M1032, M1047 |
| C7 | 7 | 0 | 1 | 6 | 100% (7/7) | 0 | M1016, M1037, M1042, M1051 |
| C8 | 5 | 0 | 1 | 4 | 100% (5/5) | 0 | M1018, M1028, M1029, M1047 |
| C9 | 5 | 2 | 3 | 0 | 60% (3/5) | 0 | M1021, M1037, M1049 |
| C10 | 5 | 1 | 0 | 0 | 0% (0/5) | 3 | 0 |
| C11 | 2 | 0 | 1 | 1 | 100% (2/2) | 0 | M1029, M1030, M1041, M1053 |
| C12 | 4 | 0 | 3 | 0 | 75% (3/4) | 1 | M1029, M1030, M1035, M1051 |
| C13 | 7 | 0 | 1 | 3 | 57% (4/7) | 0 | M1030, M1035, M1037, M1040, M1049, M1050 |
| C14 | 6 | 0 | 1 | 2 | 50% (3/6) | 0 | M1017, M1027 |
| C15 | 1 | 0 | 1 | 0 | 100% (1/1) | 0 | M1018, M1052 |
| C16 | 11 | 0 | 2 | 5 | 64% (7/11) | 1 | M1016, M1030, M1047, M1048, M1051 |
| C17 | 0 | 0 | 0 | 0 | - | 0 | - |
| C18 | 4 | 0 | 0 | 3 | 75% (3/4) | 1 | M1016, M1015, M1028, M1037, M1042, M1047, M1051, M1054, M1056 |
| **Totais** | **90** | **3** | **29** | **38** | **74% (67/90)** | | **TMU = 95% (36/38)** |

**Legenda: IDC**: Identificação do Controle; **TM**: Total de Medidas possíveis; **N/A**: Não se Aplica - medidas fora do escopo técnico; **PE**: Pré-Existente - medidas já adotadas anteriormente; **IEC**: Implementada no Estudo de Caso - medidas implementadas no estudo de caso; **PI**: Parcialmente Implementada - indica se houve implementação parcial; **Mitigações (Ativas)**: mitigações MITRE ATT&CK cobertas; **TMU**: Total de Mitigações Únicas - mitigações únicas cobertas pelo objeto Estudado, após a implementação do modelo.

dois ambientes analisados, indicando uma maturidade institucional nesses domínios antes da aplicação dos modelos. Em números totais, o Sistema Alpaca e o Sistema Lhama apresentaram, respectivamente, 30% (28/93) e 32% (29/90) de medidas pré-existentes antes da aplicação dos modelos no Estudo de Caso.

Ainda considerando a efetividade geral, observa-se que, no escopo de medidas possíveis estabelecido por cada modelo, o 3SW obteve melhor desempenho: dos 17 controles com medidas vinculadas, 10 deles (59%) tiveram todas as medidas totalmente implementadas. No Modelo WAH, esse número foi menor — seis controles com implementação total, o que representa 38%. Esse resultado reforça a superioridade do 3SW em termos de completude por controle, o que pode estar relacionado à sua maior especialização no contexto de servidores web.

A Seção a seguir detalha os resultados do Estudo de Caso, considerando os dados da Tabela 6.1 e complementando a comparação teórica da Seção 4.3. Para avaliar a efetividade prática dos modelos 3SW e WAH nos sistemas Alpaca e Lhama, respectivamente, o estudo foi estruturado em três categorias, conforme organizado na Tabela 4.3: medidas comuns aos modelos 3SW e WAH (Seção 6.1.1), medidas exclusivas do 3SW (Seção 6.1.2) e medidas exclusivas do WAH (Seção 6.1.3). Essa abordagem verifica se a priorização do 3SW promove maior viabilidade técnica no contexto de servidores web, alinhando-se ao objetivo de validação da pesquisa (OE3).

### 6.1.1 Análise das Medidas Comuns entre 3SW e WAH

A Tabela 6.2 reúne as 61 medidas comuns a ambos os modelos, apresentando os resultados obtidos no Estudo de Caso para os sistemas Alpaca e Lhama. Como pode ser visto, as 61 medidas comuns entre os modelos 3SW e WAH alcançaram taxas de implementação nos sistemas estudados de 80% (49/61) para o 3SW e 79% (48/61) para o WAH, evidenciando uma aderência praticamente equivalente. Essa alta convergência reforça a consistência das medidas técnicas selecionadas para servidores web em ambos os modelos, alinhando-se à proposta do 3SW de priorizar medidas de segurança diretamente aplicáveis ao ativo. Controles como C2 (Inventário e Controle de Ativos de Software), C4 (Configuração Segura de Ativos Corporativos e Software), C5 (Gestão de Contas), C7 (Gestão Contínua de Vulnerabilidades), C8 (Gestão de Registros de Auditoria), C11 (Recuperação de Dados), C13 (Monitoramento e Defesa da Rede) e C15 (Gestão de Provedor de Serviços) atingiram 100% de implementação em ambos os modelos, indicando que essas medidas são aplicáveis à segurança de servidores web.

A presença de medidas classificadas como “não aplicáveis” ou “parcialmente implementadas” (totalizando 9/12 no 3SW e 8/13 no WAH) reflete particularidades dos sistemas Alpaca e Lhama, como limitações técnicas ou contextuais. Se essas medidas “não aplicáveis” fossem desconsideradas ou as parciais contabilizadas como implementadas, as taxas de adesão seriam ainda mais elevadas, reforçando a robustez das medidas técnicas comuns. Assim, a análise das medidas comuns destaca que o 3SW e o WAH são consistentes na seleção de controles técnicos essenciais, com o 3SW se destacando por sua proposta de aplicabilidade direta ao servidor web, conforme definido pelos critérios de seleção CS1, CS2 e CS3, ver 3.1.1.

Tabela 6.2: Medidas comuns entre modelos 3SW e WAH

| IDC | TM | Implementação | | 3SW | | | WAH | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 3SW | WAH | Parcial | N/A | N/Impl. | Parcial | N/A | N/Impl. |
| C1 | 0 | N/I | N/I | N/I | N/I | N/I | N/I | N/I | N/I |
| C2 | 7 | 100% (7/7) | 100% (7/7) | 0 | 0 | 0 | 0 | 0 | 0 |
| C3 | 6 | 67% (4/6) | 83% (5/6) | 2 | 0 | 0 | 0 | 0 | 1 |
| C4 | 6 | 100% (6/6) | 100% (6/6) | 0 | 0 | 0 | 0 | 0 | 0 |
| C5 | 5 | 100% (5/5) | 100% (5/5) | 0 | 0 | 0 | 0 | 0 | 0 |
| C6 | 3 | 33% (1/3) | 33% (1/3) | 0 | 1 | 1 | 0 | 0 | 2 |
| C7 | 5 | 100% (5/5) | 100% (5/5) | 0 | 0 | 0 | 0 | 0 | 0 |
| C8 | 3 | 100% (3/3) | 100% (3/3) | 0 | 0 | 0 | 0 | 0 | 0 |
| C9 | 2 | 50% (1/2) | 50% (1/2) | 0 | 1 | 0 | 0 | 1 | 0 |
| C10 | 5 | 40% (2/5) | 0% (0/5) | 1 | 1 | 1 | 3 | 1 | 1 |
| C11 | 2 | 100% (2/2) | 100% (2/2) | 0 | 0 | 0 | 0 | 0 | 0 |
| C12 | 2 | 100% (2/2) | 50% (1/2) | 0 | 0 | 0 | 1 | 0 | 0 |
| C13 | 3 | 100% (3/3) | 100% (3/3) | 0 | 0 | 0 | 0 | 0 | 0 |
| C14 | 0 | N/I | N/I | N/I | N/I | N/I | N/I | N/I | N/I |
| C15 | 1 | 100% (1/1) | 100% (1/1) | 0 | 0 | 0 | 0 | 0 | 0 |
| C16 | 7 | 57% (4/7) | 71% (5/7) | 2 | 0 | 1 | 1 | 0 | 1 |
| C17 | 0 | N/I | N/I | N/I | N/I | N/I | N/I | N/I | N/I |
| C18 | 4 | 75% (3/4) | 75% (3/4) | 1 | 0 | 0 | 1 | 0 | 0 |
| **Total** | **61** | **80% (49/61)** | **79% (48/61)** | **20% (12/61)** | | | **21% (13/61)** | | |

**Legenda: IDC**: Identificador do Controle; **TM**: Total de Medidas; **Parcial**: Parcialmente Implementada; **N/A**: Não Aplicável; **N/Impl.**: Não Implementada; **N/I**: Nenhuma Interseção.

### 6.1.2 Análise das Medidas Exclusivas do 3SW no Sistema Alpaca

Em relação às 32 medidas exclusivas do 3SW (Tabela 6.3), o Sistema Alpaca alcançou uma taxa de implementação de 84% (27/32), sendo 10 dessas medidas ou 31% (10/32) medidas pré-existentes. Controles como C1 (Inventário e Controle de Ativos Corporativos), C4 (Configuração Segura de Ativos Corporativos e Software), C5 (Gestão de Contas), C6 (Gestão do Controle de Acesso), C8 (Gestão de Registros de Auditoria), C12 (Gestão da Infraestrutura de Rede), C13 (Monitoramento e Defesa da Rede), C17 (Gestão de Respostas a Incidentes) e C18 (Testes de Invasão) atingiram 100% de implementação, no que tange às medidas exclusivas do modelo, evidenciando a eficácia do 3SW em priorizar medidas técnicas diretamente aplicáveis ao servidor web. O controle C8, com 7 medidas exclusivas, destaca-se pela ênfase na gestão de registros de auditoria, essencial para monitoramento e resposta a incidentes. Além disso, conforme dado compilado na Tabela 4.6, o Modelo 3SW tem 42% a mais de medidas voltadas a esse controle, quando comparado ao WAH.

Apenas cinco medidas (16%) foram classificadas como “não aplicáveis”, “parcialmente implementadas” ou “não implementadas”, refletindo particularidades do Sistema Alpaca. Nos controles C9 (Proteções de E-mail e Navegador Web) e C10 (Defesas contra Malware), por exemplo, a taxa de 50% (1/2) deve-se a uma medida não aplicável em cada controle, por não se alinhar ao propósito do sistema analisado. A alta taxa de implementação (84%) e a presença de medidas pré-existentes (31%) confirmam que o 3SW é altamente compatível com ambientes reais, alinhando-se à sua proposta de proteção direta do servidor web.

Tabela 6.3: Medidas Únicas do 3SW no Sistema Alpaca

| IDC | TM | Pré-Exist. | Total Impl. | Parcial | N/A | N/Impl. |
|---|---|---|---|---|---|---|
| C1 | 1 | 0 | 100% (1/1) | 0 | 0 | 0 |
| C2 | SMU | SMU | SMU | SMU | SMU | SMU |
| C3 | 4 | 1 | 75% (3/4) | 1 | 0 | 0 |
| C4 | 2 | 2 | 100% (2/2) | 0 | 0 | 0 |
| C5 | 1 | 0 | 100% (1/1) | 0 | 0 | 0 |
| C6 | 2 | 1 | 100% (2/2) | 0 | 0 | 0 |
| C7 | SMU | SMU | SMU | SMU | SMU | SMU |
| C8 | 7 | 2 | 100% (7/7) | 0 | 0 | 0 |
| C9 | 2 | 0 | 50% (1/2) | 0 | 1 | 0 |
| C10 | 2 | 0 | 50% (1/2) | 0 | 1 | 0 |
| C11 | 3 | 1 | 66,7% (2/3) | 0 | 0 | 1 |
| C12 | 2 | 2 | 100% (2/2) | 0 | 0 | 0 |
| C13 | 1 | 0 | 100% (1/1) | 0 | 0 | 0 |
| C14 | SMU | SMU | SMU | SMU | SMU | SMU |
| C15 | SMU | SMU | SMU | SMU | SMU | SMU |
| C16 | 3 | 1 | 66,7% (2/3) | 0 | 0 | 1 |
| C17 | 1 | 0 | 100% (1/1) | 0 | 0 | 0 |
| C18 | 1 | 0 | 100% (1/1) | 0 | 0 | 0 |
| **Total** | **32** | **31% (10/32)** | **84% (27/32)** | **16% (5/32)** | | |

**Legenda: IDC**: Identificador do Controle; **TM**: Total de Medidas; **Pré-Exist.**: Medidas pré-existentes; **Total Impl.**: Total Implementado; **Parcial**: Parcialmente Implementada; **N/A**: Não Aplicável; **N/Impl.**: Não Implementada; **SMU**: Sem Medidas Únicas.

### 6.1.3 Análise das Medidas Exclusivas do WAH no Sistema Lhama

Já em relação às 29 medidas exclusivas do WAH (Tabela 6.3), o Sistema Lhama alcançou uma taxa de implementação de 66% (19/29), sendo 38% (11/29) das medidas pré-existentes. Controles como C6 (Gestão do Controle de Acesso), C7 (Gestão Contínua de Vulnerabilidades), C8 (Gestão de Registros de Auditoria) e C12 (Gestão da Infraestrutura de Rede) atingiram 100% de implementação, mostrando eficácia em aspectos de gestão de acessos e infraestrutura. No entanto, controles como C13 (Monitoramento e Defesa da Rede, 25%, 1/4) e C14 (Conscientização sobre Segurança e Treinamento de Competências, 50%, 3/6) apresentaram taxas mais baixas, sugerindo menor aplicabilidade dessas medidas em servidores web.

Das 29 medidas exclusivas do WAH, 10 são voltadas à criação de processos ou documentação desses, com 8 implementadas, destacando sua força em estabelecer processos organizacionais. No entanto, as 6 medidas de treinamento (C14) e as 9 medidas de infraestrutura de rede ou usuários finais (C12 e C13) enfrentaram desafios de implementação. Justamente por tratarem de escopos amplos que passam à margem dos servidores web.

Por fim, no Sistema Lhama, 34% (10/29) das medidas exclusivas foram classificadas como “não implementadas” ou “não aplicáveis”. Isso indica que o foco do WAH em aspectos organizacionais e de rede é menos alinhado à proteção direta de servidores web, especialmente em comparação com o 3SW.

Tabela 6.4: Medidas Únicas do WAH no Sistema Lhama

| IDC | TM | Pré-Exist. | Total Impl. | Parcial | N/A | N/Impl. |
|---|---|---|---|---|---|---|
| C1 | SMU | SMU | SMU | SMU | SMU | SMU |
| C2 | SMU | SMU | SMU | SMU | SMU | SMU |
| C3 | 1 | 0 | 100% (1/1) | 0 | 0 | 0 |
| C4 | 2 | 1 | 50% (1/2) | 0 | 0 | 1 |
| C5 | SMU | SMU | SMU | SMU | SMU | SMU |
| C6 | 3 | 3 | 100% (3/3) | 0 | 0 | 0 |
| C7 | 2 | 0 | 100% (2/2) | 0 | 0 | 0 |
| C8 | 2 | 1 | 100% (2/2) | 0 | 0 | 0 |
| C9 | 3 | 2 | 66,7% (2/3) | 0 | 1 | 0 |
| C10 | SMU | SMU | SMU | SMU | SMU | SMU |
| C11 | SMU | SMU | SMU | SMU | SMU | SMU |
| C12 | 2 | 2 | 100% (2/2) | 0 | 0 | 0 |
| C13 | 4 | 1 | 25% (1/4) | 0 | 0 | 3 |
| C14 | 6 | 1 | 50% (3/6) | 0 | 0 | 3 |
| C15 | SMU | SMU | SMU | SMU | SMU | SMU |
| C16 | 4 | 0 | 50% (2/4) | 0 | 0 | 2 |
| C17 | SMU | SMU | SMU | SMU | SMU | SMU |
| C18 | SMU | SMU | SMU | SMU | SMU | SMU |
| **Total** | **29** | **38% (11/29)** | **66% (19/29)** | **34% (10/29)** | | |

**Legenda: IDC**: Identificador do Controle; **TM**: Total de Medidas; **Pré-Exist.**: Medidas pré-existentes; **Total Impl.**: Total Implementado; **Parcial**: Parcialmente Implementada; **N/A**: Não Aplicável; **N/Impl.**: Não Implementada; **SMU**: Sem Medidas Unificadas.

## 6.2 VALIDAÇÃO TÉCNICA SOBRE A REDUÇÃO DE VULNERABILIDADES

Além da análise quantitativa e qualitativa da efetividade dos modelos 3SW e WAH, esta pesquisa também avaliou a redução real de vulnerabilidades como indicador objetivo de mitigação de riscos. Conforme estabelecido na metodologia (ver Seção 3.2.2.3) utilizou-se a métrica de Taxa de Redução de Vulnerabilidades (TRV), medida pela comparação entre os cenários anteriores e posteriores à aplicação de cada modelo.

A Tabela 6.5 exibe os dados obtidos por meio das ferramentas institucionais de varredura de segurança. Observa-se que ambos os modelos resultaram em uma redução significativa no número de vulnerabilidades identificadas. Após a aplicação do Modelo 3SW no Sistema Alpaca, todas as vulnerabilidades foram eliminadas. De forma semelhante, a aplicação do Modelo WAH no Sistema Lhama resultou na eliminação de todas as vulnerabilidades críticas, altas, médias e desconhecidas, restando apenas uma vulnerabilidade de baixa criticidade. A presença dessa vulnerabilidade restante não foi culpa do Modelo WAH, mas sim decorrente da inviabilidade de correção no Sistema Lhama. Portanto, esses dados quantitativos reforçam a eficácia (Tabela 6.6) dos dois modelos e evidenciam o potencial de uma análise direcionada, a exemplo da abordagem do Modelo 3SW, como estratégia técnica de resposta a riscos em servidores web.

Ao aprofundar a análise, verificou-se que as medidas responsáveis por essa efetiva redução estão rela-

Tabela 6.5: Comparativo de vulnerabilidades antes e depois da atuação

| Sistema | Modelo Aplicado | Momento | Críticas | Altas | Médias | Baixas | Desconhecidas |
|---|---|---|---|---|---|---|---|
| Alpaca | 3SW | Antes da atuação | 6 | 49 | 43 | 20 | 0 |
| | | Depois da atuação | 0 | 0 | 0 | 0 | 0 |
| Lhama | WAH | Antes da atuação | 10 | 60 | 69 | 24 | 3 |
| | | Depois da atuação | 0 | 0 | 0 | 1 | 0 |

Tabela 6.6: Taxa de Redução de Vulnerabilidades por criticidade

| Sistema | Modelo | Críticas (%) | Altas (%) | Médias (%) | Baixas (%) | Desconhecidas (%) |
|---|---|---|---|---|---|---|
| Alpaca | 3SW | 100% | 100% | 100% | 100% | — |
| Lhama | WAH | 100% | 100% | 100% | 96% | 100% |

cionadas, em ambos os modelos, a ações corretivas. Essas medidas atuam diretamente na eliminação de vulnerabilidades, seja por meio da aplicação de *patches*, da remoção de softwares não autorizados ou da correção de falhas encontradas em testes técnicos. A Tabela 6.7 lista as cinco medidas corretivas que estão presentes em ambos os modelos.

Tabela 6.7: Medidas corretivas comuns aos modelos 3SW e WAH

| Item | Descrição |
|---|---|
| **2.3** | Remover software não autorizado, encerrando o uso de softwares potencialmente vulneráveis. |
| **7.3** | Aplicar atualizações automatizadas no sistema operacional dos ativos da organização, corrigindo falhas conhecidas. |
| **7.4** | Aplicar atualizações automatizadas em aplicações, garantindo a correção contínua de vulnerabilidades em softwares utilizados. |
| **7.7** | Executar a remediação das vulnerabilidades detectadas, com base em processo definido institucionalmente. |
| **18.3** | Corrigir falhas identificadas por meio de testes de invasão, com base na priorização e impacto de cada achado. |

Dessa forma, conclui-se que, no aspecto específico da correção de vulnerabilidades técnicas, não há diferença entre os modelos 3SW e WAH. Ambos adotam as mesmas cinco medidas corretivas fundamentais, responsáveis pela eliminação das falhas identificadas. Isso indica que, independentemente do modelo adotado, essas ações representam o núcleo técnico mais efetivo para a mitigação de riscos reais em servidores web.

## 6.3 AVALIAÇÃO E APLICAÇÃO DA PROPOSTA

A pesquisa desenvolvida nesta dissertação foi orientada pela hipótese de que a adaptação do CIS Controls v8.1 para o contexto de servidores web — denominada Modelo 3SW — poderia reduzir significativamente a probabilidade de êxito de ataques cibernéticos, ao priorizar esforços na proteção de ativos mais expostos. Essa hipótese se fundamenta nos desafios recorrentes na proteção de sistemas acessíveis pela Internet, especialmente em instituições públicas com maturidade institucional em desenvolvimento. No caso da Empresa ALFA, conforme evidenciado na entrevista com o Chefe de Segurança da Informação (ver Seção 5.1.3), a principal limitação está mais na qualificação dos profissionais de áreas de apoio à segurança do que na disponibilidade de recursos, exceto em períodos pontuais de restrição orçamentária.

A proposta teve como objetivo geral desenvolver e aplicar um conjunto de medidas de segurança, com foco na realidade de servidores web, tendo como base empírica um estudo de caso em uma organização pública. Para isso, foram alcançados três objetivos específicos: (OE1) a adaptação dos controles do CIS v8.1 ao contexto de servidores web; (OE2) a identificação e classificação dos sistemas críticos; e (OE3) a verificação da efetividade da solução proposta.

A aplicação prática do Modelo 3SW foi realizada sobre um sistema real (Alpaca), e seus resultados foram comparados a outro modelo de referência (WAH) aplicado em sistema distinto (Lhama). A avaliação técnica demonstrou que ambos os modelos foram eficazes na eliminação de vulnerabilidades críticas, altas e médias, evidenciando que apenas o direcionamento do foco fez o nível de proteção aos sistemas fosse elevado independente do modelo aplicado. A análise reforçou que as medidas corretivas comuns, centradas em ações como aplicação de *patches*, remoção de software não autorizado e remediação baseada em testes, compõem o núcleo técnico responsável pela mitigação efetiva dos riscos.

Importante destacar que a execução das medidas previstas tanto no Modelo 3SW quanto no WAH envolveu a participação de profissionais de diferentes equipes internas da Empresa ALFA, especialmente da área de TI. Isso ocorreu porque as medidas abrangem múltiplas áreas de conhecimento. A título de registro: as ações relacionadas à documentação entre setores contaram com a coordenação do setor de governança; as medidas de *backup* demandaram alinhamento com a equipe de infraestrutura; a restrição e o registro de acessos ao banco de dados envolveram a equipe de banco de dados; a análise e o monitoramento de ameaças exigiram a atuação da área de segurança; e, por fim, a atualização de componentes dos sistemas contou com o apoio da equipe de desenvolvimento.

Adicionalmente, a validação institucional — por meio da entrevista com o Chefe de Segurança da Informação (Seção 5.1.3) — evidenciou que o Modelo 3SW foi bem recebido, sendo percebido como uma "segunda camada" de proteção capaz de detalhar e aprofundar as diretrizes genéricas do CIS Controls v8. O entrevistado destacou a importância de medidas específicas para servidores web e sistemas expostos à Internet, apontando que o 3SW responde a uma lacuna técnica existente na organização. A proposta mostrou-se alinhada com as necessidades estratégicas da organização, especialmente pela sua capacidade de tratar riscos concretos em sistemas expostos à Internet, mesmo diante dos desafios institucionais relacionados à priorização e alocação eficiente de recursos.

Assim, os resultados obtidos sustentam a hipótese proposta, demonstrando que a implementação do Modelo 3SW é tecnicamente eficaz, mesmo quando há necessidade de otimizar o uso dos recursos disponíveis. Ademais, o foco técnico do modelo torna sua aplicação adaptável a diferentes contextos institucionais, desde que se considere a realidade dos ativos e os riscos específicos de cada ambiente.

O modelo também se mostra útil como referência para processos contínuos de aprimoramento. Sua aplicação pode ser mensurada por indicadores como a redução de vulnerabilidades e de eventos de segurança, o que permite sua integração a ciclos de melhoria (PDCA) e ao fortalecimento da governança de segurança. Por fim, a pesquisa evidencia que o fortalecimento da segurança cibernética em ambientes críticos exige, além de boas práticas, uma abordagem contextualizada, técnica e orientada a riscos específicos, como a que foi promovida pelo Modelo 3SW.

Entretanto, para ampliar a aplicabilidade e eficácia do Modelo 3SW, algumas melhorias podem ser aplicadas. Primeiramente, a adaptação do modelo para outros tipos de ativos, como servidores de banco de

dados, ou ativos de rede, pode aumentar sua versatilidade. Isso exigiria a revisão dos critérios de seleção (CS1, CS2, CS3; Seção 3.1.1) para incluir medidas aplicáveis a diferentes arquiteturas.

Em segundo lugar, a automação de medidas, como a integração com ferramentas de varredura de vulnerabilidades ou monitoramento contínuo, poderia reduzir o esforço operacional e melhorar a escalabilidade do modelo. Por exemplo, a implementação automatizada de atualizações (medidas 7.3 e 7.4, Tabela 6.7) poderia ser vinculada a sistemas de gerenciamento de configurações. Destaca-se que a automação de atualizações pode ser restrita a aplicações menos críticas e com todo o devido cuidado com o estabelecimento de *backup* e de *snapshot*, de modo que o ambiente possa ser restaurado mediante problemas identificados.

Em terceiro lugar, a construção de uma ferramenta para suporte ao 3SW poderia ajudar a criar rastreabilidade entre as mitigações observadas pelo MITRE ATT&CK e as soluções propostas para cada sistema aplicado. Isso permitiria o acompanhamento da efetividade das implementações, bem como contribuiria para a documentação (base de conhecimento) e maturidade das ações executadas.

Por fim, o desenvolvimento de treinamentos específicos para equipes técnicas, focados na aplicação prática das medidas do 3SW, seria essencial para superar as lacunas de capacitação mencionadas pelo entrevistado (Seção 5.1.3). Essas melhorias, combinadas com a abordagem técnica do 3SW, podem consolidar o modelo como uma referência robusta para a proteção de servidores web em organizações com diferentes níveis de maturidade.

## 6.4 AMEAÇAS À VALIDADE

Embora o estudo tenha adotado medidas rigorosas para garantir a validade dos dados e a confiabilidade dos resultados, algumas limitações metodológicas devem ser reconhecidas.

Em relação à *validade de construto*, existe a possibilidade de interpretação divergente dos termos utilizados nas entrevistas, ainda que os participantes estejam diretamente envolvidos com os temas tratados. A *validade interna* pode ter sido afetada por fatores externos não controlados que também influenciaram a redução das vulnerabilidades, como atualizações sistêmicas independentes da aplicação do 3SW.

No que diz respeito à *validade externa*, os resultados obtidos referem-se a um único estudo de caso em uma organização pública específica. Apesar da sistematização dos critérios adotados, a aplicabilidade do modelo em outros contextos deve ser avaliada com cautela, principalmente diante do impacto ao negócio.

Por fim, a *confiabilidade* depende, em parte, da interpretação do pesquisador durante a análise qualitativa, o que pode introduzir algum grau de subjetividade, mesmo com a adoção de protocolos e registro das entrevistas.

O reconhecimento dessas ameaças não invalida os resultados obtidos, mas contribui para a transparência e a integridade da pesquisa, além de indicar caminhos para aprimoramentos em estudos futuros.

## 6.5 RESUMO DO CAPÍTULO

O capítulo avaliou a efetividade do 3SW em reduzir vulnerabilidades em sistemas críticos (OE3), utilizando a triangulação de dados (entrevistas, análise documental e ferramentas de varredura de vulnerabilidades) como descrito na metodologia (Seção 3.2.2.3). A análise abrangeu a aplicação prática do 3SW no Sistema Alpaca e do WAH no Sistema Lhama, com métricas quantitativas como a Taxa de Redução de Vulnerabilidades (TRV) e a cobertura MITRE ATT&CK, além de percepções qualitativas do Chefe de Segurança da Informação, consolidadas no Capítulo 5 (5.1.3). Os resultados confirmam a hipótese de que o 3SW reduz significativamente a probabilidade de ataques cibernéticos em servidores web.

A validação técnica (Seção 6.2) demonstrou que tanto o 3SW quanto o WAH reduziram praticamente 100% das vulnerabilidades identificadas (críticas, altas, médias e baixas), conforme Tabela 6.6. A redução de 96% no Sistema Lhama pelo WAH decorreu de um impedimento técnico que também limitaria o 3SW. A análise comparativa (Seção 6.1) mostra que o 3SW implementou 82% das medidas propostas (76/93, Tabela 6.1), contra 74% do WAH (67/90), com cobertura MITRE ATT&CK de 97% (35/36 mitigações) para o 3SW e 95% (36/38) para o WAH. Medidas corretivas comuns, como aplicação de *patches* e remoção de software não autorizado (Tabela 6.7), foram cruciais para a mitigação de riscos, destacando a adequação do 3SW para servidores web expostos à Internet (Seção 3.1.1).

A pesquisa usou triangulação de dados, combinando entrevistas, análise documental (Seção 5.1.1) e resultados técnicos, como a redução de vulnerabilidades (Seção 6.2). Essa abordagem, prevista na metodologia (Seção 3.2.2.3), garante que os resultados sejam confiáveis, pois unem a opinião do Chefe de Segurança da Informação, as lacunas do PPSI e as métricas do Estudo de Caso. Juntos, esses dados revelam que o 3SW é uma solução eficaz para proteger servidores web na Empresa ALFA.

Na Seção 6.3, os resultados do estudo de caso são sintetizados, confirmando o alinhamento do 3SW com as necessidades da Empresa ALFA, especialmente para sistemas expostos à Internet. A ausência de processos sistemáticos no PPSI, identificada na análise documental e confirmada pela entrevista (Capítulo 5), destaca a relevância do 3SW como uma solução direcionada, com expectativas de aplicação em curto, médio e longo prazo (ciclo PDCA). Limitações práticas, como a baixa implementação do controle C10 (43% no 3SW, devido à complexidade técnica) e desafios na expansão para outros ambientes, foram observados, mas não comprometem a eficácia do modelo. A entrevista com o Gestor de TI (Seção 5.2) contribuiu para a seleção de sistemas críticos, embora sem percepções diretas sobre o 3SW.

Também foram propostos ajustes (Seção 6.3) para ampliar a aplicabilidade do modelo, incluindo: (1) adaptação para outros tipos de ativos (ex.: ativos de rede) mediante revisão dos critérios CS1, CS2 e CS3; (2) automação de medidas, quando possível, como integração com ferramentas de varredura; e (3) desenvolvimento de treinamentos para superar lacunas de capacitação. A seção Ameaças à Validade (6.4) aborda a validade de construto, interna, externa e confiabilidade, destacando que a triangulação mitigou vieses e que os critérios de seleção favorecem a generalização analítica. Em resumo, o Capítulo 6 valida a eficácia do 3SW, sugere melhorias práticas e reforça sua relevância estratégica para organizações públicas, alinhando-se aos pilares de prevenção e repressão da Empresa ALFA.

# 7 CONCLUSÃO

Esta pesquisa teve como objetivo desenvolver e validar o Modelo 3SW, um subconjunto de medidas do CIS Controls v8.1 adaptado para a proteção de servidores web, visando reduzir a probabilidade de ataques cibernéticos. A hipótese central, de que a adaptação direcionada do CIS Controls poderia aumentar a segurança de servidores web, foi testada por meio de um estudo de caso na Empresa ALFA, utilizando uma metodologia rigorosa baseada em análise documental, entrevistas e métricas técnicas. Os resultados obtidos confirmam a hipótese inicial e esta conclusão sintetiza os principais resultados alcançados, avalia o cumprimento dos objetivos específicos (OE1, OE2, OE3), destaca as contribuições teóricas e práticas, reconhece as limitações do estudo, com ênfase nas discrepâncias identificadas do PPSI, e propõe recomendações para trabalhos futuros, reforçando a relevância do 3SW para uma transformação digital com mais segurança [14].

Para alcançar o objetivo OE1, que tratou da construção do 3SW, foi adaptada a análise de conteúdo proposta por Bardin [41], estruturada em três etapas: Pré-análise, Aplicação dos Critérios e Seleção das Medidas, e Análise dos Resultados. Ao longo da pesquisa, foram aplicados critérios objetivos para filtrar as medidas do CIS Controls v8.1 com potencial de aplicação direta em servidores web. Como resultado, foram selecionadas 93 medidas distribuídas entre 17 dos 18 controles, compondo o Modelo 3SW.

A fim de verificar a efetividade e aplicabilidade do modelo proposto (OE3), foi conduzido um estudo de caso em dois sistemas distintos (OE2), Alpaca com o Modelo 3SW e Lhama com o WAH. Como a aplicação dos modelos foi realizada em sistemas existentes no ambiente de produção, foram criados clones desses e realizado o registro do estado atual para comparativo final. Conforme registrado na Seção 5.1.1, as entidades públicas do executivo federal pertencentes ao SISP, participam de um programa que realiza a implementação das medidas do CIS Controls v8 agrupadas em Ciclos de seis meses (PPSI - Programa de Privacidade e Segurança da Informação). Portanto, o registro do estado atual dos sistemas também considerou as medidas presentes até a finalização do Ciclo 3 do PPSI.

A comparação entre o Modelo 3SW e o WAH, demonstrou que, apesar de ambos compartilharem 61 medidas, ou 40% (61/153) do total de medidas do CIS Controls v8, cada um deles possui medidas exclusivas, respectivamente, de 21% (32/153) e de 19% (29/153) — (32 contra 29) — que representam diferenças significativas na composição dos modelos. Além disso, o 3SW apresentou maior completude por controle nos resultados de implementação: 59% dos controles com medidas atribuídas foram completamente implementados, enquanto no WAH esse número foi de 38%. Isso indica que o 3SW, ao ser mais específico e direcionado, tende a obter resultados mais consistentes em ambientes críticos como os servidores web.

Outro ponto de destaque foi a confirmação, por meio de entrevista, da importância de abordagens mais específicas no contexto da segurança da informação na Administração Pública, podendo o 3SW ser uma "segunda camada de proteção", um complemento relevante às estratégias já existentes, como o PPSI.

Ainda sobre o PPSI, a análise dos dados pré-implementação dos modelos 3SW e WAH, revelaram que nenhuma das 14 medidas com nível de implementação AMT — medida integralmente implementada em mais de 50% ou em todos os ativos — constava como implementada nos sistemas do estudo de caso. Isso

significa que o nível AMT pode comprometer a visibilidade sobre falhas, visto que elas podem não ter sido corrigidas em sua totalidade e esse nível, por ser o último da avaliação do *framework* PPSI, criar a falsa impressão que as ações da medida foram concluídas.

Em termos práticos, a dissertação contribui com uma proposta metodológica clara e replicável, que pode ser adaptada a outros ativos além de servidores web. Além disso, sugere um novo olhar para a aplicação dos CIS Controls na Administração Pública, enfatizando a necessidade de adaptações que considerem o contexto e o ativo protegido.

Em resumo, os objetivos específicos desta pesquisa foram plenamente atendidos, conforme o detalhamento a seguir.

- **OE1: Adaptar as medidas do CIS Controls v8.1 ao contexto de servidores web (4).** O Modelo 3SW foi desenvolvido com 93 medidas, selecionadas com base nos critérios CS1 (relevância técnica), CS2 (individualização) e CS3 (verificabilidade), cobrindo 61% do CIS Controls e 92% das mitigações MITRE ATT&CK (4.1, Tabela 4.3). A priorização por CP1 (escopo do servidor), CP2 (esforço de implementação) e CP3 (esforço de manutenção) garantiu viabilidade prática, com 57% das medidas implementáveis diretamente no servidor e esforço predominantemente moderado (4.2, Tabela 4.2).
- **OE2: Identificar e classificar sistemas críticos (5.2).** A metodologia de classificação (3.2.2.1) identificou 58% dos sistemas da Empresa ALFA como de alta criticidade após ajustes do Gestor de TI, reduzindo o erro de classificação de 21% para 13% com faixas ajustadas (Tabelas 5.3, 5.4). Os sistemas Alpaca e Lhama, ambos de alta criticidade, foram selecionados para o estudo de caso.
- **OE3: Verificar a efetividade da solução proposta (6).** A validação na Empresa ALFA demonstrou que o 3SW atingiu 82% de implementação e 100% de redução de vulnerabilidades no Sistema Alpaca, superando o WAH (74% de implementação, 96% de TRV, 6.1, Tabela 6.6). A triangulação de dados (entrevistas, análise documental e métricas técnicas, 3.2.2.3) confirmou a aplicabilidade e eficácia do 3SW.

## 7.1 CONTRIBUIÇÕES

Em relação às contribuições deste trabalho, elas são destacadas considerando três dimensões: prática, teórica e social. Em relação à contribuição prática, o 3SW é uma solução viável para órgãos públicos, podendo integrar-se à gestão de riscos (Tabela 5.2), ao PPSI e à LGPD. Sua implementação em 39 dias úteis no Sistema Alpaca (5.3) e a eliminação total de vulnerabilidades (Tabela 6.5) demonstram sua aplicabilidade e efetividade, especialmente em contextos que, conforme o TCU [30], impõem a priorização de recursos.

Sobre a contribuição teórica, a adaptação do CIS Controls v8.1 para servidores web, validada academicamente na RISTI [42], complementa *frameworks* como o WAH (4.3) e é comparável a estudos como [133]. A cobertura de 97% das mitigações MITRE ATT&CK (6.1) reforça sua robustez teórica.

Finalmente, quanto à contribuição social, ao proteger servidores web expostos à internet, o 3SW contribui para a segurança de serviços digitais, mitigando riscos como ataques a sistemas externos [108] e promovendo confiança pública na transformação digital [14]. Adicionalmente, o modelo apoia a conformidade com a LGPD ao fortalecer as salvaguardas técnicas exigidas para o tratamento seguro de dados pessoais, especialmente em ambientes governamentais.

## 7.2 LIMITAÇÕES E TRABALHOS FUTUROS

A principal limitação deste trabalho é que o Modelo 3SW foi aplicado em apenas um estudo de caso. Assim, não é possível generalizar os resultados, que refletem principalmente as medidas presentes no PPSI e nos sistemas Alpaca e Lhama. Como trabalho futuro, recomenda-se aplicar o 3SW em outras instituições públicas e privadas, de modo a avaliar sua aderência em diferentes contextos e cenários.

Outra limitação do modelo é sua restrição a um único ativo crítico: servidores web. Estudos futuros podem ampliar a abordagem para outros ativos, como bancos de dados, dispositivos de rede ou aplicações móveis, criando metodologias específicas de seleção e priorização para cada tipo de ativo.

No que diz respeito ao *framework* CIS Controls, que serve de base para o 3SW, identificou-se uma abordagem superficial em temas críticos para servidores web, como modelagem de ameaças alinhada aos riscos de negócio (Medida 16.14) e segurança de APIs (Medida 18.1). Trabalhos futuros podem integrar metodologias de identificação de riscos de negócio [146] com técnicas de modelagem de ameaças (por exemplo, STRIDE [147]) e *frameworks* especializados (por exemplo, OWASP API Security Top 10 [148]), a fim de priorizar controles que mitiguem ameaças de aplicação com impacto direto nos objetivos organizacionais.

Além disso, as medidas do 3SW, embora relevantes, exigem esforço moderado para implementação. Uma evolução natural seria a automação dessas medidas, integrando-as a ferramentas de varredura e monitoramento contínuo, conforme sugerido pelas medidas 7.3 e 7.4 do CIS Controls v8.1 (6.7). Esse processo deve incluir mecanismos de *backup* e *snapshots* para garantir a restauração em caso de falhas. Também seria interessante desenvolver ferramentas de suporte que rastreiem mitigações do MITRE ATT&CK e consolidem uma base de conhecimento para o gerenciamento de ameaças.

Por fim, destaca-se a necessidade de reavaliar e aprimorar as escalas de avaliação atualmente utilizadas em programas como o PPSI, tornando-as mais granulares, rastreáveis e úteis para apoiar a tomada de decisão.

# REFERÊNCIAS BIBLIOGRÁFICAS


1 MITRE ATT&CK. *Enterprise Mitigations*. 2020. Disponível em: <https://attack.mitre.org/versions/v8/mitigations/enterprise/>.

2 CENTER FOR INTERNET SECURITY (CIS). *The 18 CIS Critical Security Controls*. 2024. Disponível em: <https://www.cisecurity.org/controls/cis-controls-list>.

3 BRASIL. *Guia do Framework de privacidade e Segurança da Informação. Programa de Privacidade e Segurança da Informação (PPSI)*. Brasília, DF: Ministério da Gestão e da Inovação em Serviços Públicos, 2024. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf>.

4 CENTER FOR INTERNET SECURITY (CIS). *CIS Community Defense Model 2.0*. 2021. Disponível em: <https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2.0>.

5 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Measurement Guide for Information Security*. 2024. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-55v1.pdf>.

6 BRASIL. PRESIDÊNCIA DA REPÚBLICA. *Legislação — Gabinete de Segurança Institucional*. 2025. Disponível em: <https://www.gov.br/gsi/pt-br/ssic/legislacao>.

7 BANCO CENTRAL DO BRASIL. *Estatísticas do Pix*. 2024. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/estatisticasPix>.

8 INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. *Estimativas da população residente no Brasil e unidades da federação com data de referência em 1º de julho de 2024*. 2024. Disponível em: <https://ftp.ibge.gov.br/Estimativas_de_Populacao/Estimativas_2024/POP2024_20241230.pdf>.

9 COMITÊ GESTOR DA INTERNET NO BRASIL. *Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2023*. 2024. Disponível em: <https://cetic.br/media/docs/publicacoes/2/20241104102822/tic_domicilios_2023_livro_eletronico.pdf>.

10 BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. *Painel de monitoramento de serviços federais — Governo Digital*. 2024. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/transformacao-digital/central-de-qualidade/painel-de-monitoramento-de-servicos-federaisv2>.

11 BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. *Painel de Raio-X da Administração*. 2024. Disponível em: <https://raiox.economia.gov.br>.

12 BRASIL. Ministério da Economia. *GOV.BR já oferece 4 mil serviços públicos digitais para o cidadão*. 2022. Disponível em: <https://www.gov.br/governodigital/pt-br/noticias/gov-br-ja-oferece-4-mil-servicos-publicos-digitais-para-o-cidadao>.

13 BRASIL. *Decreto nº 9.756, de 11 de abril de 2019*: Institui o portal único “gov.br” e dispõe sobre as regras de unificação dos canais digitais do governo federal. Brasília, DF: Presidência da República, 2019. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9756.htm>.

14 BRASIL. *Decreto n. 12.198, de 24 de setembro de 2024*: Institui a estratégia federal de governo digital para o período de 2024 a 2027 e a infraestrutura nacional de dados. Brasília, DF: Presidência da República, 2024. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/decreto/D12198.htm>.

15 OECD. *2023 OECD Digital Government Index: Results and key findings*. Paris: OECD Publishing, 2024.

16 WORLD BANK. *2022 GovTech Maturity Index (GTMI) - Central Government*. 2022. Disponível em: <https://datacatalogfiles.worldbank.org/ddh-published/0037889/DR0091192/WBG_GovTech%20Dataset_Mar2023.xlsx>.

17 PODER360. *Brasil é 2º em ranking de governo digital do Banco Mundial*. 2022. Disponível em <https://www.poder360.com.br/internacional/brasil-e-2o-lugar-em-ranking-de-governo-digital-do-banco-mundial/>.

18 BRASIL. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Brasília, DF: Presidência da República, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>.

19 BRASIL. Superior Tribunal de Justiça. *Comunicado da Presidência do STJ*. 2020. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/19112020-Comunicado-da-Presidencia-do-STJ.aspx>.

20 BRASIL. Ministério da Saúde. *Ministério da Saúde anuncia restabelecimento total dos sistemas afetados por ataque hacker*. 2022. Disponível em: <https://www.gov.br/saude/pt-br/assuntos/noticias/2022/janeiro/ministerio-da-saude-anuncia-restabelecimento-total-dos-sistemas-afetados-por-ataque-hacker>.

21 BRASIL. *Constituição da República Federativa do Brasil de 1988: Artigo 71*. Presidência da República, 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>.

22 METRÓPOLES. *Ataques de ransomware aumentaram 90% entre 2020 e 2021*. 2021. Disponível em: <https://www.metropoles.com/dino/ataques-de-ransomware-aumentaram-90-entre-2020-e-2021>.

23 VERIZON. *2022 Data Breach Investigations Report (DBIR)*. 2022. Disponível em: <https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf>.

24 VERIZON. *2023 Data Breach Investigations Report (DBIR)*. 2023. Disponível em: <https://www.verizon.com/business/resources/reports/2023/dbir/2023-data-breach-investigations-report-dbir.pdf>.

25 BRASIL. *Gabinete de Segurança Institucional da Presidência da República (GSI/PR)*. Presidência da República, 2024. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/gsi>.

26 JUMA, A. H.; ARMAN, A. A.; HIDAYAT, F. Cybersecurity assessment framework: A systematic review. *IEEE*, p. 1–6, set. 2023. Disponível em: <http://dx.doi.org/10.1109/ICISS59129.2023.10291832>.

27 INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27000 family. Information security management*. 2025. Disponível em: <https://www.iso.org/standard/iso-iec-27000-family>.

28 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Search CSRC*. 2025. Disponível em: <https://csrc.nist.gov/publications/sp>.

29 CROTTY, J.; DANIEL, E. Lessons from practice: insights on cybersecurity strategy for business leaders, from smes to global enterprises. *Open University*, 2021.

30 BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. *Acórdão n. 2387/2024. Plenário. Relator: Ministro Augusto Nardes. Sessão de 06/11/2024*. 2024. Disponível em: <https://pesquisa.apps.tcu.gov.br/redireciona/acordao-completo/ACORDAO-COMPLETO-2686174>.

31 BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. *Acórdão nº 1768/2022. Plenário. Relator: Ministro Vital do Rêgo. Sessão de 03/08/2022*. 2022. Disponível em: <https://pesquisa.apps.tcu.gov.br/redireciona/acordao-completo/ACORDAO-COMPLETO-2535414>.

32 BRASIL. PRESIDÊNCIA DA REPÚBLICA. *Visão Geral — CTIR Gov - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo*. 2025. Disponível em: <https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros>.

33 O GLOBO. *Vulnerabilidade virtual: número de ataques cibernéticos contra o governo aumenta; TCU vê risco de vazamento*. Rio de Janeiro, Brasil: [s.n.], 2025. Disponível em: <https://oglobo.globo.com/brasil/noticia/2024/03/01/ataques-ciberneticos-contra-orgaos-do-governo-federal-crescem-em-janeiro-puxados-por-vazamentos-de-dados.ghtml>.

34 TÁCITO, C. O princípio de legalidade: Ponto e contraponto. *Revista de direito administrativo*, v. 206, p. 1–8, 1996.

35 BRASIL. Ministério da Saúde. Coordenação-Geral de Atos Normativos. *Manual de elaboração de atos normativos*. Brasília, DF, Brasil: [s.n.], 2023. Disponível em: <https://bvsms.saude.gov.br/bvs/publicacoes/manual_elaboracao_atos_normativos.pdf>.

36 BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. *Acórdão n. 1233/2012. Plenário. Relator: Ministro Aroldo Cedraz. Sessão de 23/05/2012*. 2012. Disponível em: <https://pesquisa.apps.tcu.gov.br/redireciona/acordao-completo/ACORDAO-COMPLETO-1233850>.

37 BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. *Matriz de Riscos e Controles para serviços de hospedagem Web, e-mail e DNS*. 2024. Disponível em: <https://portal.tcu.gov.br/data/files/B2/F6/D8/64/13CB39100FB48339F18818A8/Matriz\%20de\%20risco\%20e\%20Controles\%20para\%20servicos\%20de\%20hospedagem\%20WEB_\%20e-mail\%20e\%20DNS_WEB.pdf>.

38 BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. *Cinco controles de segurança cibernética para ontem*. 2022. Disponível em: <https://portal.tcu.gov.br/data/files/4D/E3/DF/81/8C0848102DFE0FF7F18818A8/__5\%20Controles\%20de\%20seguranAa\%20cibernAtica\%20para\%20ontem_final_web.pdf>.

39 BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. *Guias e Modelos — Governo Digital*. 2025. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos>.

40 BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. *Acórdão n. 1109/2021. Plenário. Relator: Ministro Vital do Rêgo. Sessão de 12/05/2021*. 2021. Disponível em: <https://pesquisa.apps.tcu.gov.br/redireciona/acordao-completo/ACORDAO-COMPLETO-2473503>.

41 BARDIN, L. *Análise de Conteúdo*. São Paulo: Edições 70, 2016. v. 1.

42 SILVA, T.; MENDES, F. 3sw: Um conjunto de medidas de segurança para mitigar vulnerabilidades em servidores web. *Revista Ibérica de Sistemas e Tecnologias de Informação*, Associação Ibérica de Sistemas e Tecnologias de Informacao, n. 56, p. 66–81, 2024.

43 HAI, T. N.; VAN, Q. N.; TUYET, M. N. T. Digital transformation: Opportunities and challenges for leaders in the emerging countries in response to covid-19 pandemic. *Emerging Science Journal*, v. 5, n. 1, p. 21–36, 2021.

44 MATT, C.; HESS, T.; BENLIAN, A. Digital transformation strategies. *Business & information systems engineering*, Springer, v. 57, p. 339–343, 2015.

45 ALBERTIN, A. L.; ALBERTIN, R. M. de M. Transformação digital: gerando valor para o "novo futuro". *GV-EXECUTIVO*, v. 20, n. 1, p. 26–29, mar. 2021. Disponível em: <https://periodicos.fgv.br/gvexecutivo/article/view/83455>.

46 MERGEL, I.; EDELMANN, N.; HAUG, N. Defining digital transformation: Results from expert interviews. *Government information quarterly*, Elsevier, v. 36, n. 4, p. 101385, 2019.

47 DIAS, I.; REINHARD, N. Categorization of e-gov initiatives: a comparison of three perspectives. In: *X Congreso Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública*. [S.l.: s.n.], 2005. p. 18–21.

48 VIANA, A. C. A. Transformação digital na administração pública: do governo eletrônico ao governo digital. *International Journal of Digital Law*, v. 2, n. 1, p. 29–46, 2021.

49 MESQUITA, K. A evolução do governo eletrônico no brasil e a contribuição das tic na redefinição das relações entre governo e sociedade. *Comunicologia-Revista de Comunicação da Universidade Católica de Brasília*, p. 174–195, 2019.

50 BRASIL. *Decreto n. 10.332, de 28 de abril de 2020*: Institui a estratégia de governo digital para o período de 2020 a 2022. Brasília, DF: Presidência da República, 2020. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10332.htm>.

51 ALBUQUERQUE, M. R. de; COSTA, L. Transformação digital no setor público: tendências e implicações. *Revista de Gestão e Secretariado*, v. 16, n. 3, p. e4771–e4771, 2025.

52 DUMITRACHE, M.; STăNESCU, A. C.; PARASCHIV, E.-A. Digitalizarea și inteligența artificială în aplicațiile de e-guvernare. *Romanian Journal of Information Technology and Automatic Control*, v. 33, n. 3, p. 43–54, 2023.

53 BRASIL. Ministério da Economia. *Governo ultrapassa os 600 serviços transformados em digitais em 15 meses — Governo Digital*. 2020. Disponível em: <https://www.gov.br/governodigitalvideos/pt-br/noticias/governo-ultrapassa-os-600-servicos-transformados-em-digitais-em-15-meses>.

54 BAJRALIU, A.; QORRAJ, G. Digital transformation's impact on sustainable hr management: Comparative study of work-life balance and skill development in public versus private sectors of a developing country. *Public Policy and Administration*, v. 22, n. 3, p. 358–369, 2023.

55 SANTOS, A. V.; FONSECA, P. G. Transformação digital no serviço público brasileiro: uma revisão sistemática de literatura. *Revista Formadores*, v. 15, n. 1, 2022.

56 BRASIL. *Decreto nº 11.676, de 30 de agosto de 2023*: Aprova a estrutura regimental e o quadro demonstrativo dos cargos em comissão do gabinete de segurança institucional. Brasília, DF: Presidência da República, 2023. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11676.htm>.

57 BRASIL. *Decreto nº 12.102, de 08 de julho de 2024*: Aprova a estrutura regimental do ministério da gestão e da inovação em serviços públicos. Brasília, DF: Presidência da República, 2024. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/Decreto/D12102.htm>.

58 GOVERNO FEDERAL DO BRASIL. *Órgãos*. 2025. Disponível em: <https://www.gov.br/pt-br/orgaos>.

59 GOVERNO FEDERAL DO BRASIL. *Servidores e pensionistas*. 2025. Disponível em: <https://portaldatransparencia.gov.br/servidores>.

60 BRASIL. *Decreto nº 9.637, de 26 de dezembro de 2018*: Institui a política nacional de segurança da informação. Brasília, DF: Presidência da República, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm>.

61 CRAVO, V. C. *Em busca de uma estratégia nacional de segurança cibernética*: Marco legal e autoridade nacional de segurança cibernética. Tese (Doutorado) — Universidade Federal do Rio Grande do Sul, 2023.

62 BRASIL. *Decreto nº 11.856, de 26 de dezembro de 2023*: Institui a política nacional de cibersegurança e o comitê nacional de cibersegurança. Brasília, DF: Presidência da República, 2023. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm>.

63 SANTOS, C. S. A. d.; GAVIãO, L. O.; OLIVEIRA, L. A. d. S.; PEREIRA, J. C. Proposta de avaliação da política nacional de segurança da informação por processo de análise hierárquica. *Perspectivas em Ciência da Informação*, SciELO Brasil, v. 27, n. 4, p. 108–145, 2022.

64 BRASIL. *Decreto nº 10.222, de 05 de fevereiro de 2020*: Aprova a estratégia nacional de segurança cibernética. Brasília, DF: Presidência da República, 2020. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm>.

65 PINTO, D. J. A.; GRASSI, J. M. Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do brasil. *Revista Brasileira de Estudos de Defesa*, v. 7, n. 2, 2020.

66 BRASIL. *Portaria nº 852, de 08 de março de 2023*: Dispõe sobre o programa de privacidade e segurança da informação - ppsi. Brasília, DF: Ministério da Gestão e da Inovação em Serviços Públicos, 2023. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908>.

67 TOMAZ, L. B. P.; OLIVEIRA, P. A. de; GUALBERTO, E. S. Investigação da ferramenta keycloak na mitigação de incidentes cibernéticos: Uma abordagem integrada com o programa de privacidade e segurança da informação (ppsi). In: SBC. *Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)*. [S.l.], 2024. p. 201–204.

68 GOLDONI, L. R. F.; RODRIGUES, K. F.; MEDEIROS, B. P. Qual é o futuro da governança de cibersegurança no brasil? *Cadernos Gestão Pública e Cidadania*, SciELO Brasil, v. 29, p. e90972, 2024.

69 BRUSTOLIN, V.; NUNES, I. A.; ASSUNçãO, J. Z. de. Análise estrutural das estratégias de segurança cibernética do brasil e dos estados unidos. *Revista Brasileira de Estudos de Defesa*, v. 9, n. 2, 2022.

70 GEORG, M. A. C.; RODRIGUES, W. M. S.; ALVES, C. A. de M.; JúNIOR, A. S.; NUNES, R. R. *Os desafios da Segurança Cibernética no setor público federal do Brasil*: Estudo sob a ótica de gestores de tecnologia da informação. 2023.

71 GOVERNO FEDERAL DO BRASIL. *Órgãos do SISP*. 2025. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/sisp/sobre-o-sisp/orgaos-do-sisp>.

72 BELLI, L.; FRANQUEIRA, B.; BAKONYI, E.; CHEN, L.; COUTO, N. D.; CHANG, S.; HORA, N. da; GASPAR, W. B. Cybersecurity: A systemic vision towards a proposal for a regulatory framework for a digitally sovereign brazil. *Dados Internacionais de Catalogação na Publicação (CIP)*, 2023.

73 BUOGO, M.; FACHINELLI, A. C.; GIACOMELLO, C. P. Gestão do conhecimento e segurança da informação. *Revista AtoZ*, v. 8, n. 2, p. 39–59, 2019.

74 PRESTES, M. V. P.; BONINI, D. M. S.; MELO, F. C. de; BASTOS, M.; BONINI, J. S.; SILVA, W. C. F. N. da. Lei geral de proteção de dados n° 13.709/2018: Apontamentos sobre sua contextualização como marco legal no brasil. *Research, Society and Development*, v. 10, n. 12, p. e568101220906–e568101220906, 2021.

75 COMMISSION, E. *Regulation (EU) 2016/679 of the European Parliament and of the Council*. Official Journal of the European Union, 2016. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>.

76 GARRIDO, P. P. *Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD)*. São Paulo: Editora Saraiva, 2023. v. 4.

77 GOVERNO DIGITAL. *Privacidade e Segurança*. 2025. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca>.

78 BRASIL. *Guia de Boas Práticas para Implementação na Administração Pública Federal*. Brasília, DF: Ministério da Economia, 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf>.

79 BRASIL. *Guia do Framework de Segurança*. Brasília, DF: Ministério da Economia, 2021. Disponível em: <https://www.legiscompliance.com.br/images/pdf/GuiadoFrameworkdeSegurana.pdf>.

80 BRASIL. *Guia de Avaliação de Riscos de Segurança e Privacidade*. Brasília, DF: Ministério da Economia, 2020. Disponível em: <https://www.lgpd.ms.gov.br/wp-content/uploads/2024/02/Guia-de-Avaliacao-de-Riscos-CGU-2021.pdf>.

81 ZOTTMANN, C. E. M.; GEORG, M. A. C.; ALVES, R. S.; SILVA, M. A. da; NUNES, R. R. Proposta de metodologia para avaliação de riscos de privacidade para Órgãos do poder judiciário no brasil. *ENAJUS*, 2023.

82 FARIAS, L. *Guia Definitivo: Diferenças entre Normas Técnicas, Frameworks, Leis e Regulamentações*. Agência de Conformidade e Proteção de Dados, 2024. Disponível em: <https://www.acpdbrasil.com/guia-definitivo-diferencas-entre-normas-tecnicas-frameworks-leis-e-regulamentacoes/>.

83 SILVA, D. A. d.; SILVA, J. A. d.; ALVES, G. d. F.; SANTOS, C. D. d. Gestão de riscos no setor público: revisão bibliométrica e proposta de agenda de pesquisa. *Escola Nacional de Administração Pública (Enap)*, 2021.

84 BRASIL. Presidência da República. *Instrução Normativa Conjunta CGU/MP nº 1, de 10 de maio de 2016*: Dispõe sobre controles internos, gestão de riscos e governança no âmbito do poderexecutivo federal. 2016. Disponível em: <https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/21519355/do1-2016-05-11-instrucao-normativa-conjunta-n-1-de-10-de-maio-de-2016-21519197>.

85 SILVA, D. E. L. d. S.; ARAÚJO, S. L. E.; CAMPELLO, L. d. O. S. Gestão de riscos: o método do coso aplicado à gestão de uma unidade de informa ção. *RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação*, SciELO Brasil, v. 18, p. e020021, 2020.

86 BRASIL. *Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão do Ministério do Planejamento, Desenvolvimento e Gestão GIRC – M*. Brasília, DF: Ministério do Planejamento, 2017. Disponível em: <https://repositorio.cgu.gov.br/bitstream/1/74041/1/Manual_de_GIRC_Versao_2.pdf>.

87 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *Norma NBR ISO 31000. Gestão de riscos — Diretrizes*. Rio de Janeiro, RJ, Brasil: ABNT, 2018.

88 THE INSTITUTE OF INTERNAL AUDITORS. *The IIA's Three Lines Model*. Lake Mary, USA: The IIA, 2020. Disponível em: <https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf>.

89 ARAÚJO, V. S.; SANTOS, B. d. B. A. d.; XAVIER, L. V. Compliance na administração pública brasileira. *A&C-Revista de Direito Administrativo & Constitucional*, v. 19, n. 77, p. 247–272, 2019.

90 KUUSISTO, M. Organizational effects of digitalization: A literature review. *International Journal of Organization Theory and Behavior*, Emerald Publishing Limited, v. 20, n. 3, p. 341–362, 2017.

91 FADZISO, T.; THADURI, U.; DEKKATI, S.; BALLAMUDI, V.; DESAMSETTI, H. Evolution of the cyber security threat: An overview of the scale of cyber threat. *Digitalization & Sustainability Review*, v. 3, n. 1, p. 1–12, 2023.

92 CHAKKARAVARTHY, S. S.; SANGEETHA, D.; RATHNAM, M. V.; SRINITHI, K.; VAIDEHI, V. Futuristic cyber-attacks. *International Journal of Knowledge-based and Intelligent Engineering Systems*, SAGE Publications, v. 22, n. 3, p. 195–204, 2018.

93 GREEN, P. E. *Enterprise risk management: A common framework for the entire organization*. [S.l.]: Butterworth-Heinemann, 2015.

94 CEBULA, J. J.; YOUNG, L. R. A taxonomy of operational cyber security risks. *Software Engineering Institute, Carnegie Mellon University*, Citeseer, 2010.

95 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *The NIST Cybersecurity Framework (CSF) 2.0*. 2024. Disponível em: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>.

96 KWEON, E.; LEE, H.; CHAI, S.; YOO, K. The utility of information security training and education on cybersecurity incidents: An empirical evidence. *Information Systems Frontiers*, Springer, v. 23, p. 361–373, 2021.

97 SOLMS, R. V.; NIEKERK, J. V. From information security to cyber security. *Computers & Security*, Elsevier, v. 38, p. 97–102, 2013.

98 STRUPCZEWSKI, G. Defining cyber risk. *Safety Science*, Elsevier, v. 135, p. 105143, 2021.

99 ELING, M.; MCSHANE, M.; NGUYEN, T. Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, Wiley Online Library, v. 24, n. 1, p. 93–125, 2021.

100 IBM. *Cost of a Data Breach Report 2024*. 2024. Disponível em: <https://www.ibm.com/reports/data-breach>.

101 CHEN, Q.; BRIDGES, R. A. Automated behavioral analysis of malware: A case study of wannacry ransomware. In: IEEE. *2017 16th IEEE International Conference on machine learning and applications (ICMLA)*. [S.l.], 2017. p. 454–460.

102 ALAWIDA, M.; OMOLARA, A. E.; ABIODUN, O. I.; AL-RAJAB, M. A deeper look into cybersecurity issues in the wake of covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, v. 34, n. 10, Part A, p. 8176–8206, 2022. ISSN 1319-1578. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1319157822002762>.

103 ALQUDHAIBI, A.; KRISHNA, A.; JAGTAP, S.; WILLIAMS, N.; AFY-SHARARAH, M.; SALONITIS, K. Cybersecurity 4.0: safeguarding trust and production in the digital food industry era. *Discover Food*, Springer, v. 4, n. 1, p. 2, 2024.

104 GHANBARI, H.; KOSKINEN, K. When data breach hits a psychotherapy clinic: The vastaamo case. *Journal of Information Technology Teaching Cases*, 2024. Disponível em: <https://doi.org/10.1177/20438869241258235>.

105 MOORE, G.; KHURSHID, Z.; MCDONNELL, T.; ROGERS, L.; HEALY, O. A resilient workforce: patient safety and the workforce response to a cyber-attack on the ict systems of the national health service in ireland. *BMC Health Services Research*, Springer, v. 23, n. 1, p. 1112, 2023.

106 BERCI, L.; LANNES, Y. N. da C.; STEFANELLI, S. A responsabilidade civil do poder judiciário frente aos vazamento de dados dos tribunais sob a óptica da lei geral de proteção de dados. *Revista Direito & Paz*, v. 1, n. 48, p. 4–18, 2023.

107 LEMES, D. Lei geral de proteção de dados pessoais (lgpd): O setor público e vazamentos de dados pessoais. *Revista Eixo*, v. 12, n. 2, p. 109–118, 2023. Disponível em: <https://arquivorevistaeixo.ifb.edu.br/index.php/RevistaEixo/article/view/1089>.

108 BRASIL. *Ataque cibernético contra sistemas do Governo Federal será apurado pela PF*. 2024. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias/ataque-cibernetico-contra-sistemas-do-governo-federal-sera-apurado-pela-pf>.

109 CNN BRASIL. *Entenda o sistema de informações do governo que pode ter sofrido ataque hacker*. 2024. Disponível em: <https://www.cnnbrasil.com.br/politica/entenda-o-sistema-de-informacoes-do-governo-que-pode-ter-sofrido-ataque-hacker/>.

110 VEJA. *Sistema digital do governo é restaurado uma semana após ataque hacker*. 2024. Disponível em: <https://veja.abril.com.br/coluna/maquiavel/sistema-digital-do-governo-e-restaurado-uma-semana-apos-ataque-hacker>.

111 STROM, B. E.; APPLEBAUM, A.; MILLER, D. P.; NICKELS, K. C.; PENNINGTON, A. G.; THOMAS, C. B. *MITRE ATT&CK: Design and Philosophy*. The MITRE Corporation, 2020. Originally published July 2018; Revised March 2020. Disponível em: <https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf>.

112 GEORGIADOU, A.; MOUZAKITIS, S.; ASKOUNIS, D. Assessing mitre att&ck risk using a cyber-security culture framework. *Sensors*, MDPI, v. 21, n. 9, p. 3267, 2021.

113 MITRE. *MITRE ATT&CK*. 2025. Disponível em: <https://attack.mitre.org/resources/versions/>.

114 STROM, B. E. *ATT&CK 101*. 2018. Disponível em: <https://medium.com/mitre-attack/att-ck-101-17074d3bc62>.

115 IBM. *Usando o arquivo /etc/passwd*. 2025. Disponível em: <https://www.ibm.com/docs/pt-br/aix/7.2.0?topic=passwords-using-etcpasswd-file>.

116 NEGUS, C. *Linux Bible*: Operating system. [S.l.]: Wiley, 2020.

117 COMMONS, C. *Legal Code - Attribution-NonCommercial-NoDerivatives 4.0 International - Creative Commons*. 2025. Disponível em: <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.en>.

118 FERDOUS, J.; ISLAM, R.; MAHBOUBI, A.; ISLAM, M. Z. A review of state-of-the-art malware attack trends and defense mechanisms. *IEEE Access*, 2023.

119 VERIZON. *2020 Data Breach Investigations Report (DBIR)*. 2020. Disponível em: <https://www.verizon.com/business/resources/reports/2020-data-breach-investigations-report.pdf>.

120 DOMíNGUEZ-DORADO, M.; CARMONA-MURILLO, J.; CORTéS-POLO, D.; RODRíGUEZ-PéREZ, F. J. Cybertomp: A novel systematic framework to manage asset-focused cybersecurity from tactical and operational levels. *IEEE Access*, IEEE, v. 10, p. 122454–122485, 2022.

121 ALVES, R.; SILVA, J.; JUNIOR, L. R.; NUNES, R. Enhancing cybersecurity in the judiciary: Integrating additional controls into the cis framework. *Computers & Security*, 2025.

122 BASHOFI, I.; SALMAN, M. Cybersecurity maturity assessment design using nistcsf, cis controls v8 and iso/iec 27002. In: IEEE. *2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom)*. [S.l.], 2022. p. 58–62.

123 HORTA, A.; HOLANDA, R.; MARINHO, R. A multi-criteria approach to improve the cyber security visibility through breach attack simulations. In: SBC. *Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)*. [S.l.], 2022. p. 330–343.

124 GONZALEZ-GRANADILLO, G.; MENESIDOU, S. A.; PAPAMARTZIVANOS, D.; ROMEU, R.; NAVARRO-LLOBET, D.; OKOH, C.; NIFAKOS, S.; XENAKIS, C.; PANAOUSIS, E. Automated cyber and privacy risk management toolkit. *Sensors*, MDPI, v. 21, n. 16, p. 5493, 2021.

125 RAHMAN, M. R.; WILLIAMS, L. An investigation of security controls and mitre att&ck techniques. *arXiv preprint arXiv:2211.06500*, 2022.

126 KERN, M.; LANDAUER, M.; SKOPIK, F.; WEIPPL, E. A logging maturity and decision model for the selection of intrusion detection cyber security solutions. *Computers & Security*, Elsevier, v. 141, p. 103844, 2024.

127 SKOPIK, F.; LANDAUER, M.; WURZENBERGER, M. Blind spots of security monitoring in enterprise infrastructures: A survey. *IEEE Security & Privacy*, v. 20, n. 6, p. 18–26, 2022.

128 CUE, H. A. A.; BOURLAI, T.; LUPO, M. A cis controls v8. 0 scoring system using combined ranking-weight methods. In: IEEE. *2024 IEEE International Systems Conference (SysCon)*. [S.l.], 2024. p. 1–8.

129 ABOHATEM, A. Y.; BA-ALWI, F. M. Cybersecurity maturity assessment of information systems for yemen telecoms. *International Journal of Intelligent Systems and Applications in Engineering*, v. 12, n. 8s, p. 539–548, 2023. Disponível em: <https://ijisae.org/index.php/IJISAE/article/view/4185>.

130 AL-HAWAMLEH, A. Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. *International Journal of Computing and Digital Systems*, University of Bahrain, v. 15, n. 1, p. 1315–1331, 2024.

131 CARíAS, J. F.; ARRIZABALAGA, S.; LABAKA, L.; HERNANTES, J. Cyber resilience progression model. *Applied Sciences*, MDPI, v. 10, n. 21, p. 7393, 2020.

132 CENTER FOR INTERNET SECURITY (CIS). *CIS Critical Security Controls® v8.1 Industrial Control Systems (ICS) Guide*. 2024. Disponível em: <https://www.cisecurity.org/insights/white-papers/cis-critical-security-controls-v8-1-industrial-control-systems-ics-guide>.

133 DISANAYAKE, C.; DILHARA, B.; DHARMARATNA, N. Rationalized security frameworks for web applications. *ACCELERATING SOCIETAL CHANGE THROUGH DIGITAL TRANSFORMATION*, p. 532, 2023.

134 SONG, L.; GARCíA-VALLS, M. Improving security of web servers in critical iot systems through self-monitoring of vulnerabilities. *Sensors*, MDPI, v. 22, n. 13, p. 5004, 2022.

135 FADLIL, A.; RIADI, I.; MU'MIN, M. Mitigation from sql injection attacks on web server using open web application security project framework. *International Journal of Engineering*, v. 37, n. 4, p. 635–645, 2024.

136 YIN, R. K. Planejamento e métodos. *Trad. Cristhian Matheus Herrera*, v. 5, 2015.

137 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Web Server - Glossary | CSRC*. 2025. Disponível em: <https://csrc.nist.gov/glossary/term/web_server>.

138 GIL, A. C. *Como elaborar projetos de pesquisa*. São Paulo: Editora Atlas, 2023. v. 7.

139 RUNESON, P.; HöST, M. Guidelines for conducting and reporting case study research in software engineering. *Empirical software engineering*, Springer, v. 14, p. 131–164, 2009.

140 TéCNICAS, A. B. de N. *Norma NBR ISO 27005. Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação*. Rio de Janeiro, RJ, Brasil: ABNT, 2023.

141 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Guide for Conducting Risk Assessments*. 2012. Disponível em: <https://csrc.nist.gov/pubs/sp/800/30/r1/final>.

142 YEE, C. K.; ZOLKIPLI, M. F. Review on confidentiality, integrity and availability in information security. *Journal of ICT in Education*, v. 8, n. 2, p. 34–42, 2021.

143 SILVA, T.; MENDES, F. *CIS Controls v8 para servidores web*. Zenodo, 2024. Disponível em: <https://doi.org/10.5281/zenodo.14175601>.

144 MOHAMMED, Z. Data breach recovery areas: an exploration of organization's recovery strategies for surviving data breaches. *Organizational Cybersecurity Journal: Practice, Process and People*, Emerald Publishing Limited, v. 2, n. 1, p. 41–59, 2022.

145 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Incident Response Recommendations and Considerations for Cybersecurity Risk Management*. 2025. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf>.

146 ALVES, R. S.; GEORG, M. A. C.; NUNES, R. R. Judiciário sob ataque hacker: riscos de negócio para segurança cibernética em tribunais brasileiros. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 2023. Disponível em: <https://zenodo.org/record/8032915>.

147 MICROSOFT. *Ameaças - Microsoft Threat Modeling Tool - Azure | Microsoft Learn*. 2023. Disponível em: <https://learn.microsoft.com/pt-br/azure/security/develop/threat-modeling-tool-threats>.

148 OWASP. *OWASP Top 10 API Security Risks – 2023 - OWASP API Security Top 10*. 2023. Disponível em: <https://owasp.org/API-Security/editions/2023/en/0x11-t10/>.

# APÊNDICES

# TABELA DE MITIGAÇÕES DO MITRE ATT&CK FOR ENTERPRISE

Este apêndice apresenta as 42 mitigações documentadas na versão 8.2 do MITRE ATT&CK for Enterprise, conforme mencionado na Seção 2.6.1. A Tabela A.1 lista os identificadores (ID), os nomes e as descrições de cada mitigação, fornecendo uma visão geral das medidas que podem ser adotadas para reduzir o impacto de técnicas e táticas utilizadas por agentes maliciosos.

Tabela A.1: Tabela de Mitigações do MITRE ATT&CK for Enterprise (com tradução)

| ID | Nome | Descrição |
|---|---|---|
| M1013 | Guia para Desenvolvedores de Aplicativos | Forneça orientações ou treinamentos aos desenvolvedores para evitar a introdução de fragilidades que possam ser exploradas por agentes mal-intencionados. |
| M1015 | Configuração do Active Directory | Configure o Active Directory para prevenir o uso de certas técnicas; utilize SID Filtering, entre outros. |
| M1016 | Verificação de Vulnerabilidades | Realize varreduras periódicas para identificar vulnerabilidades exploráveis e corrigi-las. |
| M1017 | Treinamento do Usuário | Treine os usuários para que reconheçam tentativas de acesso ou manipulação por agentes mal-intencionados, reduzindo riscos de phishing e engenharia social. |
| M1018 | Gerenciamento de Contas de Usuário | Gerencie a criação, modificação, uso e permissões das contas de usuários. |
| M1019 | Programa de Inteligência contra Ameaças | Implemente um programa de inteligência de ameaças para gerar informações próprias e monitorar tendências, orientando prioridades defensivas. |
| M1020 | Inspeção SSL/TLS | Intercepte e inspecione sessões SSL/TLS para analisar tráfego web criptografado em busca de atividades maliciosas. |
| M1021 | Restringir Conteúdo Web | Restrinja acesso a determinados sites, downloads, anexos, scripts (como JavaScript) e extensões de navegador. |
| M1022 | Restringir Permissões de Arquivos e Diretórios | Aplique permissões restritivas em arquivos e diretórios para limitar o acesso a usuários não autorizados. |
| M1024 | Restringir Permissões no Registro | Restringe a capacidade de modificar chaves e hives específicos no Registro do Windows. |
| M1025 | Integridade de Processos Privilegiados | Proteja processos de alto privilégio contra interferências utilizando recursos como Protected Process Light e defesas contra injeção de processos. |
| M1026 | Gerenciamento de Contas Privilegiadas | Gerencie criação, modificação, uso e permissões de contas privilegiadas, como SYSTEM ou root. |
| M1027 | Políticas de Senhas | Defina e aplique políticas seguras de senhas para todas as contas. |
| M1028 | Configuração do Sistema Operacional | Realize ajustes de configuração no sistema operacional para aumentar sua segurança contra técnicas de ataque. |

| | | |
|---|---|---|
| M1029 | Armazenamento Remoto de Dados | Utilize armazenamento remoto para logs e arquivos sensíveis, garantindo melhor controle de acesso e proteção contra exposição. |
| M1030 | Segmentação de Rede | Estruture a rede para isolar sistemas e recursos críticos, utilizando segmentação física ou lógica, além de DMZs e VPCs na nuvem. |
| M1031 | Prevenção de Intrusão na Rede | Utilize assinaturas de detecção para bloquear tráfego suspeito nos limites da rede. |
| M1032 | Autenticação Multifator | Utilize dois ou mais fatores para autenticação, como senha e token físico ou gerador de código. |
| M1033 | Limitar Instalação de Software | Bloqueie usuários ou grupos de instalar softwares não autorizados. |
| M1034 | Limitar Instalação de Hardware | Bloqueie usuários ou grupos de instalar ou utilizar hardware não aprovado, como dispositivos USB. |
| M1035 | Limitar Acesso a Recursos pela Rede | Previna o acesso a compartilhamentos, serviços remotos e outros recursos não necessários, utilizando concentradores de rede, gateways RDP, entre outros. |
| M1036 | Políticas de Uso de Conta | Configure recursos relacionados ao uso de contas, como bloqueio após tentativas de login malsucedidas, horários específicos de login, entre outros. |
| M1037 | Filtrar Tráfego de Rede | Utilize appliances de rede para filtrar tráfego de entrada e saída, aplicando filtros baseados em protocolos. |
| M1038 | Prevenção de Execução | Bloqueie a execução de código no sistema por meio de controle de aplicações e/ou bloqueio de scripts. |
| M1039 | Permissões de Variáveis de Ambiente | Impeça que usuários ou grupos não autorizados modifiquem variáveis de ambiente. |
| M1040 | Prevenção de Comportamento no Endpoint | Utilize recursos para prevenir padrões suspeitos de comportamento nos endpoints, como processos, arquivos e chamadas de API. |
| M1041 | Criptografar Informações Sensíveis | Proteja informações sensíveis utilizando criptografia forte. |
| M1042 | Desabilitar ou Remover Recurso ou Programa | Remova ou negue acesso a softwares desnecessários ou potencialmente vulneráveis para evitar abuso por agentes mal-intencionados. |
| M1043 | Proteção de Acesso a Credenciais | Utilize recursos para prevenir o acesso não autorizado a credenciais, incluindo bloqueio de técnicas de credential dumping. |
| M1044 | Restringir Carregamento de Biblioteca | Impeça abusos nos mecanismos de carregamento de bibliotecas do sistema operacional e software, configurando corretamente e monitorando vulnerabilidades. |
| M1045 | Assinatura de Código | Aplique verificação de assinatura digital para garantir a integridade de binários e aplicativos, evitando execução de código não confiável. |
| M1046 | Integridade de Inicialização | Utilize métodos seguros para inicialização do sistema e verificação da integridade do sistema operacional e seus carregadores. |

| | | |
|---|---|---|
| M1047 | Auditoria | Realize auditorias ou varreduras em sistemas, permissões, softwares inseguros e configurações para identificar possíveis fragilidades. |
| M1048 | Isolamento e Sandboxing de Aplicações | Restrinja a execução de código a ambientes virtuais no endpoint ou em trânsito até ele. |
| M1049 | Antivírus/Antimalware | Utilize assinaturas ou heurísticas para detectar softwares maliciosos. |
| M1050 | Proteção contra Exploit | Utilize recursos para detectar e bloquear condições que possam indicar a exploração de vulnerabilidades de software. |
| M1051 | Atualização de Software | Realize atualizações regulares de software para reduzir o risco de exploração de vulnerabilidades. |
| M1052 | Controle de Conta de Usuário (UAC) | Configure o UAC no Windows para reduzir o risco de agentes mal-intencionados obterem acesso elevado aos processos. |
| M1053 | Backup de Dados | Realize e armazene backups dos sistemas e servidores críticos, garantindo que estejam protegidos e isolados da rede corporativa. |
| M1054 | Configuração de Software | Aplique mudanças de configuração em softwares (exceto no sistema operacional) para mitigar riscos associados à sua operação. |
| M1055 | Não Mitigar | Categoria usada quando a mitigação pode aumentar o risco de comprometimento e, portanto, não é recomendada. |
| M1056 | Pré-Comprometimento | Categoria usada para atividades de mitigação que ocorrem antes do acesso inicial, como contra Reconhecimento e Desenvolvimento de Recursos. |

# INSTRUMENTOS DE COLETA DE DADOS DURANTE AS ENTREVISTAS

Este apêndice apresenta os instrumentos de coleta utilizados nas entrevistas realizadas com o Gestor de TI e o Chefe de Segurança da Informação da Empresa ALFA. A Tabela B.1 reúne o roteiro aplicado ao Gestor de TI, cujo objetivo foi classificar os sistemas institucionais de acordo com a criticidade frente a riscos cibernéticos. Enquanto a Tabela B.2 traz as perguntas destinadas ao Chefe de Segurança, voltadas à análise do Programa de Privacidade e Segurança da Informação (PPSI) vigente, da aplicação dos controles do CIS v8 e da avaliação da proposta apresentada por esta dissertação. As perguntas da segunda entrevista foram organizadas em blocos temáticos para facilitar o entendimento do contexto abordado em cada conjunto de questões.

Tabela B.1: Instrumento de Coleta de Dados para Classificação da Criticidade do Sistema

| **Pergunta** | **Resposta** |
|---|---|
| Nome do sistema avaliado | |
| O sistema trata dados pessoais? (Sim/Não) | |
| O sistema trata dados sensíveis? (Sim/Não) | |
| O sistema trata dados restritos? (Sim/Não) | |
| Qual o impacto do comprometimento da **confidencialidade** neste sistema? | ( ) Muito Baixo (1)<br>( ) Baixo (2)<br>( ) Médio (3)<br>( ) Alto (4)<br>( ) Muito Alto (5) |
| Qual o impacto do comprometimento da **integridade** neste sistema? | ( ) Muito Baixo (1)<br>( ) Baixo (2)<br>( ) Médio (3)<br>( ) Alto (4)<br>( ) Muito Alto (5) |
| Qual o impacto do comprometimento da **disponibilidade** neste sistema? | ( ) Muito Baixo (1)<br>( ) Baixo (2)<br>( ) Médio (3)<br>( ) Alto (4)<br>( ) Muito Alto (5) |
| Este sistema impacta diretamente a missão institucional? (Sim/Não) | |
| Se sim, em qual(is) eixo(s) ele impacta? | ( ) Prevenção<br>( ) Repressão<br>( ) Educação |
| **Pontuação final (automática ou manual)** | C + I + D = ___ |
| Classificação final do sistema | ( ) Baixa Criticidade (3–7)<br>( ) Média Criticidade (8–11)<br>( ) Alta Criticidade (12–13) |
| Validação final do Gestor | ( ) Concordo com a classificação<br>( ) Sugiro reclassificação. Justificativa: |

Tabela B.2: Roteiro de Entrevista com o Chefe de Segurança da Informação

| Bloco | Perguntas |
|---|---|
| **Bloco 1 – Contexto e Experiência com o PPSI e CIS Controls v8** | 1. Nome e experiência:<br>- Nome:<br>- Experiência no CADE (em anos):<br>- Experiência com a temática de segurança da informação (em anos):<br><br>2. Como o componente de segurança do PPSI, o CIS Controls v8, tem sido implementado na instituição?<br>- Quais são os principais benefícios que você observou com a aplicação desses frameworks?<br>- Quais foram os maiores desafios enfrentados durante a implementação?<br><br>3. Qual é o nível de adesão da instituição ao componente de segurança do PPSI (CIS Controls v8)?<br>- (Alto $\geq$ 85%, Moderado 50–84%, Baixo $\leq$ 49%) |
| **Bloco 2 – Adequação aos Sistemas Críticos** | 4. O PPSI e o CIS Controls v8 têm sido suficientes para proteger os sistemas críticos da instituição?<br>- Quais são as principais lacunas ou limitações que você identifica na aplicação desses frameworks em sistemas críticos?<br><br>5. Como você avalia a proteção atual dos sistemas críticos expostos à internet?<br>- Quais são os principais riscos que esses sistemas enfrentam? |
| **Bloco 3 – Recursos e Capacitação** | 6. A instituição possui recursos humanos e financeiros suficientes para implementar o PPSI e o CIS Controls v8 de forma eficaz?<br>- Como a falta de recursos impacta a capacidade de proteger sistemas críticos?<br><br>7. Qual é o nível de capacitação da equipe em relação ao PPSI e ao CIS Controls v8?<br>- Há necessidade de treinamentos ou capacitações adicionais?<br>- Como a organização tem apoiado nas lacunas de capacitação para implementar o PPSI? |
| **Bloco 4 – Lacunas e Desafios Atuais na Proteção de Sistemas Críticos** | 8. Como o PPSI e o CIS Controls v8 abordam a proteção de sistemas críticos?<br>- Eles são suficientes para mitigar os riscos atuais?<br><br>9. Mesmo com a aplicação do PPSI e do CIS Controls v8, ainda persistem vulnerabilidades nesses sistemas? |

*Continua na próxima página*

| Bloco | Perguntas (continuação) |
|---|---|
| **Bloco 5 – Maturidade em Segurança da Informação** | 10. Como você avalia o nível de maturidade da instituição em segurança da informação?<br>- Resposta: Alto, moderado, baixo.<br>- Considere profissionais disponíveis e capacitados, ferramentas disponíveis e processos maduros.<br><br>11. O PPSI e o CIS Controls v8 têm contribuído para elevar essa maturidade?<br>- De que forma?<br><br>12. Quais são os principais indicadores de maturidade que você utiliza para avaliar a segurança da informação na instituição? |
| **Bloco 6 – Incidentes e Respostas** | 13. A instituição já enfrentou incidentes de segurança cibernética em sistemas críticos?<br>- Quais foram os impactos desses incidentes?<br>- Houve falhas ou limitações no processo de resposta?<br><br>14. Como o PPSI e o CIS Controls v8 ajudaram a mitigar esses incidentes?<br><br>15. Quais lições foram aprendidas com esses incidentes? |
| **Bloco 7 – Proposta de um Novo Modelo Estruturado (3SW)** | 16. Na sua opinião, o que falta no PPSI e no CIS Controls v8 para que sejam mais eficazes na proteção de sistemas críticos?<br>*(Explicar a proposta antes de seguir para a próxima pergunta)*<br><br>17. Como você avalia a proposta de um novo modelo de referência, como o 3SW, adaptado para servidores web e sistemas expostos à internet?<br>- Quais seriam os principais benefícios e desafios dessa abordagem?<br><br>18. Quais seriam as principais recomendações para a implementação do 3SW na instituição? |
| **Bloco 8 – Comparação e Expectativas** | 19. Que métricas ou indicadores poderiam ser usados para comparar a eficácia do novo modelo (3SW) em relação ao PPSI?<br><br>20. Quais são suas expectativas em relação à implementação do 3SW na instituição?<br>- Quais resultados você esperaria ver em curto, médio e longo prazo? |
| **Bloco 9 – Validação do Problema e Alinhamento com o Estudo** | 21. Quais são os principais problemas de segurança cibernética que você identifica na instituição atualmente?<br>- Esses problemas estão alinhados com o foco do estudo (proteção de sistemas expostos à internet)?<br><br>22. Como você avalia a relevância do estudo que está sendo realizado para a instituição?<br>- Ele aborda os problemas mais críticos que você identifica?<br><br>23. Há algum aspecto adicional que você gostaria de destacar em relação à segurança cibernética na instituição? |

# ARCABOUÇO JURÍDICO DE SEGURANÇA DA INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA FEDERAL BRASILEIRA

Este apêndice apresenta uma compilação dos principais normativos relacionados à segurança da informação no âmbito da administração pública federal brasileira. A Tabela C.1, mencionada na Seção 2.2, organiza 56 instrumentos legais segundo sua classificação normativa (Leis, Decretos, Portarias, entre outros), oferecendo uma visão abrangente da base jurídica que orienta políticas, práticas e obrigações legais em segurança da informação no setor público federal.

Tabela C.1: Arcabouço jurídico de segurança da informação na administração pública federal brasileira. Fonte: Adaptado de [6]

| Classificação/Ano | Norma e Descrição |
|---|---|
| **Lei (2021)** | **LEI Nº 14.155/2021**<br>Altera o Código Penal para crimes eletrônicos (violação de dispositivo, furto e estelionato digital). |
| **Lei (2021)** | **LEI Nº 14.129/2021**<br>Governo Digital e eficiência pública (altera Lei de Acesso à Informação). |
| **Lei (2020)** | **LEI Nº 14.063/2020**<br>Uso de assinaturas eletrônicas e licenças de softwares públicos. |
| **Lei (2012)** | **LEI Nº 12.737/2012**<br>Lei Carolina Dieckmann (tipificação de delitos informáticos). |
| **Lei (2012)** | **LEI Nº 12.735/2012**<br>Tipifica condutas contra sistemas informatizados. |
| **Lei (2011)** | **LEI Nº 12.527/2011**<br>Lei de Acesso à Informação (transparência pública). |
| **Lei Complementar (2001)** | **LC Nº 105/2001**<br>Sigilo de operações financeiras. |
| **Lei (2000)** | **LEI Nº 9.983/2000**<br>Crimes contra a administração pública (inclui falsificação digital). |
| **Lei (2014)** | **LEI Nº 12.965/2014**<br>Marco Civil da Internet (direitos e deveres no uso da web). |
| **Lei (2018)** | **LEI Nº 13.709/2018**<br>Lei Geral de Proteção de Dados Pessoais (LGPD). |
| **Decreto (2023)** | **DECRETO Nº 11.856/2023**<br>Política Nacional de Cibersegurança e Comitê Nacional. |
| **Decreto (2021)** | **DECRETO Nº 10.748/2021**<br>Rede Federal de Gestão de Incidentes Cibernéticos. |
| **Decreto (2021)** | **DECRETO Nº 10.641/2021**<br>Altera Política Nacional de Segurança da Informação. |
| **Decreto (2024)** | **DECRETO Nº 12.198/2024**<br>Estratégia Federal de Governo Digital (2024-2027). |

*Continua na próxima página*

| Classificação/Ano | Norma e Descrição (continuação) |
|---|---|
| **Decreto (2020)** | **DECRETO Nº 10.569/2020**<br>Estratégia Nacional de Segurança de Infraestruturas Críticas. |
| **Decreto (2019)** | **DECRETO Nº 10.046/2019**<br>Governança de compartilhamento de dados e Cadastro Base do Cidadão. |
| **Decreto (2019)** | **DECRETO Nº 9.854/2019**<br>Plano Nacional de Internet das Coisas (IoT). |
| **Decreto (2018)** | **DECRETO Nº 9.637/2018**<br>Política Nacional de Segurança da Informação. |
| **Decreto (2016)** | **DECRETO Nº 8.771/2016**<br>Regulamenta o Marco Civil da Internet (neutralidade da rede). |
| **Decreto (2012)** | **DECRETO Nº 7.845/2012**<br>Credenciamento para tratamento de informação sigilosa. |
| **Decreto (2003)** | **DECRETO Nº 4.829/2003**<br>Criação do Comitê Gestor da Internet no Brasil (CGI.br). |
| **Decreto (2018)** | **DECRETO Nº 9.573/2018**<br>Política Nacional de Segurança de Infraestruturas Críticas. |
| **Decreto (2022)** | **DECRETO Nº 11.200/2022**<br>Plano Nacional de Segurança de Infraestruturas Críticas. |
| **Decreto (2019)** | **DECRETO Nº 9.832/2019**<br>Altera normas sobre Comitê Gestor da Segurança da Informação. |
| **Portaria (2023)** | **Portaria SGD/MGI nº 852/2023**<br>Programa de Privacidade e Segurança da Informação (PPSI). |
| **Portaria (2022)** | **Portaria GSI/PR nº 120/2022**<br>Plano de Gestão de Incidentes Cibernéticos na administração pública. |
| **Portaria (2017)** | **Portaria nº 85 GSI/PR/2017**<br>Uso do Terminal de Comunicação Segura (TCS) da ABIN. |
| **Instrução Normativa (2020)** | **IN GSI nº 1/2020**<br>Estrutura de Gestão da Segurança da Informação na APF. |
| **Instrução Normativa (2020)** | **IN GSI nº 2/2020**<br>Altera IN GSI nº 1/2020 (gestão de segurança da informação). |
| **Instrução Normativa (2013)** | **IN GSI nº 2/2013**<br>Credenciamento para tratamento de informação classificada. |
| **Instrução Normativa (2021)** | **IN GSI nº 3/2021**<br>Processos de gestão de segurança da informação na APF. |
| **Instrução Normativa (2013)** | **IN GSI nº 3/2013**<br>Parâmetros para criptografia de informação classificada. |
| **Instrução Normativa (2020)** | **IN GSI nº 4/2020**<br>Requisitos de segurança cibernética para redes 5G. |
| **Instrução Normativa (2021)** | **IN GSI nº 5/2021**<br>Segurança em computação em nuvem na APF. |
| **Instrução Normativa (2021)** | **IN GSI nº 6/2021**<br>Diretrizes para uso seguro de mídias sociais na APF. |
| **Instrução Normativa (2022)** | **IN GSI nº 7/2022**<br>Altera INs anteriores sobre segurança da informação. |

*Continua na próxima página*

| Classificação/Ano | Norma e Descrição (continuação) |
|---|---|
| **Norma Complementar (2009)** | **NC nº 05/2009**<br>Criação de Equipes de Resposta a Incidentes (ETIR). |
| **Norma Complementar (2010)** | **NC nº 08/2010**<br>Diretrizes para gerenciamento de incidentes em redes. |
| **Norma Complementar (2014)** | **NC nº 09/2014**<br>Uso de recursos criptográficos na APF. |
| **Norma Complementar (2012)** | **NC nº 12/2012**<br>Segurança no uso de dispositivos móveis na APF. |
| **Norma Complementar (2013)** | **NC nº 17/2013**<br>Diretrizes para profissionais de segurança da informação. |
| **Norma Complementar (2013)** | **NC nº 18/2013**<br>Capacitação em segurança da informação na APF. |
| **Norma Complementar (2014)** | **NC nº 20/2014**<br>Processo de tratamento da informação na APF. |
| **Norma Complementar (2014)** | **NC nº 21/2014**<br>Coleta de evidências de incidentes de segurança. |
| **Norma Complementar (2013)** | **NC nº 01/2013**<br>Credenciamento para tratamento de informações sigilosas. |
| **Portaria (2024)** | **PORTARIA SGD/MGI Nº 6.618/2024**<br>Estratégia Federal de Governo Digital (2024-2027). |
| **Instrução Normativa (2022)** | **IN SGD/ME Nº 94/2022**<br>Contratação de soluções de TIC no SISP. |
| **Portaria (2023)** | **Portaria SGD/MGI nº 750/2023**<br>Contratação de desenvolvimento de software no SISP. |
| **Portaria (2023)** | **PORTARIA SGD/MGI Nº 1.070/2023**<br>Contratação de serviços de infraestrutura de TIC. |
| **Portaria (2023)** | **Portaria SGD/MGI nº 5.950/2023**<br>Contratação de computação em nuvem no SISP. |
| **Portaria (2023)** | **PORTARIA SGD/MGI Nº 2.715/2023**<br>Gestão de estações de trabalho no SISP. |
| **Portaria (2024)** | **PORTARIA SGD/MGI Nº 6.680/2024**<br>Altera normas de contratação de infraestrutura de TIC. |
| **Portaria (2024)** | **Portaria SGD/MGI Nº 6.679/2024**<br>Altera normas de contratação de software. |
| **Portaria (2023)** | **PORTARIA SGD/MGI Nº 370/2023**<br>Contratação de serviços de impressão no SISP. |
| **Portaria (2023)** | **PORTARIA SGD/MGI Nº 852/2023**<br>Programa de Privacidade e Segurança da Informação (PPSI). |
| **Instrução Normativa (2020)** | **IN SGD/ME Nº 117/2020**<br>Encarregado pelo Tratamento de Dados Pessoais na APF. |