risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido/Submission: 22/06/2024
Aceitação/Acceptance: 18/10/2024

3SW: Um Conjunto de Medidas de Segurança para Mitigar Vulnerabilidades em Servidores Web

Silva, Tássio[1], Mendes, Fabiana[1,2]

tassio.silva@aluno.unb.br; fabiana.mendes@aalto.fi.

[1] Programa de Pós-Graduação em Engenharia Elétrica, Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Universidade de Brasília. Brasília-DF-Brazil. 70910-900

[2] Department of Computer Science, Aalto University. Espoo-Finland. 02150

DOI: 10.17013/risti.56.66–81

Resumo: Por hospedar serviços digitais, servidores web tornam-se alvos prioritários para ações mal-intencionadas. Entretanto, faltam guias amplos que auxiliem sua proteção. Assim, esse trabalho propõe o modelo 3SW que tem como objetivo auxiliar na mitigação de vulnerabilidades em servidores web. Para seu desenvolvimento, foi feita a seleção das medidas de segurança mais relevantes do CIS Controls, considerando nosso escopo (servidores web) e o esforço de implementação. Além disso, o 3SW é comparado com abordagens reconhecidas na cibersegurança para atestar sua utilidade. O 3SW é composto de 93 medidas, que correspondem a 61% das medidas do CIS Controls v8.1. A comparação do 3SW com MITRE ATT&CK mostrou uma cobertura de 86%, com ênfase em auditoria de registros, defesa contra malware e recuperação de dados. Dessa forma, o 3SW oferece uma abordagem que facilita a priorização estratégica e a implementação eficiente de medidas de segurança.

Palavras-chave: CIS Controls; cibersegurança; segurança da informação; servidor web; medidas de segurança.

3SW: A Set of Safeguards to Mitigate Vulnerabilities in Web Servers

Abstract: Web servers are often targeted for malicious attacks because they host various applications. Unfortunately, there are not many comprehensive guides available to help implement effective protection measures. This work aims to propose a model called the 3SW model, which is designed to help mitigate vulnerabilities in web servers. To develop this model, we selected the most relevant safeguards from the CIS Controls, focusing specifically on web servers and the effort required for implementation. Additionally, the 3SW model is compared with well-recognized cybersecurity approaches to validate its usefulness. The 3SW consists of 93 safeguards, representing 61% of the CIS Controls v8.1 safeguards. A comparison between the 3SW model and the MITRE ATT&CK framework revealed an 86% coverage, emphasizing log auditing, malware defense, and data recovery. Therefore,

we concluded that the 3SW model presents an approach that facilitates strategic prioritization and efficient implementation of protective safeguards for web servers.

Keywords: CIS Controls; cybersecurity; information security; web server; safeguards.

1. Introdução

Os ataques cibernéticos têm sido frequentemente noticiados devido ao impacto significativo nos serviços das organizações afetadas (Bada & Nurse, 2020). Entre as consequências mais evidentes, destacam-se a indisponibilidade de serviços e o vazamento de dados pessoais e confidenciais, que podem gerar danos severos à reputação e ao funcionamento das empresas (Kamiya et al., 2020).

Em 2021, um ataque de *ransomware*, caracterizado pelo sequestro de dados e exigência de resgate para liberação (Chen & Bridge, 2017), interrompeu as operações da empresa JBS nos EUA, Canadá e Austrália (BBC, 2021). Outros ataques podem dar origem a extorsões pelo vazamento de dados pessoais, como ocorreu, entre 2018 e 2019, com a clínica Vastaamo de Psiquiatria na Finlândia, que levou a decretar falência em 2021 (Ghanbari & Koskinen, 2024). Esses eventos ilustram a gravidade e o alcance desses incidentes, com impactos diretos na economia, na privacidade dos indivíduos e até na viabilidade das empresas.

A evolução e as consequências dessas ameaças impulsionam o desenvolvimento de metodologias para mitigar seus efeitos, como a família ISO/IEC 27000 (ISO, 2024), as publicações do NIST (NIST, 2024a), o MITRE ATT&CK (MITRE, 2024), o OWASP (OWASP, 2024) e a metodologia CIS Controls v8.1 (CIS, 2024a), que em grande parte já foram incorporadas à cultura de proteção nas áreas de Tecnologia da Informação (TI) e cibersegurança (Leszczyna, 2021).

Apesar disso, mais de 80% das vulnerabilidades estão ligadas a aplicações web (Verizon, 2023), frequentemente suportadas por servidores web, que desempenham um papel crítico ao fornecer serviços a usuários finais. No entanto, as metodologias mencionadas anteriormente não consideram esses servidores como alvos específicos de ataques cibernéticos, o que resulta na ausência de um guia específico para determinados contextos e situações.

Dentre essas metodologias, o CIS Controls destaca-se por priorizar ações e apoiar gestores de TI na escolha das medidas de segurança mais urgentes (Crotty & Daniel, 2021). Contudo, essa priorização não considera diretamente alvos específicos de ataques cibernéticos, como os servidores web. Até onde vai o conhecimento dos autores, não há uma metodologia que relacione diretamente as medidas do CIS Controls com a proteção de servidores web — sistemas definidos como aqueles que fornecem serviços na Internet, compostos por hardware, sistema operacional, software de servidor web e páginas do site (NIST, 2024b).

Com a finalidade de preencher essa lacuna, este estudo propõe uma simplificação da metodologia CIS v8.1 para servidores web, criando um Subconjunto de Safeguards para Servidores Web, o 3SW.

Como resultado, obteve-se um conjunto de 93 medidas diretamente focadas em servidores web, com ênfase em auditoria de registros, defesa contra *malware* e recuperação de dados.

O uso do 3SW disponibiliza aos gestores de TI uma priorização mais direcionada das ações de segurança, atendendo de forma mais eficaz às demandas dos servidores web. Além disso, os critérios definidos no estudo permitem adaptar as medidas para outros tipos de ativos, ampliando o alcance do 3SW na mitigação de riscos.

O documento está organizado da seguinte forma: a Seção 2 apresenta o referencial teórico e os trabalhos correlatos; a Seção 3 descreve a metodologia utilizada; a Seção 4 discute os resultados e comparações; e a Seção 5 traz as conclusões da pesquisa.

2. Referencial Teórico

Esta seção apresenta conceitos fundamentais e estruturas utilizadas no contexto da segurança cibernética, com foco especial na mitigação de ameaças em servidores web. São discutidos riscos cibernéticos, *frameworks* como o CIS Controls v8.1 (CIS v8.1) e o MITRE ATT&CK, além de modelos correlatos que contribuem para o aumento da maturidade cibernética. Esses elementos fundamentam a proposta do modelo 3SW deste estudo.

2.1. Risco Cibernético

Cebula et al. (2021) definem os riscos cibernéticos como resultantes de ações humanas, falhas tecnológicas e de processos internos, bem como de eventos externos, que podem comprometer a confidencialidade, integridade ou disponibilidade de informações. Além dos impactos na segurança, essas falhas acarretam prejuízos financeiros e de reputação. Em 2024, o custo médio de uma violação de dados atingiu 4,88 milhões de dólares, um aumento de 10% em relação ao ano anterior, evidenciando o impacto econômico crescente dessas ameaças (IBM, 2024).

Os ataques a aplicações web são particularmente críticos, uma vez que muitas organizações dependem de servidores web para operações online (Verizon, 2023). Por armazenarem dados sensíveis e operações críticas, esses servidores tornam-se alvos de ataques que exploram vulnerabilidades de softwares e de configurações inadequadas (Alves et al., 2023). Nesse contexto, *frameworks* de segurança são fundamentais para mitigar riscos e proteger ativos organizacionais, pois suas medidas visam reduzir a ocorrência de incidentes e seus impactos (Cue et al., 2024). A próxima seção aborda alguns desses frameworks.

2.2. Frameworks de segurança

Diferentes frameworks de segurança proporcionam abordagens estruturadas para identificar e mitigar ameaças cibernéticas, cada um com foco e aplicação específicos. No contexto deste estudo, destacam-se o CIS 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 v8.1 fornece diretrizes práticas para melhorar a postura de segurança de forma geral, o MITRE ATT&CK ajuda a entender o comportamento dos

atacantes 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*.

O Center for Internet Security® (CIS), uma organização sem fins lucrativos que reúne o conhecimento de especialistas de diferentes setores, é responsável pela metodologia CIS Controls, amplamente adotada por organizações ao redor do mundo (CIS, 2024a; Juma et al., 2023). Atualmente na versão 8.1, a metodologia é composta por 18 controles e 153 medidas de segurança (*safeguards*), desenvolvidas para apoiar organizações com diferentes níveis de maturidade em segurança e necessidades operacionais. Neste estudo, o CIS v8.1 é utilizado como base para a avaliação de práticas de segurança voltadas especificamente para servidores web, permitindo uma comparação estruturada com o ataque *Web Application Hacking* (WAH) do CDM.

Complementando essas práticas, o MITRE ATT&CK constitui um framework que descreve táticas e técnicas empregadas por agentes maliciosos em ataques cibernéticos, assim como as possíveis mitigações. Esse framework proporciona uma estrutura didática para que profissionais de segurança compreendam e atuem contra essas ameaças (MITRE, 2024). Embora a versão mais recente do MITRE ATT&CK seja a 15.1, lançada em abril de 2024, este artigo utiliza a versão 8.2 para a comparação entre os modelos 3SW e WAH, uma vez que o mapeamento oficial disponibilizado pelo CIS para o WAH está alinhado com essa versão. A versão 15.1 contém 43 mitigações, enquanto a 8.2 inclui 42, sendo a mitigação ausente a '*Data Loss Prevention (M1057)*'. Essa mitigação foi introduzida na versão 10.1 do MITRE ATT&CK e não faz parte do escopo deste estudo (MITRE, 2024).

Apesar da mitigação '*Data Loss Prevention (M1057)*' não ser incluída no mapeamento oficial utilizado neste estudo, é plausível que, caso estivesse presente, ela pudesse ser associada ao Controle 3 – proteção de dados do CIS v8.1, que trata de identificar, classificar, manipular com segurança, reter e descartar dados (CIS, 2024a).

Por fim, o CDM v2.0, também desenvolvido pelo CIS, 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* (CIS, 2024b). 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 (CIS, 2024a). O CDM concluiu que a implementação de todas as medidas relacionadas a essas cinco ameaças proporciona uma de proteção 91% contra as subtécnicas descritas no MITRE ATT&CK v8.2 (CIS, 2024b).

Entretanto, considerando a aplicação do 3SW em servidores web, apenas o *Web Application Hacking* é diretamente relacionado. Esse ataque inclui 90 medidas de segurança, cobrindo 38 das 42 mitigações identificadas no MITRE ATT&CK v8.2, sendo, portanto, utilizado como base para comparação com o modelo proposto neste artigo (CIS, 2024b).

2.3. Trabalhos correlatos

Diversos estudos recentes têm explorado a aplicação de frameworks de cibersegurança (Juma et al., 2023; Domínguez-Dorado et al., 2022; Lima et al.; 2022), modelos de

maturidade (Bashofi & Salman, 2022) e ferramentas para auxiliar na mitigação de ameaças cibernéticas (Gonzalez-Granadillo et al., 2021), especialmente relacionados ao CIS Controls. Esta seção analisa as principais contribuições que abordam a aplicação, adaptação e simplificação dos controles CIS e metodologias similares para enfrentar riscos cibernéticos.

Kern et al. (2024) elaboraram um modelo de maturidade para melhorar a detecção precoce de ataques cibernéticos por meio de gerenciamento de logs de auditoria e monitoramento de redes. Horta et al. (2022), por sua vez, desenvolveram um modelo para criar planos de ação priorizados, visando fortalecer a visibilidade frente a ameaças e facilitar a tomada de decisão. Trabalhos similares foram realizados por Tsiodra et al. (2023) e AL-Hawamleh (2024), que também apresentaram modelos com ênfase na tomada de decisão em segurança cibernética. Todavia, esses modelos adotam uma aplicação abrangente, em contraste com a abordagem focada em servidores web neste artigo.

Alguns trabalhos mais próximos deste estudo também focam em medidas de segurança, como Cue et al. (2024), que classificaram medidas de segurança do CIS Controls v8 para monitorar o progresso contínuo na implementação de controles e orientar gestores na melhoria de programas de segurança. Apesar da proximidade metodológica, esses estudos também não tratam especificamente de servidores web, como ocorre neste artigo.

Por outro lado, autores como Song & Garcia-Valls (2022), restringiram suas propostas ao monitoramento de servidores web de sistemas IoT críticos, combinando detecção e resposta automatizada a vulnerabilidades. Fadlil et al. (2024) utilizaram a metodologia OWASP para criar um framework que identifica e trata vulnerabilidades de injeção SQL (SQLi) em servidores web. Esses estudos, embora direcionados a servidores web, tratam de vulnerabilidades específicas e de contextos restritos, enquanto o modelo proposto aqui visa uma abordagem de segurança mais ampla para o ambiente de servidores web.

Nesse contexto, o modelo 3SW, desenvolvido neste artigo, segue a tendência de adaptação a cenários específicos, priorizando a segurança de servidores web. Diferente de abordagens mais amplas, ele simplifica a implementação e direciona esforços para medidas diretamente aplicáveis a esse ambiente. Essa estratégia busca garantir eficácia e agilidade, essenciais para organizações que demandam respostas rápidas e eficientes.

3. Método de Pesquisa

Esta pesquisa tem como objetivo **simplificar a metodologia CIS v8.1 para aplicação em Servidores Web**, resultando em um subconjunto de medidas de segurança denominado 3SW. A abordagem adotada para condução da pesquisa é exploratória e utiliza análise qualitativa para a redução, categorização e interpretação dos dados (Gil, 2023).

Para alcançar o objetivo estabelecido, foi adaptada a metodologia de análise de conteúdo proposta por Bardin (2016), dividida em três fases, conforme ilustrado na Figura 1. A primeira, a **Pré-análise**, envolve três atividades: *Seleção do Material a ser Analisado*, *Definição de Estratégia de Análise* e *Definição dos Critérios Qualitativos*.

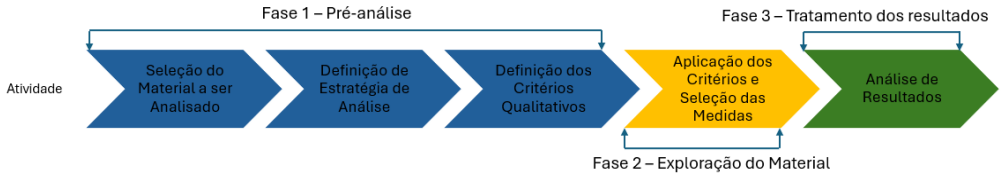

Figura 1 – Fases e Atividades da Metodologia de Pesquisa

Na atividade *Seleção do Material a ser Analisado* (**Fase 1 - Pré-Análise),** foi aplicada a regra de pertinência (Bardin, 2016), em que os documentos selecionados devem corresponder ao objetivo da análise. Como resultado da execução desse passo, foram selecionados o CIS v8.1, que guia a implementação de medidas de segurança (Crotty & Daniel, 2021); o MITRE ATT&CK, que apresenta um conjunto de técnicas e táticas amplamente utilizado para mitigar ataques cibernéticos (MITRE, 2024a); e o CDM v2.0, que disponibiliza um modelo para comparação com o 3SW ao alinhar as medidas do CIS Controls a ataques direcionados a aplicações web (CIS, 2024b).

Na atividade subsequente, *Definição da Estratégia de Análise* (**Fase 1),** foram formuladas as questões de pesquisa (QP) para direcionar a investigação e alcançar o objetivo proposto:

> **QP1:** É possível selecionar as medidas de segurança do CIS 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?

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

Tipo	Critérios	Respostas Possíveis
Seleção	CS1 - A medida está no escopo do servidor web?	Sim/Não
	CS2 - A medida pode ser individualizada?	Sim/Não
	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
	CP2 – Qual o esforço para implementar a medida no servidor web?	Alto/Moderado/Baixo
	CP3 – Qual o esforço para manter a medida aplicada e atualizada no servidor web?	Alto/Moderado/Baixo

Tabela 1 – Critérios para seleção e priorização de Medida de Segurança.

Como pode ser visto na Tabela 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 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 (NIST, 2024c). A Tabela 2 apresenta as descrições para as categorias de esforço.

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.

Tabela 2 – Categorias por Esforço (Baseado no NIST SP 800-55v1).

A **Fase 2 - Exploração do Material**, contém a atividade *Aplicação dos Critérios e Seleção das Medidas*, nela são aplicados os critérios discriminados na Tabela 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 **Fase 3 – Tratamento dos Resultados**, última fase da metodologia, consiste na análise dos resultados obtidos a partir da aplicação dos critérios na Fase 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 deste estudo.

4. Resultados e Discussões

Conforme mencionado anteriormente, o objetivo deste trabalho é simplificar a metodologia CIS v8.1 para aplicação em servidores web, resultando na criação do subconjunto aqui denominado 3SW. A investigação foi guiada por três questões de pesquisa (Seção 3), respondidas por meio de uma análise qualitativa dos documentos selecionados. Os documentos contendo detalhes da análise desenvolvida estão disponíveis em um pacote no Zenodo (DOI: 10.5281/zenodo.14175601). A seguir, são apresentados os resultados da análise, em que a resposta de cada uma das três questões de pesquisa listadas na Seção 3 é detalhada em subseções.

4.1. Medidas de segurança para o Servidor Web (QP1)

Inicialmente foram avaliados os critérios de seleção (vide Tabela 1) para decidir sobre a inclusão de uma medida no 3SW. Para a inclusão é necessário que todos os critérios fossem marcados como verdadeiros, ou seja, que a medida seja relevante, individualizável e verificável para os servidores web. A Tabela 3 oferece uma visão geral das medidas de segurança selecionadas com base nos critérios aplicados na Fase 2.

Observe que a Tabela 3 apresenta os 18 controles do CIS 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 (PMS).

Como resultado, das 153 medidas de segurança disponibilizadas no framework CIS v8.1, 93 (61%) atenderam aos três critérios de seleção estabelecidos na Fase 1 (CS1, CS2 e CS3). 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.

IDC	Descrição	QMS	PMS
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)

IDC	Descrição	QMS	PMS
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; PMS - Porcentagem de Medidas de Segurança (Total de medidas selecionadas / Total de Medidas Possíveis do Controle).

Tabela 3 – Resultado da seleção das medidas de segurança.

Os demais controles dividem-se em outros dois grupos: controles com baixa aderência ao 3SW (entre 1% e 49%), no qual incluem-se os controles C1, C13, C15 e C17; e **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. Avaliação das medidas de segurança por esforço de implementação e de manutenção no Servidor Web (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 2. A consolidação desses resultados está disposta na Tabela 4, que oferece uma visão abrangente do esforço requerido para aplicação e sustentação das medidas no contexto dos servidores web.

CP1	CP2	CP3			Total CP2 (%)
		Baixo	Moderado	Alto	
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%)	

CP1	CP2	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%)	
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?.

Tabela 4 – Consolidação da análise dos critérios de priorização sobre as medidas do 3SW.

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 podem ser geridas 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 indicam que, mesmo entre as medidas que não dependem de recursos externos, a implementação moderada é predominante, mas uma parte considerável das medidas ainda requer um esforço baixo, facilitando a aplicação.

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 demonstra 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.

Assim, priorizar medidas que podem ser implementadas diretamente no servidor web pode resultar em uma otimização do uso de recursos e na liberação de tempo para a equipe se concentrar em outras estratégias de mitigação de riscos cibernéticos.

4.3. Comparação do Modelo 3SW com o *Web Application Hacking* do CDM (QP3)

O último passo dessa pesquisa envolveu a comparação do 3SW com o modelo que mais se aproxima de nossa proposta, o *Web Application Hacking* (WAH). O resumo da análise comparativa entre 3SW e WAH é apresentado na Tabela 5.

IDC	QTD 3SW	QTD WAH	DP	IDC	QTD 3SW	QTD WAH	DP
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; DP - Diferença Percentual - (Total de medidas exclusivas do 3SW – Total de medidas exclusivas do WAH) / Total de Medidas do Controle).

Tabela 5 – Medidas de Segurança únicas em 3SW e WAH.

Como os dois modelos, 3SW e WAH, selecionam medidas do CIS Controls na versão 8 para sua composição, a Tabela 5 aborda a Diferença Percentual (DP) que cada modelo possui, a partir de medidas exclusivas distribuídas por cada um dos 18 controles. De modo que, das 93 medidas que compõe o 3SW e das 90 medidas presentes no WAH, 61 medidas estão contidas nos dois modelos. Sendo as exclusivas de cada modelo respectivamente 32 para o 3SW e 29 para o WAH. Assim, a Tabela 5 busca mostrar o que representa essa diferença no total medidas de segurança por controle.

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 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. Observe que apenas quatro controles possuem a mesma cobertura em ambos os modelos, em cinco controles o WAH obteve melhor cobertura e no restante dos controles (9), o 3SW possui maior quantidade de medidas. O que se pode concluir que o modelo

3SW possui uma maior distribuição 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 6.

Controle	DP	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.

Tabela 6 – Análise dos controles com diferença percentuais > 25% e < -25%.

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 à 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, 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, avaliamos a aderência de cada modelo às mitigações do MITRE ATT&CK. O CIS 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 (*Application Developer Guidance*) e M1017 (*User Training*), 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.

Essa análise reitera que, embora ambos os modelos compartilhem o objetivo de mitigar riscos cibernéticos, suas abordagens diferem para atender aos desafios específicos de seus ambientes. O modelo 3SW, ao focar em medidas com maior aplicabilidade para servidores web, proporciona uma simplificação e adaptação dessas medidas do CIS v8.1, maximizando aspectos voltados para a recuperação de dados (Mohammed, 2022), gestão de registros de auditoria (Kern et al., 2024) e defesas contra *malwares* (Ferdous et al., 2023), ressaltando a relevância das medidas selecionadas para os desafios específicos desse ambiente.

5. Conclusões

Este estudo propôs o modelo 3SW, um subconjunto simplificado do CIS v8.1 para aplicação em servidores web, visando facilitar a implementação de medidas de segurança neste contexto específico. Para alcançar esse objetivo, o estudo selecionou medidas de segurança (QP1), classificou o esforço de implementação e manutenção (QP2) e comparou o 3SW com o WAH (QP3).

Foram selecionadas 93 das 153 medidas do CIS v8.1, correspondendo a 61% do total, destacando cinco controles totalmente aplicáveis ao contexto de servidores web. Em contrapartida, o controle de conscientização (C14) foi considerado inadequado para esse contexto. Além disso, foi possível categorizar os controles de acordo com a aderência ao 3SW, o que facilita a priorização estratégica das medidas de segurança.

Quanto ao esforço (QP2), foi identificado que 57% das medidas presentes no 3SW são aplicáveis diretamente nos servidores, apresentando menor esforço de implementação.

Na comparação do 3SW com o WAH (QP3), o 3SW demonstrou uma abordagem mais focada em auditoria de registros, defesa contra malware e recuperação de dados. Pontos que reforçam os aspectos de proteção de ativos expostos à Internet. Além disso, o 3SW, no que tange ao MITRE ATT&CK, abrange 92% das mitigações presente nesse modelo para o CIS v8.1, contra 97% do WAH, sendo o principal diferencial a ausência de medidas voltadas ao treinamento e à conscientização dos usuários, presente no WAH, mas consideradas fora do escopo específico do 3SW para servidores web.

Entretanto, apesar desses resultados voltados para uma maior proteção do ativo, uma limitação do 3SW é a ausência de validação prática em cenários reais, o que ressalta a importância de estudos futuros que apliquem o modelo em ambientes operacionais, permitindo ajustes a partir de feedbacks. Adicionalmente, a metodologia definida para o 3SW pode ser adaptada para outros ativos, como bancos de dados e redes, bem como ser integrado a frameworks como ISO/IEC 27000 e NIST para ampliar sua cobertura de proteção durante a análise de medidas para o ativo. A criação de ferramentas automatizadas para a implementação e monitoramento contínuo das medidas, aliada a uma análise do impacto econômico, são caminhos promissores para futuras pesquisas.

Em síntese, o 3SW simplifica a aplicação do CIS v8.1 para servidores web, contribuindo para a eficiência na mitigação de riscos e auxiliando na priorização técnica de medidas de

segurança. Sua comparação com outros modelos confirmou sua adequação às melhores práticas de segurança, mostrando-se relevante para aprimoramentos futuros e para uma abordagem mais estratégica na proteção de servidores web.

5.1. Disponibilidade dos Dados

Os arquivos completos com os resultados da análise qualitativa, bem como os documentos complementares utilizados no estudo, estão disponíveis em um pacote no Zenodo. Acesse através do DOI: 10.5281/zenodo.14175601.

Referências

AL-Hawamleh, A. (2024). Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. International Journal of Computing and Digital Systems, 15(1), 1315-1331.

Alves, R. S., Georg, M. A. C., & Nunes, R. R. (2023). Judiciário sob ataque hacker: riscos de negócio para segurança cibernética em tribunais brasileiros. Revista Ibérica de Sistemas e Tecnologias de Informação, (E56), 344-357. DOI:10.5281/zenodo.8032915

Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. In Emerging cyber threats and cognitive vulnerabilities (pp. 73-92). Academic Press. https://doi.org/10.1016/B978-0-12-816203-3.00004-6

Bardin, L. (2016). Análise de conteúdo. São Paulo, Brasil: Edições, 70.

Bashofi, I., & Salman, M. (2022). Cybersecurity maturity assessment design using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002. In 2022 IEEE International Conference on Cybernetics and Computational Intelligence. https://doi.org/10.1109/CyberneticsCom55287.2022.9865640

BBC. (2021). JBS: Cyber-attack hits world's largest meat supplier. BBC News, 2 de junho de 2021. https://www.bbc.com/news/world-us-canada-57318965

Cebula, J. J., & Young, L. R. (2010). A taxonomy of operational cyber security risks. Software Engineering Institute, Carnegie Mellon University.

Center for Internet Security (CIS). (2024a). CIS Controls V8.1. https://www.cisecurity.org/controls/cis-controls-list/

Center for Internet Security (CIS). (2024b). CIS Community Defense Model 2.0. https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

Chen, Q., & Bridges, R. A. (2017). Automated behavioral analysis of malware: A case study of wannacry ransomware. In 2017 16th IEEE International Conference on machine learning and applications (ICMLA) (pp. 454-460). IEEE. https://doi.org/10.1109/ICMLA.2017.0-119

Crotty, J., & Daniel, L. (2021). Lessons from practice: insights on cybersecurity strategy for business leaders, from SMEs to global enterprises. Milton Keynes: Open University.

Cue, H. A. A., Bourlai, T., & Lupo, M. (2024). A CIS Controls V8. 0 Scoring System using Combined Ranking-Weight Methods. In 2024 IEEE International Systems Conference (SysCon) (pp. 1-8). IEEE. https://doi.org/ 10.1109/ SysCon61195.2024.10553474

Domínguez-Dorado, M., Carmona-Murillo, J., Cortés-Polo, D., & Rodríguez-Pérez, F. J. (2022). CyberTOMP: A novel systematic framework to manage asset-focused cybersecurity from tactical and operational levels. IEEE Access, 10, 122454-122485. https://doi.org/10.1109/ACCESS.2022.3223440

Fadlil, A., Riadi, I., & Mu'min, M. A. (2024). Mitigation from SQL Injection Attacks on Web Server using Open Web Application Security Project Framework. International Journal of Engineering, 37(4), 635-645.

Ferdous, J., Islam, R., Mahboubi, A., & Islam, M. Z. (2023). A State-of-the-Art Review of Malware Attack Trends and Defense Mechanism. IEEE Access. https://doi.org/10.1109/ACCESS.2023.3328351

Ghanbari, H., & Koskinen, K. (2024). When data breach hits a psychotherapy clinic: The Vastaamo case. Journal of Information Technology Teaching Cases. https://doi.org/10.1177/20438869241258235

Gil, A. C. (2023). Como elaborar projetos de pesquisa. 7. Ed. . Editora Atlas.

Gonzalez-Granadillo, G., Menesidou, S. A., Papamartzivanos, D., Romeu, R., Navarro-Llobet, D., Okoh, C., & Panaousis, E. (2021). Automated cyber and privacy risk management toolkit. Sensors, 21(16), 5493. https://doi.org/10.3390/s21165493

Horta, A., Holanda, R., & Marinho, R. (2022). A Multi-criteria Approach to Improve the Cyber Security Visibility Through Breach Attack Simulations. In Anais do XXII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (pp. 330-343). SBC.

IBM. (2024). Cost of a Data Breach Report 2024. https://www.ibm.com/reports/data-breach.

International Organization for Standardization (ISO). (2024). ISO - ISO/IEC 27000 family — Information security management. https://www.iso.org/standard/iso-iec-27000-family

Juma, A. H., Arman, A. A., & Hidayat, F. (2023). Cybersecurity Assessment Framework: A Systematic Review. In 2023 10th International Conference on ICT for Smart Society (ICISS) (pp. 1-6). IEEE. 10.1109/ICISS59129.2023.10291832.

Kamiya, S., Kang, J., Kim, J., Milidonis, A. & Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics, 139(3), 719-749. https://dx.doi.org/10.1016/j.jfineco.2019.05.019.

Kern, M., Landauer, M., Skopik, F., & Weippl, E. (2024). A logging maturity and decision model for the selection of intrusion detection cyber security solutions. Computers & Security, 141, 103844. https://doi.org/10.1016/j.cose.2024.103844

Leszczyna, R. (2021). Review of cybersecurity assessment methods: Applicability perspective. Computers & Security, 108, 102376.

Lima, E. D., Moreira, F. R., Deus, F. E., Nze, G. D., Sousa, R. T., & Nunes, R. R. (2022). Avaliação da rotina operacional do operador nacional do sistema elétrico brasileiro (ONS) em relação às ações de gerenciamento de riscos associados à segurança cibernética. RISTI- Revista Iberica de Sistemas e Tecnologia de Informação, E49, 301-312.

MITRE. (2024). MITRE ATT&CK. Mitre Corporation. https://attack.mitre.org/resources/versions/

Mohammed, Z. (2022). Data breach recovery areas: an exploration of organization's recovery strategies for surviving data breaches. Organizational Cybersecurity Journal: Practice, Process and People, 2(1), 41-59. https://doi.org/10.1108/OCJ-05-2021-0014

NIST. (2024a). National Institute of Standards and Technology. Special Publications (SP). NIST Computer Security Resource Center. https://csrc.nist.gov/publications/sp

NIST. (2024b). National Institute of Standards and Technology. Web Server. NIST Computer Security Resource Center. https://csrc.nist.gov/glossary/term/web_server

NIST. (2024c). National Institute of Standards and Technology. Special Publications (SP). Measurement Guide for Information Security: Volume 1 — Identifying and Selecting Measures (NIST SP 800-55v1 ipd). https://doi.org/10.6028/NIST.SP.800-55v1.ipd.

OWASP. (2024). About OWASP. OWASP Foundation. https://owasp.org/about/

Song, L., & García-Valls, M. (2022). Improving security of web servers in critical IoT systems through self-monitoring of vulnerabilities. Sensors, 22(13), 5004.

Tsiodra, M., Panda, S., Chronopoulos, M., & Panaousis, E. (2023). Cyber risk assessment and optimization: A small business case study. IEEE Access, 11, 44467-44481. https://doi.org/10.1109/ACCESS.2023.3272670

Verizon. (2023). 2023 Data Breach Investigations Report. https://www.verizon.com/business/resources/T94e/reports/2023-data-breach-investigations-report-dbir.pdf