DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Auditoria Reproduzível de Firmware em Pontos de Acesso Sem Fio: uma análise para a Governança de Cibersegurança em Ambientes Institucionais

Leonardo de Paiva Souza

Programa de Pós-Graduação Profissional em Engenharia Elétrica

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Auditoria Reproduzível de Firmware em Pontos de Acesso Sem Fio: uma análise para a Governança de Cibersegurança em Ambientes Institucionais

Leonardo de Paiva Souza

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

PUBLICAÇÃO: PPEE.MP.117

Banca Examinadora

Prof. Dr. Georges Daniel Amvame Nze, ENE/FT/UnB
Orientador _____

Prof. Dr. Fábio Lúcio Lopes de Mendonça, ENE/FT/UnB
Examinador Interno _____

Prof. Dr. Francisco Lopes Caldas, IESB
Examinador Externo _____

FICHA CATALOGRÁFICA

SOUZA, LEONARDO DE PAIVA
Auditoria Reproduzível de Firmware em Pontos de Acesso Sem Fio: uma análise para a Governança de Cibersegurança em Ambientes Institucionais [Distrito Federal] 2026.
xi, 84 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2026).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Pontos de Acesso Sem Fio
2. Segurança de Firmware
3. Análise Estática
4. Governança de Cibersegurança
I. ENE/FT/UnB
II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

SOUZA, L. P. (2026). *Auditoria Reproduzível de Firmware em Pontos de Acesso Sem Fio: uma análise para a Governança de Cibersegurança em Ambientes Institucionais*. Dissertação de Mestrado Profissional, Publicação: PPEE.MP.117, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 84 p.

Leonardo de Paiva Souza
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Dedico este trabalho à minha esposa, Alline Silva Paes Landim, pelo amor, pela paciência e pelo apoio constante durante toda esta caminhada.

À minha mãe, Almeí de Paiva Lima, em memória, por ter sido uma presença extraordinária em minha vida. Seu amor, sua força e seus ensinamentos continuam comigo e fazem parte desta conquista.

À minha avó, Maria Anié Ferreira de Sousa, pelo carinho, pela sabedoria e pelos valores que ajudaram a formar quem sou.

Dedico também a toda a minha família, que, de diferentes formas, esteve presente nesta trajetória e contribuiu para que este momento fosse possível.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, pela força, pela saúde e pela perseverança concedidas ao longo desta caminhada.

Ao meu orientador, Prof. Dr. Georges Daniel Amvame Nze, pela orientação, paciência, disponibilidade e pelas contribuições fundamentais para o desenvolvimento deste trabalho. Suas observações foram essenciais para o amadurecimento da pesquisa e para a construção desta dissertação.

Aos membros da banca examinadora, Prof. Dr. Fábio Lúcio Lopes de Mendonça e Prof. Dr. Francisco Lopes Caldas, pela disponibilidade em participar deste momento e pelas contribuições ao aprimoramento deste trabalho.

À minha esposa, Alline Silva Paes Landim, pelo amor, companheirismo, apoio e compreensão durante todo este período. Sua presença foi fundamental para que eu pudesse seguir em frente, mesmo nos momentos mais difíceis.

À minha mãe, Almeí de Paiva Lima, em memória, por todo amor, dedicação, exemplo e ensinamentos deixados ao longo da minha vida. Sua trajetória permanece viva em mim e faz parte desta conquista.

À minha avó, Maria Anié Ferreira de Sousa, pelo carinho, pela sabedoria e pelos valores transmitidos, que contribuíram para minha formação pessoal e humana.

A toda a minha família, pelo incentivo, apoio e compreensão ao longo desta jornada.

Ao Programa de Pós-Graduação Profissional em Engenharia Elétrica da Universidade de Brasília, aos professores e servidores envolvidos, pelo suporte acadêmico e institucional durante o curso.

Por fim, agradeço a todos que, direta ou indiretamente, contribuíram para a realização deste trabalho.

RESUMO

A dependência de equipamentos de rede sem fio amplia a superfície de ataque das infraestruturas digitais e torna a segurança de firmware relevante para a continuidade de serviços institucionais. Esta dissertação concentra-se em pontos de acesso sem fio e equipamentos de rede sem fio com firmware embarcado, responsáveis por funções de conectividade, segmentação e controle de tráfego e que frequentemente operam com baixa transparência sobre componentes internos, atualizações e mecanismos de suporte.

A pesquisa combina revisão narrativa orientada pelo problema, análise documental de referenciais técnicos e normativos, reinterpretação crítica de uma base empírica previamente publicada com quatro imagens de firmware e uma reprodução técnica complementar e direcionada, realizada em julho de 2026 para recomposição da trilha documental. A reprodução confirmou os hashes das imagens, registrou ambiente, ferramentas, comandos e escopo de análise e preservou relatórios verificáveis. O cve-bin-tool correlacionou o componente curl/libcurl 7.79.1 do firmware TP-Link a 31 registros de CVE, tratados como candidatos que exigem validação contextual. A análise textual com Semgrep produziu 1.516 ocorrências brutas, posteriormente reduzidas, por inspeção e consolidação, a 11 achados estáticos: quatro relacionados a material criptográfico, três a credenciais padrão e quatro à exposição potencial de credenciais em registros. A matriz documental resultante reúne 42 registros, sem atribuir automaticamente explorabilidade ou exposição em rede.

Como contribuição principal, propõe-se o MARF-GC (Modelo para Auditoria Reproduzível de Firmware para Governança de Cibersegurança), concebido como camada complementar entre produção de evidências técnicas, validação operacional e decisão institucional. O modelo organiza entradas, entregáveis, atores, critérios de risco, tratamento, responsabilização e reauditoria. Sua aplicação permanece retrospectiva e ilustrativa, constituindo avaliação preliminar de aplicabilidade, e não validação empírica de efetividade.

Palavras-chave: Pontos de Acesso Sem Fio; Segurança de Firmware; Análise Estática; Governança de Cibersegurança; Reprodutibilidade.

ABSTRACT

Dependence on wireless network equipment expands the attack surface of digital infrastructures and makes firmware security relevant to institutional service continuity. This dissertation focuses on wireless access points and wireless network equipment with embedded firmware that provide connectivity, segmentation, and traffic-control functions while often offering limited transparency regarding internal components, updates, and support mechanisms.

The research combines a problem-oriented narrative review, documentary analysis of technical and normative references, critical reappraisal of a previously published empirical dataset involving four firmware

images, and a complementary directed reproduction performed in July 2026 to reconstruct the documentary trail. The reproduction confirmed image hashes, recorded the environment, tools, commands, and analysis scope, and preserved verifiable reports. CVE Binary Tool correlated the curl/libcurl 7.79.1 component found in the TP-Link firmware with 31 public CVE records, treated as candidates requiring contextual validation. Semgrep-based textual analysis produced 1,516 raw matches, later reduced through inspection and consolidation to 11 static findings: four related to cryptographic material, three to default credentials, and four to potential credential exposure in logs. The resulting documentary matrix contains 42 records without automatically claiming exploitability or network exposure.

As its main contribution, this work proposes MARF-GC (Model for Reproducible Firmware Auditing for Cybersecurity Governance), conceived as a complementary layer between technical evidence production, operational validation, and institutional decision-making. The model organizes inputs, mandatory deliverables, actors, risk criteria, treatment, accountability, and reassessment. Its application remains retrospective and illustrative, representing a preliminary assessment of applicability rather than an empirical validation of effectiveness.

Keywords: Wireless Access Points; Firmware Security; Static Analysis; Cybersecurity Governance; Reproducibility.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1 INTRODUÇÃO

Em ambientes institucionais, dispositivos de rede sem fio constituem elementos permanentes da infraestrutura digital. Pontos de acesso, roteadores sem fio, gateways e outros equipamentos com software embarcado sustentam conectividade, segmentação, autenticação e acesso a serviços, muitas vezes operando continuamente e com forte dependência de firmware para inicialização, configuração, comunicação e controle. Nesse contexto, a segurança de firmware deixa de ser uma questão restrita ao fabricante e passa a representar um aspecto relevante para a proteção e a continuidade das infraestruturas digitais.

Esses equipamentos coexistem com outros sistemas embarcados e dispositivos conectados que compõem ecossistemas mais amplos de Internet das Coisas (IoT). Nesta dissertação, entretanto, IoT é empregado como contexto tecnológico ampliado e não como sinônimo do objeto empírico analisado. O recorte do trabalho concentra-se em dispositivos de rede sem fio, especialmente pontos de acesso e equipamentos com funções de roteamento e conectividade. Essa distinção é importante porque nem todo roteador ou ponto de acesso é classificado como dispositivo IoT em todas as taxonomias, embora compartilhe características relevantes com sistemas embarcados conectados, como dependência de firmware, operação contínua e integração com serviços de rede [2, 3].

A literatura especializada tem demonstrado que firmwares de sistemas embarcados e equipamentos de rede podem apresentar fragilidades como credenciais embutidas, bibliotecas desatualizadas, serviços inseguros e falhas na integração de componentes de terceiros. A heterogeneidade arquitetural desses equipamentos, associada à dificuldade de atualização e à baixa transparência sobre componentes internos, agrava o problema e torna a auditoria de firmware uma atividade relevante para avaliação de segurança [4, 5, 6, 7].

Esta dissertação dialoga diretamente com o estudo *Auditable Security Assessment of Proprietary and Open-Source Wi-Fi Router Firmware: A Reproducible Approach for Academic Infrastructures* [1]. Esse estudo analisou quatro imagens de firmware — TP-Link Archer C7 (US) v5.0, D-Link DIR-842 R1, Intelbras RG1200 e OpenWrt 22.03.5 — comparando soluções proprietárias e de código aberto. Os equipamentos analisados acumulam funções de roteamento e acesso sem fio; por isso, o recorte empírico desta dissertação é tratado como composto por dispositivos de rede sem fio, com ênfase em pontos de acesso, sem generalização para todo o universo de dispositivos conectados.

O estudo de base publicou contagens agregadas de componentes e versões correlacionados a registros de CVE, além de achados relacionados a configurações e serviços. Nesta dissertação, essas correlações são tratadas como indicadores técnicos que exigem contextualização e, quando necessário, validação complementar; não são interpretadas automaticamente como vulnerabilidades exploráveis. A análise desenvolvida amplia a discussão ao articular essas evidências com auditabilidade, gestão de riscos e governança de cibersegurança em ambientes institucionais.

Essa perspectiva parte do entendimento de que a segurança de dispositivos de rede sem fio não deve ser analisada apenas sob a ótica de vulnerabilidades isoladas, mas também considerando sua interdependência com redes, serviços e práticas institucionais de proteção de ativos, segmentação, controle de acesso, monitoramento e continuidade operacional. Estudos recentes indicam que falhas em firmware podem atuar

como vetores de comprometimento transversal, permitindo escalonamento de privilégios, movimentação lateral e degradação da disponibilidade de serviços críticos em ambientes organizacionais [7, 8]. Diferentemente de trabalhos focados exclusivamente em análise técnica ou experimentação laboratorial, esta dissertação enfatiza a articulação entre segurança de firmware, auditabilidade e governança institucional, destacando a produção de evidências como elemento central para a gestão de riscos em infraestruturas dependentes de dispositivos de rede sem fio.

1.1 PROBLEMA DE PESQUISA

Apesar da crescente dependência de pontos de acesso sem fio e outros equipamentos de rede embarcados em ambientes institucionais, responsáveis pela conectividade e pelo suporte a serviços digitais, ainda existem limitações relevantes na capacidade organizacional de avaliar os riscos associados ao firmware desses dispositivos de forma sistemática, reproduzível e auditável.

Em muitos contextos, a segurança desses ativos permanece fortemente dependente de fornecedores, da disponibilidade de atualizações e da existência de documentação técnica limitada, o que reduz a capacidade de verificação independente por parte das instituições. Como consequência, vulnerabilidades presentes na camada de firmware podem permanecer invisíveis aos processos tradicionais de gestão de riscos, comprometendo a continuidade operacional, a segmentação lógica da rede, a proteção de serviços críticos e a própria governança de cibersegurança.

Diante desse cenário, esta dissertação parte do seguinte problema de pesquisa:

Como a auditoria reproduzível de firmware em pontos de acesso sem fio pode ampliar a capacidade institucional de avaliação de riscos e apoiar a governança de cibersegurança?

1.2 OBJETIVO GERAL

Analisar a segurança de firmware em pontos de acesso sem fio e discutir suas implicações para a governança de cibersegurança em ambientes institucionais.

1.3 OBJETIVOS ESPECÍFICOS

1. Revisar a literatura recente sobre segurança de firmware, sistemas embarcados e vulnerabilidades em equipamentos de rede sem fio;
2. Sistematizar conceitos, técnicas, fragilidades recorrentes e desafios associados à análise e à auditabilidade de firmware;
3. Retomar e reinterpretar criticamente evidências empíricas previamente produzidas sobre firmwares proprietários e de código aberto, à luz da governança de cibersegurança;

4. Discutir a relação entre auditoria reproduzível de firmware, engenharia de segurança, auditabilidade e gestão de riscos, bem como sua complementaridade com scanners, testes de intrusão e operações Red, Blue e Purple Team;

5. Propor o modelo conceitual MARF-GC como estrutura analítica para articulação entre auditoria de firmware, produção de evidências e governança de cibersegurança;

6. Formular diretrizes institucionais para governança de firmware em pontos de acesso sem fio e equipamentos de rede embarcados.

1.4 PROPOSIÇÃO CENTRAL DA PESQUISA

Parte-se da proposição de que a auditoria reproduzível de firmware, quando articulada à produção sistemática de evidências técnicas e à sua interpretação no contexto organizacional, pode ampliar a capacidade institucional de avaliação de riscos e fortalecer processos de governança de cibersegurança em ambientes dependentes de equipamentos de rede sem fio. Em outras palavras, a hipótese subjacente a esta dissertação é que a auditabilidade do firmware não constitui apenas um recurso técnico de diagnóstico, mas um elemento capaz de apoiar decisões institucionais sobre atualização, aquisição, segmentação, substituição e proteção de ativos conectados.

1.5 JUSTIFICATIVA

Esta dissertação justifica-se pela necessidade de ampliar a compreensão sobre mecanismos reproduzíveis de análise de firmware e suas implicações para a governança institucional da cibersegurança. Ao articular segurança de firmware, auditabilidade, produção de evidências e gestão de riscos, o estudo busca contribuir para práticas que favoreçam maior capacidade institucional de interpretação, monitoramento e tomada de decisão em ambientes organizacionais dependentes de dispositivos de rede sem fio.

A relevância do tema torna-se particularmente evidente em universidades, centros de pesquisa e órgãos públicos, nos quais a infraestrutura de rede tende a combinar heterogeneidade tecnológica, restrições orçamentárias, múltiplos fornecedores e dependência crescente de equipamentos conectados para suporte a atividades acadêmicas, administrativas e laboratoriais. Nesses contextos, falhas de firmware não representam apenas um problema de configuração local ou de manutenção, mas um risco com potencial de afetar disponibilidade de serviços, segmentação lógica, proteção de dados e continuidade operacional. Discutir segurança de firmware sob a ótica da governança de cibersegurança permite, portanto, deslocar o debate de uma visão centrada apenas no fabricante para uma perspectiva orientada à gestão institucional de riscos.

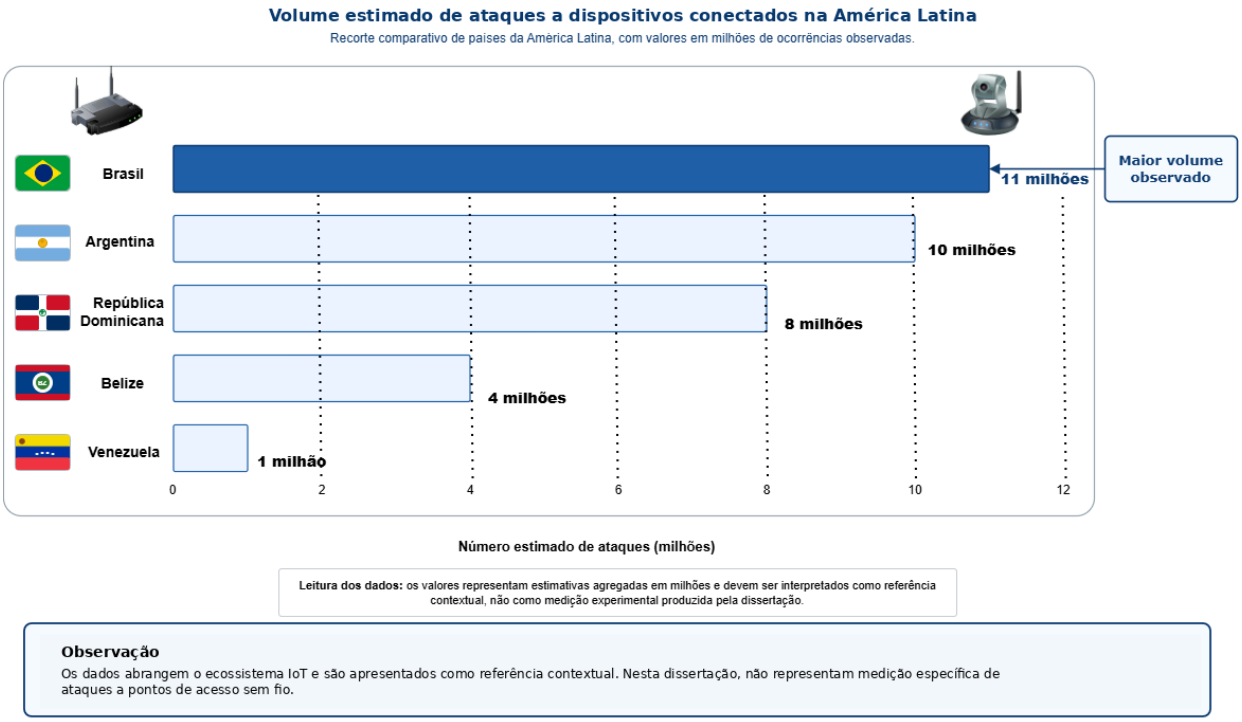

Figura 1: Indicador contextual de ataques a dispositivos conectados na América Latina.

Fonte: Elaborado pelo autor, com base em dados da Kaspersky divulgados por Crypto ID [9].

A Figura 1 apresenta dados agregados sobre ataques a dispositivos do ecossistema IoT na América Latina. Esses dados não medem exclusivamente ataques a pontos de acesso sem fio e, por isso, são utilizados apenas como contexto ampliado do ambiente de dispositivos conectados no qual roteadores, gateways e outros equipamentos de rede podem estar inseridos. Segundo dados da Kaspersky divulgados pela Crypto ID, o Brasil registrou aproximadamente 11 milhões de tentativas de ataques direcionadas a dispositivos IoT no recorte divulgado [9]. O dado reforça a necessidade de tratar equipamentos conectados como parte de uma superfície de ataque mais ampla, sem transferir automaticamente essa estatística para o conjunto específico de firmwares analisado nesta dissertação.

Sob a perspectiva institucional, o ponto relevante para este trabalho está nos mecanismos de inventário de equipamentos de rede, segmentação, autenticação robusta, atualização contínua e monitoramento de tráfego. Tais mecanismos aproximam a segurança de firmware da gestão de riscos organizacional e da governança de cibersegurança, pois vulnerabilidades na camada embarcada podem afetar diretamente continuidade operacional, segurança da informação e resiliência institucional.

Ao final, esta dissertação busca oferecer duas contribuições concretas para universidades federais, órgãos públicos e demais instituições dependentes de infraestrutura de rede sem fio: (i) o modelo MARF-GC, como instrumento analítico para conectar auditoria de firmware a decisões institucionais; e (ii) um conjunto de diretrizes que podem orientar políticas de inventário, atualização e aquisição de equipamentos de

rede em contextos como Institutos Federais de Educação, unidades do SISP e Núcleos de Tecnologia da Informação (NTIs) de universidades.

Embora a literatura sobre segurança de firmware em sistemas embarcados e dispositivos conectados tenha avançado significativamente na identificação de vulnerabilidades, na automação de auditorias e na análise de componentes, grande parte desses estudos permanece concentrada na dimensão estritamente técnica do problema. Esta dissertação parte de uma perspectiva complementar. Em vez de tratar a auditoria de firmware apenas como mecanismo de detecção de fragilidades, o trabalho a interpreta como fonte de evidências relevantes para processos institucionais de avaliação de riscos, definição de prioridades de segurança e tomada de decisão sobre infraestrutura de rede.

Nesse sentido, a contribuição central desta pesquisa está na articulação entre três dimensões que frequentemente aparecem dissociadas na literatura: (i) a análise reproduzível de firmware como prática de produção de evidências técnicas; (ii) a governança de cibersegurança como estrutura organizacional de direcionamento, priorização e gestão de riscos; e (iii) o contexto institucional no qual pontos de acesso e outros equipamentos de rede sem fio sustentam serviços críticos e ampliam a superfície de ataque das organizações.

Além da separação entre literatura técnica e referenciais de governança, existe uma segunda descontinuidade: scanners, testes de intrusão, análise dinâmica e equipes ofensivas ou defensivas produzem validações importantes, mas seus resultados nem sempre são vinculados a um registro institucional de responsabilidade, prazo, tratamento, risco residual e reauditoria. O MARF-GC é posicionado nessa interface, como camada complementar que organiza a passagem entre evidências internas do firmware, validações operacionais e decisão institucional documentada.

1.6 ESTRUTURA DA DISSERTAÇÃO

Além desta introdução, a dissertação está organizada da seguinte forma. O Capítulo 2 apresenta a fundamentação teórica, abordando dispositivos de rede sem fio, sistemas embarcados, o contexto ampliado de IoT, segurança de firmware, vulnerabilidades recorrentes e governança de cibersegurança. O Capítulo 3 descreve a metodologia adotada. O Capítulo 4 apresenta a discussão dos resultados e das implicações institucionais do tema. Por fim, o Capítulo 5 expõe as conclusões e os encaminhamentos para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 DISPOSITIVOS DE REDE SEM FIO E SISTEMAS EMBARCADOS

Em ambientes institucionais, dispositivos de rede sem fio incluem pontos de acesso, roteadores sem fio, gateways, nós de redes em malha e outros equipamentos responsáveis por prover ou intermediar conectividade. Muitos desses ativos são implementados sobre plataformas embarcadas, combinando processadores de propósito específico ou geral, memória não volátil, interfaces de comunicação e software de baixo nível responsável pela operação do equipamento.

A Internet das Coisas (IoT) constitui um ecossistema mais amplo de dispositivos conectados, que pode incluir sensores, atuadores, controladores, câmeras, gateways e, em determinados contextos, equipamentos de rede [2, 3]. Para evitar ambiguidade terminológica, esta dissertação não utiliza IoT como sinônimo do objeto empírico. O objeto analisado é composto por dispositivos de rede sem fio com firmware embarcado; referências a IoT são mantidas quando necessárias para discutir literatura, normas, ameaças ou ecossistemas de dispositivos conectados.

Pontos de acesso sem fio têm como função principal disponibilizar conectividade de rede a clientes por meio de interfaces sem fio. Roteadores sem fio podem acumular, no mesmo equipamento, funções de roteamento, NAT, filtragem, administração e acesso sem fio. Gateways e controladores acrescentam outras funções de intermediação e gerenciamento. Embora essas categorias possuam papéis distintos, compartilham características relevantes para esta pesquisa: operação contínua, dependência de firmware, exposição a serviços de rede, integração com infraestrutura institucional e necessidade de atualização e rastreabilidade.

A literatura recente aponta que a análise de segurança de sistemas embarcados exige atenção a características como heterogeneidade arquitetural, dependência de hardware, baixa transparência de implementação e forte reutilização de componentes de software [8, 10]. Essas características também são relevantes para equipamentos de rede sem fio, nos quais vulnerabilidades em bibliotecas, serviços, credenciais ou mecanismos de atualização podem afetar não apenas o dispositivo isolado, mas a conectividade e os serviços dependentes dele.

2.2 ARQUITETURA DE DISPOSITIVOS DE REDE SEM FIO COM FIRMWARE EMBARCADO

Dispositivos de rede sem fio com software embarcado apresentam arquiteturas compostas por múltiplos componentes de hardware e software. Em termos gerais, incluem processador ou sistema em chip, memória não volátil, interfaces de rede, módulos de rádio e componentes responsáveis pelo armazenamento e execução do firmware. Dependendo do equipamento, podem coexistir funções de acesso sem fio, roteamento, firewall, administração, monitoramento e serviços auxiliares.

A arquitetura lógica desses dispositivos é normalmente organizada em camadas. Na base encontra-se o hardware embarcado, responsável pela execução das instruções e pela interface com periféricos e interfaces de comunicação. Sobre essa camada opera o firmware, que pode incluir bootloader, kernel de sistema operacional embarcado, drivers, bibliotecas, serviços de rede e aplicações responsáveis pela lógica de controle. Sistemas baseados em Linux embarcado são comuns em equipamentos de rede mais complexos, incluindo roteadores, gateways e pontos de acesso.

A reutilização de bibliotecas de terceiros, serviços e módulos facilita o desenvolvimento, mas também amplia a superfície de ataque quando componentes vulneráveis ou desatualizados são incorporados ao firmware [8, 10]. Essa composição justifica a análise de firmware como mecanismo de visibilidade sobre elementos internos que nem sempre podem ser inferidos apenas por observação da rede.

O ecossistema IoT permanece relevante como contexto comparativo e normativo, pois parte da literatura e dos referenciais de segurança trata conjuntamente dispositivos conectados, sistemas embarcados e equipamentos de rede. Entretanto, as categorias não são equivalentes. Nesta dissertação, o termo *dispositivo de rede sem fio* é utilizado para o objeto técnico sob análise, enquanto IoT é reservado ao ecossistema mais amplo quando a fonte ou o fenômeno discutido assim o exigir.

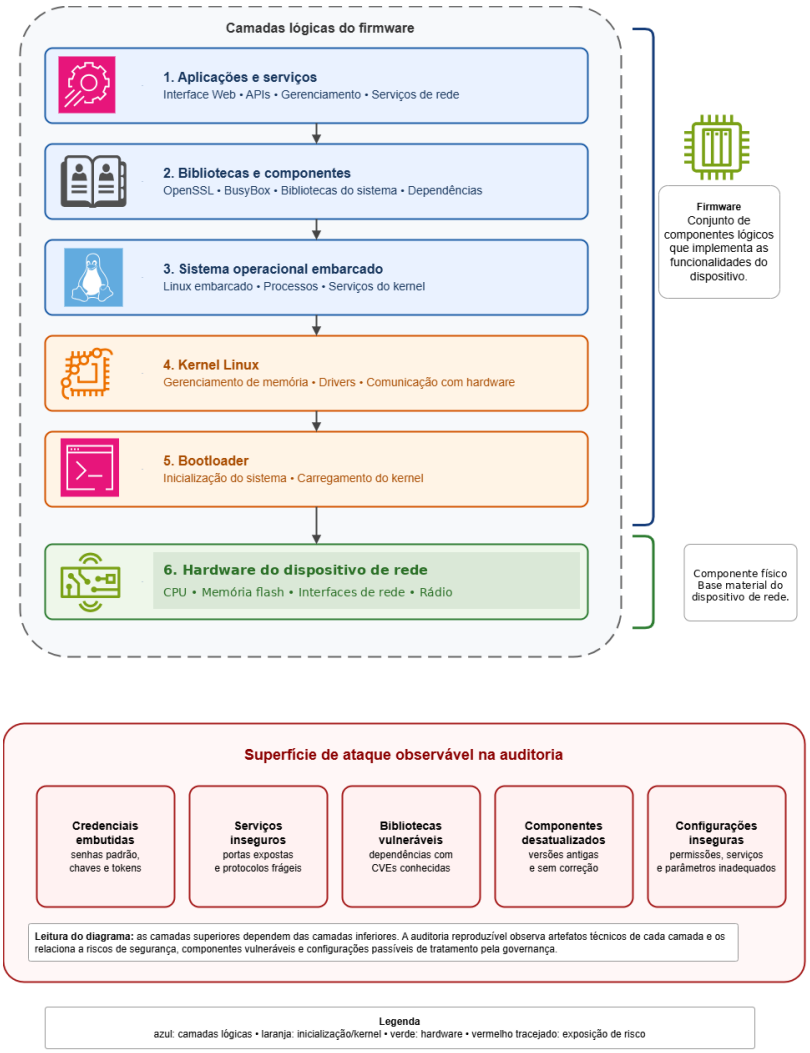

Figura 2: Arquitetura em camadas de um dispositivo de rede sem fio com firmware embarcado.

Fonte: Elaborado pelo autor (2026).

A Figura 2 apresenta uma arquitetura em camadas utilizada como referência conceitual para sistemas embarcados conectados. No recorte desta dissertação, a leitura da figura é direcionada aos componentes relevantes em equipamentos de rede sem fio: hardware, bootloader, kernel, bibliotecas, serviços e aplicações. Vulnerabilidades podem surgir em diferentes pontos dessa pilha, desde componentes reutilizados até serviços expostos na camada de aplicação.

2.3 SEGURANÇA DE FIRMWARE

O firmware representa uma das camadas mais críticas de segurança em dispositivos de rede sem fio e sistemas embarcados, frequentemente negligenciada durante o desenvolvimento, a implantação e a manutenção dos equipamentos. Vulnerabilidades nessa camada podem permitir comprometimento persistente, exploração em larga escala e permanência de falhas conhecidas ao longo do ciclo de vida operacional do dispositivo [7].

Estudos recentes indicam que a segurança de firmware envolve tanto desafios técnicos de identificação de vulnerabilidades quanto questões associadas à auditabilidade, transparência, atualização e manutenção contínua de dispositivos de rede e sistemas embarcados. Como o firmware ocupa posição central na operação desses sistemas, falhas nessa camada podem comprometer mecanismos de autenticação, serviços de administração, comunicação em rede, integridade de arquivos e a própria disponibilidade do equipamento [4].

Nesse contexto, a análise estática se destaca como uma abordagem particularmente relevante, sobretudo em cenários nos quais há limitações de hardware, custo ou reprodutibilidade que dificultam a validação dinâmica. Ao permitir a inspeção de imagens de firmware sem necessidade de execução direta no dispositivo, essa estratégia favorece a identificação de bibliotecas vulneráveis, scripts inseguros, credenciais embutidas, configurações potencialmente sensíveis e componentes de terceiros reutilizados. Além disso, por possibilitar procedimentos documentáveis e repetíveis, a análise estática contribui para a produção de evidências técnicas auditáveis, aspecto relevante tanto para estudos acadêmicos quanto para processos institucionais de avaliação de risco [7, 11, 10, 8].

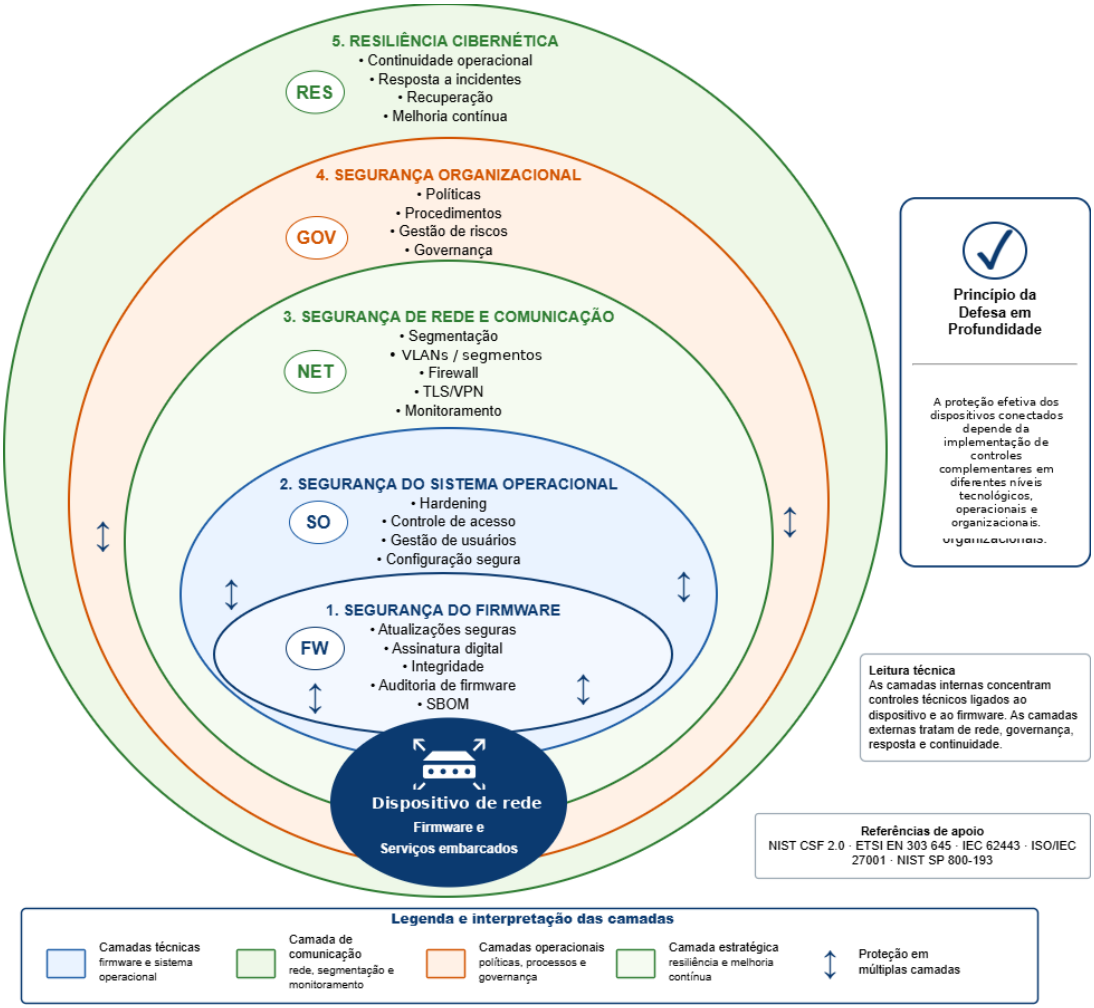

Figura 3: Arquitetura conceitual de segurança para dispositivos de rede sem fio e sistemas embarcados, ilustrando o princípio de defesa em profundidade aplicado ao firmware e à infraestrutura embarcada.

Fonte: Elaborado pelo autor (2026).

A Figura 3 apresenta uma arquitetura conceitual de segurança para dispositivos conectados e sistemas embarcados. Nesse modelo, a proteção é distribuída em múltiplas camadas, incluindo mecanismos de *secure boot*, validação de integridade do firmware, autenticação, comunicação criptografada e monitoramento contínuo da infraestrutura. Essa abordagem de defesa em profundidade é coerente com recomendações da literatura para reduzir riscos em ecossistemas IoT [12, 13, 3].

Além dos mecanismos tradicionais de segurança em redes, a proteção do firmware tornou-se um elemento crítico na segurança de dispositivos de rede sem fio e outros sistemas embarcados. Técnicas como Secure Boot, verificação criptográfica de firmware e mecanismos seguros de atualização OTA (Over-The-Air) são frequentemente utilizadas para garantir a integridade do software embarcado. Esses mecanismos buscam impedir a execução de firmware não autorizado, reduzindo o risco de comprometimento do dispositivo por malware ou modificações maliciosas [12, 2].

2.4 DESAFIOS DE SEGURANÇA EM DISPOSITIVOS DE REDE SEM FIO E SISTEMAS EMBARCADOS

A expansão de dispositivos conectados e de equipamentos de rede sem fio tem ampliado significativamente a superfície de ataque em ambientes digitais. Muitos desses ativos operam de forma contínua, utilizam software embarcado e apresentam limitações de transparência, atualização ou capacidade de monitoramento. Esses fatores podem aumentar a exposição a ataques cibernéticos e comprometer não apenas dispositivos individuais, mas também infraestruturas inteiras conectadas em rede.

De acordo com [2], a arquitetura de IoT envolve múltiplas camadas de interação entre dispositivos físicos, sistemas embarcados e serviços em rede. Cada uma dessas camadas pode apresentar vulnerabilidades específicas, desde falhas de autenticação até erros de implementação em firmware e bibliotecas de software.

Roman et al. [12] destacam que os principais desafios de segurança em IoT incluem restrições computacionais, heterogeneidade de dispositivos e ausência de mecanismos padronizados de atualização segura. Tais limitações dificultam a implementação de mecanismos robustos de proteção, como criptografia avançada e monitoramento contínuo.

Além disso, equipamentos de rede e sistemas embarcados são implantados em ambientes críticos, incluindo infraestruturas institucionais, redes industriais e ecossistemas IoT. Nesses cenários, vulnerabilidades em firmware podem permitir a execução de código malicioso, comprometendo a integridade e disponibilidade dos serviços oferecidos pelos dispositivos [14]. Na prática, isso faz com que a segurança de firmware se torne um componente central na proteção de sistemas embarcados e infraestruturas de rede.

2.5 SEGURANÇA NA CADEIA DE SUPRIMENTOS DE FIRMWARE

A cadeia de suprimentos de software tem sido reconhecida como um dos vetores mais críticos de ataque em sistemas modernos. No contexto de dispositivos de rede e sistemas embarcados, o firmware

frequentemente incorpora componentes provenientes de múltiplas fontes, incluindo bibliotecas de código aberto, drivers e módulos desenvolvidos por terceiros.

Segundo [4], a reutilização extensiva de componentes de software em firmware embarcado pode introduzir vulnerabilidades herdadas, especialmente quando versões desatualizadas de bibliotecas são incorporadas aos sistemas. A análise em larga escala conduzida pelos autores demonstrou que milhares de imagens de firmware compartilham bibliotecas vulneráveis, ampliando significativamente o risco de exploração. Esse problema é ampliado pelo uso intensivo de componentes de terceiros em firmware, o que introduz riscos adicionais relacionados à cadeia de suprimentos de software, frequentemente explorados em ataques direcionados a sistemas embarcados [5].

Além disso, falhas na gestão da cadeia de suprimentos podem resultar na distribuição de firmware comprometido ou adulterado. Ataques direcionados à cadeia de desenvolvimento e distribuição de software têm sido observados em diversos setores, destacando a necessidade de mecanismos de verificação de integridade e autenticação de firmware [15].

Outro elemento cada vez mais relevante nesse contexto é o uso de SBOM (*Software Bill of Materials*), ou lista de materiais de software. O SBOM consiste em um inventário estruturado dos componentes que compõem um software, incluindo bibliotecas, dependências, versões e fornecedores. Em firmware de dispositivos de rede e sistemas embarcados, esse tipo de documentação pode contribuir para aumentar a visibilidade sobre componentes reutilizados e facilitar a identificação de bibliotecas vulneráveis.

A ausência de SBOM ou de mecanismos equivalentes de rastreabilidade dificulta a avaliação de risco em firmwares proprietários, pois impede que equipes técnicas compreendam de forma precisa quais componentes estão presentes no dispositivo. Essa limitação torna mais complexa a correlação entre vulnerabilidades divulgadas publicamente e os componentes efetivamente embarcados no equipamento.

Em ambientes institucionais, a adoção de critérios relacionados a SBOM pode apoiar processos de aquisição, atualização e governança de dispositivos de rede sem fio e equipamentos embarcados. Ao exigir maior transparência sobre componentes de software, a organização passa a ter melhores condições de avaliar riscos de cadeia de suprimentos, priorizar atualizações e decidir pela substituição de equipamentos sem suporte adequado.

Assim, a rastreabilidade de componentes de firmware deve ser compreendida como requisito técnico e também como requisito de governança. Em vez de depender exclusivamente de declarações do fabricante, instituições podem utilizar informações sobre componentes, versões e dependências como evidências para gestão de riscos e planejamento de segurança.

Para mitigar esses riscos, práticas como assinatura digital de firmware, verificação de integridade criptográfica e mecanismos de atualização segura têm sido amplamente recomendadas por organizações de segurança e padrões internacionais. Esse cenário evidencia que a segurança de firmware não pode ser analisada de forma isolada, sendo necessário considerar todo o ecossistema de desenvolvimento e distribuição de software. A crescente dependência de componentes de terceiros reforça a necessidade de mecanismos de rastreabilidade, validação de dependências e auditoria contínua, especialmente em ambientes institucionais que demandam maior controle sobre sua infraestrutura tecnológica [15].

2.6 ATUALIZAÇÕES SEGURAS DE FIRMWARE

Atualizações de firmware desempenham um papel fundamental na manutenção da segurança de dispositivos de rede sem fio e sistemas embarcados. A capacidade de corrigir vulnerabilidades após a implantação do dispositivo permite reduzir riscos associados à exploração de falhas conhecidas.

Mecanismos de atualização Over-The-Air (OTA) são amplamente utilizados para distribuir novas versões de firmware remotamente. Entretanto, a implementação inadequada desses mecanismos pode introduzir novas vulnerabilidades, como a possibilidade de instalação de firmware malicioso ou adulterado [16, 12].

Uma abordagem amplamente recomendada envolve a utilização de assinaturas digitais para garantir a autenticidade do firmware distribuído. Nesse modelo, o dispositivo verifica a assinatura criptográfica do firmware antes de permitir sua instalação, assegurando que apenas versões autorizadas possam ser executadas [16].

Além disso, mecanismos de proteção como Secure Boot permitem garantir que o dispositivo execute apenas firmware confiável desde o processo inicial de inicialização. Essa técnica estabelece uma cadeia de confiança que protege o sistema contra modificações não autorizadas no software embarcado.

Dessa forma, a adoção de práticas seguras de atualização de firmware é essencial para garantir a resiliência e a confiabilidade de dispositivos de rede sem fio e sistemas embarcados ao longo de seu ciclo de vida operacional.

2.7 VULNERABILIDADES RECORRENTES EM FIRMWARE DE DISPOSITIVOS DE REDE SEM FIO

Estudos da área identificam um conjunto recorrente de fragilidades em firmware de dispositivos conectados e equipamentos de rede. Entre elas, destacam-se o uso de credenciais embutidas, bibliotecas desatualizadas, serviços inseguros expostos, falhas de validação de entrada, mecanismos inadequados de atualização e integração insegura de componentes de terceiros [4, 5, 6].

Também são frequentes problemas associados à complexidade interna do firmware, como interações entre múltiplos binários, reutilização de bibliotecas vulneráveis e baixa observabilidade dos fluxos de dados. Esses fatores dificultam a análise e contribuem para a persistência de falhas ao longo de diferentes fabricantes e versões de produto [17, 18].

Além dessas vulnerabilidades, também são comuns problemas relacionados à gestão inadequada de atualizações de firmware. Muitos dispositivos embarcados não implementam mecanismos seguros de verificação de integridade ou assinatura digital para atualizações, permitindo que firmware modificado seja instalado no dispositivo. Essa fragilidade pode ser explorada por atacantes para introduzir código malicioso ou persistência no equipamento.

Outro problema recorrente envolve a presença de serviços de rede desnecessários habilitados por padrão. Interfaces administrativas expostas, protocolos inseguros e configurações padrão fracas podem per-

mitir acesso não autorizado ao dispositivo. Esses fatores contribuem para a exploração em larga escala de dispositivos conectados vulneráveis em campanhas de botnets e ataques distribuídos [4, 12, 13].

2.8 BOTNETS E EXPLORAÇÃO DE DISPOSITIVOS CONECTADOS

O crescimento da Internet das Coisas também ampliou significativamente a superfície de ataque disponível na internet. Dispositivos como roteadores domésticos, câmeras IP, gravadores digitais e gateways frequentemente permanecem conectados continuamente e, em muitos casos, operam com firmware desatualizado ou com configurações de segurança inadequadas, tornando-se alvos recorrentes de campanhas de exploração em larga escala, como discutido em detalhe na Seção 2.16. O exemplo mais emblemático desse cenário é a botnet Mirai, identificada em 2016, que demonstrou como fragilidades aparentemente simples, como credenciais padrão e serviços expostos, podem ser exploradas para comprometer milhares de dispositivos e gerar impacto global [19, 20]. Esse cenário reforça a importância da análise sistemática de firmware como mecanismo de identificação antecipada de vulnerabilidades, retomada de forma sistematizada nesta dissertação.

2.9 ANÁLISE DE FIRMWARE

A análise de firmware pode ser conduzida por diferentes abordagens, incluindo análise estática, emulação, fuzzing e técnicas híbridas. No escopo desta dissertação, o foco está na análise estática, por ser uma abordagem viável, reproduzível e compatível com a proposta de consolidação teórica e documental do trabalho.

A análise estática permite inspecionar imagens de firmware, extrair sistemas de arquivos, identificar bibliotecas, localizar padrões inseguros, examinar scripts de inicialização, detectar más configurações e correlacionar achados com bases públicas de vulnerabilidades. Seu valor metodológico reside na capacidade de produzir evidências auditáveis sem exigir execução direta do firmware em hardware real [1, 21]. Apesar dessas vantagens, a análise estática apresenta limitações na identificação de comportamentos dinâmicos, o que reforça a necessidade de abordagens complementares em cenários mais complexos. Ainda assim, sua natureza reproduzível a torna especialmente relevante para auditorias e estudos acadêmicos [1, 21].

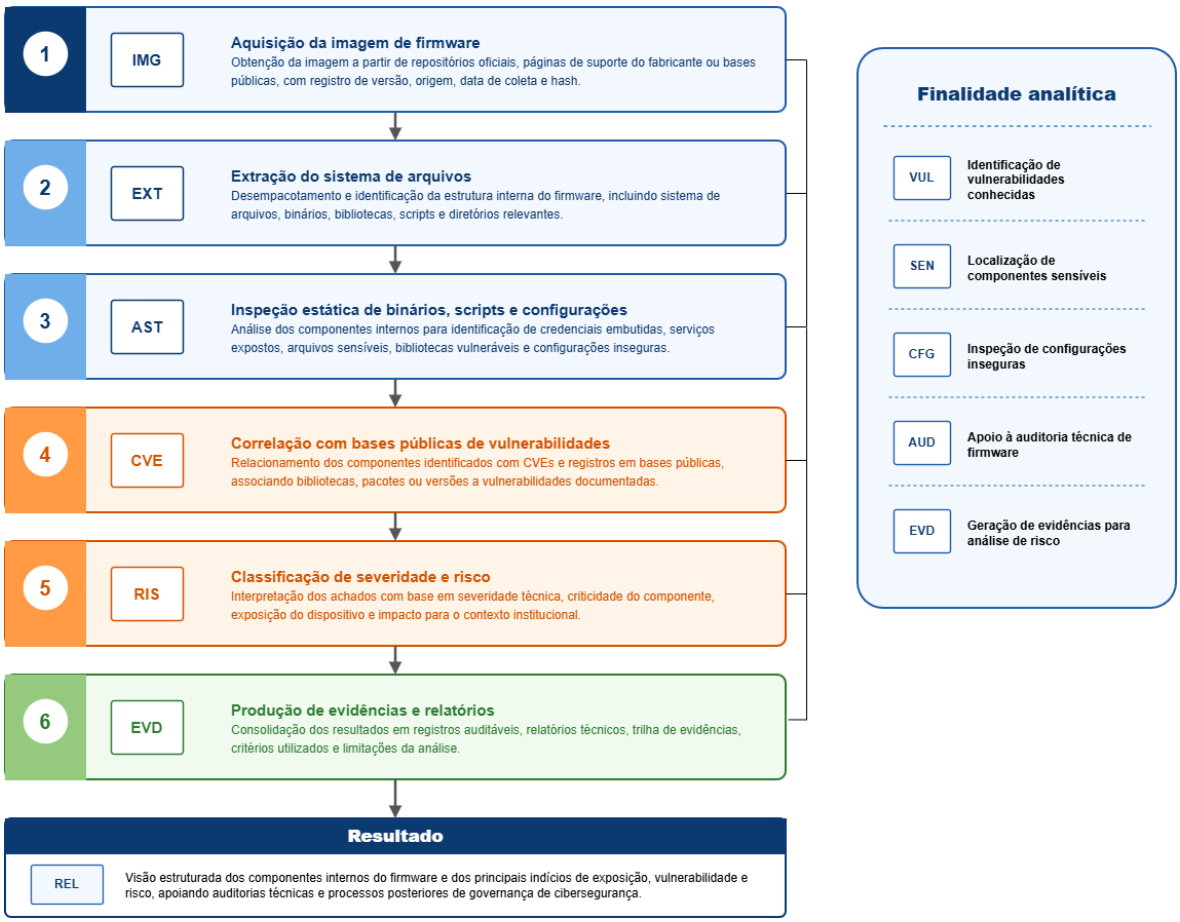

Figura 4: Fluxo simplificado de análise estática de firmware adotado em auditorias reproduzíveis.

Fonte: Elaborado pelo autor (2026).

A Figura 4 sintetiza as etapas conceituais de uma auditoria de firmware baseada em análise estática, desde a obtenção da imagem até a produção de evidências técnicas e relatórios.

Além de identificar vulnerabilidades específicas, a análise de firmware também contribui para compreender padrões estruturais de segurança presentes em diferentes dispositivos e fabricantes. Essa capacidade analítica permite avaliar riscos de forma mais abrangente, apoiando processos institucionais de auditoria, seleção tecnológica e definição de políticas de segurança.

2.10 COMPLEMENTARIDADE COM SCANNERS, TESTES DE INTRUSÃO E OPERAÇÕES DE SEGURANÇA

A análise estática de firmware é apenas uma das fontes possíveis de evidência sobre a segurança de um dispositivo conectado. Scanners de rede e de vulnerabilidades observam portas, serviços, banners, versões aparentes e configurações expostas durante a execução. Testes de intrusão e operações de Red Team podem verificar caminhos de ataque, exploração, encadeamento de falhas, persistência, movimentação lateral e impacto. A análise dinâmica, a emulação e o fuzzing, por sua vez, permitem observar comportamento em

execução e respostas a entradas que não podem ser inferidas apenas pela inspeção de arquivos [21, 22].

A análise estática possui uma vantagem complementar: pode revelar bibliotecas internas, scripts de inicialização, arquivos de configuração, credenciais embutidas, certificados, componentes de terceiros e mecanismos de atualização que não necessariamente ficam expostos pela rede. Essa visibilidade, entretanto, não comprova por si só que um componente seja utilizado, alcançável ou explorável no equipamento em operação. Uma correspondência entre componente, versão e CVE pode ser afetada por correções retroportadas, recursos desabilitados, diferenças de compilação ou ausência das condições necessárias à exploração.

O trabalho do Blue Team, do SOC e das equipes de infraestrutura transforma evidências e validações em controles defensivos, como segmentação, restrição de acesso administrativo, regras de firewall, telemetria, casos de uso de detecção e acompanhamento de atualizações. Em uma dinâmica Purple Team, achados estáticos priorizados podem ser submetidos a testes ofensivos controlados; os resultados são então utilizados para verificar e aprimorar controles defensivos, realimentando o processo de avaliação [23, 24, 22].

Tabela 1: Comparação entre análise de firmware e abordagens operacionais de segurança

Abordagem	**Visibilidade principal**	**Limitação**	**Relação com o MARF-GC**
Scanner de rede e serviços	Portas, serviços, banners, protocolos e exposição observável	Não identifica todo o conteúdo interno do firmware e pode depender de identificação remota incompleta	Produz evidências de exposição e ajuda a priorizar validações
Scanner de vulnerabilidades	Correspondências entre serviços, versões aparentes e falhas conhecidas	Pode gerar falsos positivos ou negativos e não comprova impacto institucional	Complementa a correlação estática e informa a probabilidade de exposição
Análise estática de firmware	Bibliotecas, scripts, configurações, credenciais, certificados e componentes internos	Não demonstra, sozinha, comportamento em execução ou explorabilidade	Fornece a evidência interna e reproduzível organizada pelo modelo
Emulação, análise dinâmica e fuzzing	Comportamento em execução, interações e respostas a entradas	Dependem de compatibilidade, hardware, instrumentação e maior esforço técnico	Validam achados priorizados e reduzem incerteza técnica
Teste de intrusão / Red Team	Caminhos de ataque, exploração, impacto, persistência e evasão	Não necessariamente produz inventário completo dos componentes e dependências do firmware	Verifica exposição e impacto de achados selecionados
Blue Team / SOC	Prevenção, telemetria, detecção, resposta e melhoria de controles	Depende de contexto e evidências para definir controles específicos	Converte achados em segmentação, regras, alertas e monitoramento
Purple Team	Integração iterativa entre validação ofensiva e defesa	Exige coordenação, autorização e ambiente controlado	Realimenta classificação, tratamento e reauditoria

Fonte: Elaborado pelo autor (2026), com base em [21, 23, 24, 22].

Assim, o MARF-GC não substitui gestão de vulnerabilidades, scanners, testes de intrusão ou equipes ofensivas e defensivas. Sua função é organizar os resultados dessas práticas em uma trilha que preserve evidência, contexto, confiança, responsabilidade, decisão, prazo, risco residual e reavaliação.

2.11 GOVERNANÇA DE CIBERSEGURANÇA

Antes de prosseguir, é necessário distinguir dois conceitos frequentemente tratados como sinônimos nesta dissertação e na literatura correlata: gestão de riscos e governança de cibersegurança. A gestão de riscos corresponde ao processo operacional de identificar, avaliar, tratar e monitorar riscos específicos, por exemplo, decidir se uma vulnerabilidade em uma biblioteca de firmware deve ser corrigida, mitigada ou aceita. A governança, por sua vez, define a estrutura sob a qual essas decisões são tomadas: quem tem autoridade para decidir, sob qual política institucional, com que critérios de priorização orçamentária e com que mecanismo de prestação de contas. Nesta dissertação, a auditoria reproduzível de firmware é tratada como instrumento de gestão de riscos, por produzir evidências técnicas sobre ativos específicos. O MARF-GC conecta essas evidências às estruturas de governança, explicitando quem decide, sob qual política e mediante quais mecanismos de responsabilização. Essa distinção é retomada na Seção 4.7 e na etapa 5 do modelo.

A governança de cibersegurança pode ser compreendida como o conjunto de mecanismos organizacionais voltados à definição de responsabilidades, processos, prioridades e critérios de decisão relacionados à proteção de ativos digitais e à gestão de riscos em segurança da informação [25, 26]. Diferentemente de abordagens puramente técnicas, a governança estabelece diretrizes estratégicas que orientam a adoção de tecnologias, a definição de políticas e a priorização de investimentos em segurança.

Nesse contexto, a governança de cibersegurança assume papel central na articulação entre aspectos técnicos e organizacionais, especialmente em ambientes institucionais complexos, como universidades e centros de pesquisa. Essa articulação envolve, no nível de governança, a definição de políticas de segurança, a priorização orçamentária para atualização de infraestrutura e a atribuição de responsabilidades formais por ativos críticos; e, no nível de gestão, práticas como segmentação de rede, gestão contínua de vulnerabilidades e auditoria técnica recorrente [27, 28].

No entanto, observa-se que, na prática, muitas abordagens de governança ainda negligenciam camadas críticas da infraestrutura tecnológica, como o firmware de dispositivos de rede sem fio e outros sistemas embarcados. Essa limitação reduz a efetividade dos processos de gestão de riscos, uma vez que vulnerabilidades presentes em firmware podem comprometer elementos fundamentais da rede, muitas vezes fora do escopo das ferramentas tradicionais de monitoramento.

Dessa forma, a segurança de firmware deve ser compreendida não apenas como uma questão operacional, mas como um componente estratégico da governança de cibersegurança. A capacidade institucional de identificar, analisar e mitigar vulnerabilidades nesse nível influencia diretamente a qualidade das decisões relacionadas à infraestrutura tecnológica, à continuidade dos serviços e à proteção de ativos digitais.

Sob essa perspectiva, integrar práticas de auditoria de firmware aos processos de governança contribui para ampliar a visibilidade sobre riscos técnicos, fortalecer a rastreabilidade de decisões e reduzir a dependência de avaliações exclusivamente baseadas em fornecedores. Essa integração representa um avanço na maturidade da governança de cibersegurança, especialmente em contextos onde dispositivos de rede sem fio e outros sistemas embarcados desempenham papel crítico na operação institucional. Frameworks amplamente adotados, como o NIST Cybersecurity Framework, os CIS Critical Security Controls e modelos de governança como COBIT, estruturam práticas de identificação, proteção, detecção e resposta a inciden-

tes com base em risco. Esses referenciais reforçam a importância da integração entre aspectos técnicos e organizacionais, sendo fundamentais para a construção de estratégias de cibersegurança em ambientes institucionais complexos [23, 29, 30].

2.12 NORMAS, FRAMEWORKS E REFERENCIAIS APLICÁVEIS À GOVERNANÇA DE FIRMWARE

A análise de firmware em dispositivos de rede sem fio e sistemas embarcados não deve ser compreendida apenas como uma prática técnica de identificação de vulnerabilidades. Em ambientes institucionais, seus resultados precisam ser interpretados à luz de referenciais normativos, modelos de governança e estruturas de gestão de riscos capazes de transformar achados técnicos em critérios de decisão. Nesse sentido, normas e frameworks como NIST Cybersecurity Framework 2.0, NIST SP 800-53, NIST SP 800-193, CIS Critical Security Controls, COBIT, ISO/IEC 27001, ETSI EN 303 645, IEC 62443 e ISO/IEC 27402 oferecem bases conceituais relevantes para contextualizar a segurança de firmware como parte da governança de cibersegurança [23, 24, 31, 29, 30, 32, 33, 34, 35].

O NIST Cybersecurity Framework 2.0 organiza a gestão de riscos cibernéticos em funções voltadas a governar, identificar, proteger, detectar, responder e recuperar. No contexto desta dissertação, esse framework é especialmente útil porque permite posicionar a auditoria de firmware como mecanismo de apoio às funções de governança, identificação de ativos, proteção da infraestrutura e detecção de fragilidades técnicas. Assim, evidências como versões de firmware, bibliotecas vulneráveis, serviços expostos, ausência de atualização e componentes sem rastreabilidade podem ser interpretadas como insumos para a gestão institucional de riscos [23].

A NIST SP 800-53, por sua vez, apresenta um catálogo amplo de controles de segurança e privacidade aplicáveis a sistemas e organizações. Embora não trate exclusivamente de firmware de dispositivos de rede sem fio, seus controles relacionados a inventário de ativos, gerenciamento de configuração, controle de acesso, auditoria, monitoramento, avaliação de vulnerabilidades e resposta a incidentes dialogam diretamente com os objetivos do MARF-GC. A contribuição dessa norma para a presente pesquisa está em reforçar que a segurança de firmware precisa ser incorporada a processos formais de controle, documentação e gestão contínua [24].

A NIST SP 800-193 possui aderência ainda mais direta ao tema da dissertação, pois aborda diretrizes de resiliência de firmware de plataforma. Esse referencial destaca a importância de mecanismos de proteção, detecção e recuperação relacionados ao firmware, especialmente diante de ataques capazes de comprometer componentes fundamentais de inicialização e operação do sistema. Embora o escopo da norma esteja associado a firmware de plataforma, seus princípios contribuem para sustentar a discussão sobre integridade, recuperação, verificabilidade e continuidade operacional em dispositivos embarcados [31].

Os CIS Critical Security Controls contribuem com uma visão operacional de boas práticas de defesa cibernética. Controles relacionados ao inventário de ativos, inventário de software, gestão contínua de vulnerabilidades, configuração segura, proteção contra malware, controle de acesso e monitoramento são

relevantes para ambientes institucionais que dependem de roteadores, pontos de acesso, gateways e outros dispositivos conectados. No contexto desta dissertação, esses controles ajudam a demonstrar que a análise de firmware pode apoiar práticas já reconhecidas de gestão de vulnerabilidades e endurecimento da infraestrutura [29].

O COBIT, por sua natureza voltada à governança e à gestão corporativa de tecnologia da informação, contribui para posicionar o MARF-GC no nível decisório. Enquanto normas técnicas apoiam a identificação e o tratamento de vulnerabilidades, o COBIT permite relacionar os achados da auditoria de firmware a objetivos de governança, responsabilização, priorização, gestão de riscos, conformidade e entrega de valor. Dessa forma, a integração com COBIT reforça que o modelo proposto não se limita à execução técnica da análise, mas busca apoiar processos institucionais de decisão [30].

A ISO/IEC 27001 oferece uma base para sistemas de gestão de segurança da informação, orientando a definição de políticas, controles, responsabilidades e ciclos de melhoria contínua. No contexto da segurança de firmware, sua utilidade está em permitir que evidências técnicas sejam incorporadas a processos mais amplos de gestão de riscos, auditoria interna, tratamento de não conformidades e melhoria contínua. Já a ISO/IEC 27402, voltada a requisitos de segurança e privacidade para dispositivos IoT, aproxima-se diretamente da discussão desta dissertação ao tratar requisitos de linha de base para dispositivos conectados [32, 35].

A ETSI EN 303 645 também se destaca como referência relevante para segurança de dispositivos IoT, especialmente por estabelecer uma linha de base de requisitos de cibersegurança para dispositivos conectados. Embora seu foco seja frequentemente associado a IoT de consumo, seus princípios sobre atualização segura, ausência de senhas padrão universais, proteção de dados, comunicação segura e gerenciamento de vulnerabilidades podem ser reinterpretados em ambientes institucionais que utilizam dispositivos embarcados e equipamentos de rede [33].

A IEC 62443, originalmente orientada a sistemas de automação e controle industrial, contribui para a discussão ao tratar segurança ao longo do ciclo de vida, zonas, conduítes, segmentação, requisitos de proteção e responsabilidades organizacionais. Mesmo não sendo específica para roteadores Wi-Fi, sua lógica de segmentação, defesa em profundidade e gestão de riscos é útil para ambientes institucionais complexos que combinam redes, dispositivos embarcados e serviços críticos [34].

No campo da cadeia de suprimentos de software, o SBOM (*Software Bill of Materials*) assume papel central. Formatos como SPDX e CycloneDX permitem representar componentes, dependências, versões, licenças e metadados de software de forma estruturada. Em firmware de dispositivos de rede e sistemas embarcados, a ausência de SBOM ou de mecanismos equivalentes dificulta a identificação de bibliotecas vulneráveis, a correlação com CVEs e a rastreabilidade de componentes reutilizados. Por essa razão, SPDX e CycloneDX são relevantes para fortalecer a auditabilidade e a transparência técnica em processos de governança de firmware [36, 37].

No horizonte regulatório europeu, o AI Act (Regulamento (UE) 2024/1689) também merece menção, ainda que de forma pontual. Embora seu foco central seja a governança de sistemas de inteligência artificial, e não de firmware de dispositivos de rede, o regulamento sinaliza uma tendência mais ampla de responsabilização regulatória sobre tecnologias digitais críticas, aproximando-se do espírito do Cyber Resilience Act discutido na Seção 2.12.2. Essa convergência reforça a hipótese de que a exigência de audi-

tabilidade e rastreabilidade técnica, central ao MARF-GC, tende a se tornar um requisito regulatório cada vez mais comum para produtos digitais em geral, não apenas para dispositivos conectados [38].

2.12.1 Políticas Institucionais de Segurança da Informação e PPSI

No contexto brasileiro, a discussão sobre governança de cibersegurança em ambientes institucionais também deve considerar políticas, programas e referenciais voltados à segurança da informação no setor público. Entre esses referenciais, destaca-se o Programa de Privacidade e Segurança da Informação (PPSI), conduzido no âmbito da Secretaria de Governo Digital, como uma estrutura voltada à promoção de controles, guias, processos, modelos e procedimentos relacionados à privacidade e à segurança da informação [39, 40].

O PPSI organiza ações relacionadas a governança, maturidade, metodologia, pessoas e tecnologia, buscando elevar a capacidade dos órgãos e entidades em relação à proteção de dados, à segurança da informação e à resiliência institucional [39]. Além disso, o ciclo de implementação de 2026 do framework do PPSI foi regulamentado no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), reforçando a relevância do tema para a Administração Pública Federal [41].

Para esta dissertação, o PPSI é relevante por oferecer um referencial institucional brasileiro voltado à estruturação de controles, maturidade e governança em segurança da informação. No entanto, assim como outros frameworks de caráter mais amplo, o PPSI não tem como foco específico a auditoria reproduzível de firmware em dispositivos de rede sem fio e sistemas embarcados. Essa observação é importante porque evidencia uma lacuna operacional: políticas e frameworks institucionais orientam a proteção de ativos, a gestão de riscos e a maturidade em segurança, mas nem sempre detalham como produzir evidências técnicas sobre firmware, componentes embarcados, bibliotecas vulneráveis, versões, atualizações e rastreabilidade.

Nesse sentido, o MARF-GC pode ser compreendido como uma proposta complementar aos referenciais institucionais existentes. Seu papel não é substituir políticas de segurança da informação, programas institucionais ou frameworks consolidados, mas oferecer uma camada analítica específica para transformar achados técnicos de firmware em evidências úteis à governança. Assim, enquanto o PPSI contribui com diretrizes gerais de maturidade, controles, governança e segurança da informação, o MARF-GC atua no nível operacional-conceitual da auditoria de firmware de dispositivos de rede sem fio, conectando evidências técnicas à classificação de risco, à tomada de decisão e à melhoria contínua.

2.12.2 Referenciais Regulatórios Emergentes

Por fim, referenciais regulatórios emergentes, como o Cyber Resilience Act europeu, reforçam a tendência de exigir maior responsabilidade de fabricantes e fornecedores sobre requisitos de cibersegurança em produtos com elementos digitais. Embora esta dissertação não tenha como foco a análise jurídica desse regulamento, sua menção é pertinente como sinalização de que a segurança de firmware, a gestão de vulnerabilidades e a transparência sobre componentes tendem a ganhar maior relevância normativa nos próximos

anos [42].

2.12.3 Síntese dos Referenciais Aplicáveis à Governança de Firmware

Tabela 2: Relação entre referenciais normativos e a governança de firmware em dispositivos de rede sem fio

Referencial	Contribuição principal	Relação com a dissertação
NIST CSF 2.0	Estrutura de governança e gestão de riscos cibernéticos baseada nas funções Governar, Identificar, Proteger, Detectar, Responder e Recuperar.	Apoia o enquadramento da auditoria de firmware como mecanismo de identificação, proteção, detecção e governança de riscos em dispositivos de rede sem fio e sistemas embarcados.
NIST SP 800-53	Catálogo de controles de segurança e privacidade para sistemas e organizações.	Relaciona-se a inventário, configuração segura, auditoria, monitoramento, avaliação de vulnerabilidades e gestão de riscos.
NIST SP 800-193	Diretrizes para resiliência de firmware de plataforma.	Sustenta a discussão sobre integridade, proteção, detecção e recuperação de firmware comprometido.
CIS Controls	Conjunto de controles críticos para defesa cibernética operacional.	Contribui para inventário de ativos, gestão contínua de vulnerabilidades, configuração segura e monitoramento de dispositivos conectados.
COBIT	Framework de governança e gestão de tecnologia da informação.	Permite conectar evidências técnicas de firmware a processos decisórios, responsabilização, priorização e gestão institucional de riscos.
ISO/IEC 27001	Sistema de gestão de segurança da informação.	Apoia a incorporação da segurança de firmware a políticas, controles, auditoria, tratamento de riscos e melhoria contínua.
ETSI EN 303 645	Linha de base de segurança para dispositivos IoT.	Contribui com requisitos de atualização segura, autenticação, proteção de dados e gestão de vulnerabilidades em dispositivos conectados.
IEC 62443	Segurança para sistemas de automação e controle ao longo do ciclo de vida.	Reforça conceitos de segmentação, defesa em profundidade, zonas, conduítes e proteção de infraestruturas conectadas.
ISO/IEC 27402	Requisitos de linha de base para segurança e privacidade em dispositivos IoT.	Aproxima a análise de firmware de requisitos específicos para dispositivos conectados.
SBOM, SPDX e CycloneDX	Representação estruturada de componentes, dependências, versões e metadados de software.	Fortalecem a rastreabilidade de bibliotecas, a correlação com CVEs e a auditabilidade de componentes embarcados em firmware.
Cyber Resilience Act	Requisitos horizontais de cibersegurança para produtos com elementos digitais.	Indica tendência regulatória de maior responsabilidade sobre vulnerabilidades, atualizações e segurança de produtos digitais.

Fonte: Elaborado pelo autor (2026).

Em síntese, esses referenciais não substituem o modelo proposto nesta dissertação. Ao contrário, eles oferecem a base normativa e conceitual sobre a qual o MARF-GC pode ser posicionado. A contribuição do modelo está em operacionalizar, para o contexto específico de firmware de dispositivos de rede sem fio e sistemas embarcados, a passagem entre achados técnicos, evidências auditáveis, classificação de risco e decisão institucional.

2.13 ENGENHARIA DE SEGURANÇA E CICLO DE VIDA

A engenharia de segurança amplia a compreensão da segurança para além da correção reativa de falhas. Sob essa perspectiva, requisitos de proteção, confiabilidade, resiliência e rastreabilidade devem ser considerados ao longo de todo o ciclo de vida do sistema, desde a definição de requisitos até operação, manutenção e descarte [43].

Aplicada ao contexto de firmware de dispositivos de rede sem fio e sistemas embarcados, essa visão evidencia que muitos problemas decorrem da ausência de práticas sistemáticas de projeto, atualização e manutenção. Assim, discutir vulnerabilidades de firmware sob a ótica da engenharia e da governança torna possível propor diretrizes mais consistentes para ambientes institucionais.

2.13.1 Dependabilidade, Resiliência e Segurança em Sistemas Embarcados

A segurança de firmware em dispositivos de rede sem fio e sistemas embarcados também pode ser compreendida a partir dos conceitos de dependabilidade e resiliência operacional. Em sistemas embarcados, especialmente aqueles utilizados em infraestruturas institucionais, a confiabilidade do funcionamento não depende apenas da ausência de falhas de hardware, mas também da integridade, atualização e verificabilidade do software embarcado.

A dependabilidade envolve atributos como disponibilidade, confiabilidade, integridade, manutenibilidade e segurança. No contexto de dispositivos de rede sem fio, esses atributos tornam-se particularmente relevantes porque roteadores, gateways, pontos de acesso e controladores frequentemente operam de forma contínua, sustentando serviços acadêmicos, administrativos e laboratoriais. Assim, uma falha de firmware pode produzir efeitos que ultrapassam o dispositivo individual, afetando a continuidade de serviços e a estabilidade da infraestrutura de rede.

A resiliência, por sua vez, refere-se à capacidade de um sistema manter ou recuperar sua operação diante de falhas, ataques ou condições adversas. Em ambientes institucionais, essa capacidade depende não apenas de mecanismos de proteção tradicionais, como firewalls e segmentação de rede, mas também da qualidade dos componentes embarcados utilizados na infraestrutura. Um firmware vulnerável, desatualizado ou pouco auditável pode reduzir a capacidade de resposta da organização diante de incidentes.

Sob a perspectiva da engenharia de segurança, vulnerabilidades em firmware devem ser analisadas como fatores que afetam a dependabilidade do sistema como um todo. Credenciais embutidas, bibliotecas desatualizadas, serviços inseguros e falhas de atualização podem comprometer a disponibilidade, a integridade e a confiabilidade de dispositivos conectados. Dessa forma, a análise de firmware contribui para antecipar riscos que, em muitos casos, não seriam identificados por avaliações restritas à camada de rede ou aplicação.

Essa abordagem reforça a necessidade de integrar a segurança de firmware ao ciclo de vida dos sistemas embarcados. Desde a seleção e aquisição de equipamentos até sua implantação, operação, atualização e descarte, critérios de auditabilidade, suporte, rastreabilidade e segurança devem ser considerados. Em ambientes institucionais, essa integração permite alinhar decisões técnicas a objetivos mais amplos de continuidade operacional, proteção de ativos digitais e governança de cibersegurança.

2.14 FERRAMENTAS DE ANÁLISE DE FIRMWARE

A análise de firmware depende frequentemente do uso de ferramentas especializadas capazes de extrair, inspecionar e interpretar imagens de firmware. Entre as ferramentas mais utilizadas destacam-se utilitários

de extração de sistemas de arquivos, analisadores estáticos e frameworks de análise automatizada.

Ferramentas como *binwalk* permitem identificar e extrair componentes internos de imagens de firmware, incluindo sistemas de arquivos comprimidos, bibliotecas e executáveis. Após a extração, ferramentas de análise de binários e scripts podem ser empregadas para identificar configurações inseguras, credenciais embutidas ou bibliotecas potencialmente vulneráveis.

Além disso, frameworks de análise automatizada têm sido desenvolvidos para escalar a avaliação de segurança em grandes conjuntos de firmwares. Esses sistemas utilizam técnicas de análise estática, correlação com bases públicas de vulnerabilidades e identificação de padrões de código vulnerável. Estudos recentes demonstram que abordagens automatizadas são capazes de identificar vulnerabilidades recorrentes em diferentes dispositivos e fabricantes, evidenciando a presença de problemas estruturais na cadeia de desenvolvimento de firmware [7, 11].

2.15 CATEGORIAS DE VULNERABILIDADES EM FIRMWARE DE DISPOSITIVOS DE REDE SEM FIO

As vulnerabilidades encontradas em firmware de dispositivos de rede sem fio e sistemas embarcados podem ser classificadas em diferentes categorias técnicas. Entre as mais recorrentes estão credenciais embutidas no código, serviços de administração inseguros, bibliotecas desatualizadas e falhas de validação de entrada.

Credenciais embutidas representam uma das fragilidades mais documentadas em estudos sobre segurança de dispositivos embarcados. Nessas situações, usuários e senhas são incorporados diretamente no código ou em arquivos de configuração, permitindo acesso administrativo não autorizado caso esses dados sejam descobertos [4].

Outro problema frequente envolve o uso de bibliotecas desatualizadas ou vulneráveis. Muitas implementações utilizam versões antigas de bibliotecas criptográficas ou componentes de rede, expondo o dispositivo a vulnerabilidades já documentadas em bases públicas de segurança.

Tabela 3: Categorias recorrentes de vulnerabilidades em firmware de dispositivos de rede sem fio e sistemas embarcados

Categoria	Descrição
Credenciais embutidas	Usuários, senhas, chaves ou parâmetros sensíveis embutidos diretamente em binários, scripts ou arquivos de configuração.
Bibliotecas desatualizadas	Uso de componentes de software conhecidos por conter vulnerabilidades já documentadas em bases públicas.
Serviços inseguros expostos	Interfaces administrativas ou serviços de rede habilitados sem proteção adequada, como HTTP, Telnet ou FTP.
Falhas de atualização	Ausência de verificação de integridade, autenticação fraca ou mecanismo inseguro de atualização OTA.
Integração insegura de terceiros	Reutilização de bibliotecas e módulos externos sem controle adequado de dependências, versões e segurança.
Configurações inseguras	Parâmetros padrão fracos, permissões inadequadas e exposição indevida de recursos do sistema.

A Tabela 3 resume categorias recorrentes de fragilidades observadas na literatura sobre segurança de firmware. Essa sistematização contribui para organizar a análise teórica do problema e reforça que a segurança de dispositivos de rede e sistemas embarcados depende tanto da correção de falhas específicas quanto da adoção de práticas sistemáticas de engenharia e governança.

Também são observadas falhas relacionadas à exposição desnecessária de serviços de rede. Interfaces administrativas acessíveis via HTTP, Telnet ou SSH podem ampliar a superfície de ataque caso não sejam protegidas por mecanismos adequados de autenticação ou segmentação de rede.

Essas categorias de vulnerabilidades evidenciam que a segurança de firmware depende não apenas da correção de falhas específicas, mas também da adoção de práticas sistemáticas de engenharia de segurança ao longo do ciclo de vida do dispositivo.

2.16 ATAQUES REAIS EM DISPOSITIVOS DE REDE SEM FIO E ECOSSISTEMAS CONECTADOS

A crescente adoção de dispositivos de rede sem fio e outros equipamentos conectados em ambientes domésticos, industriais e institucionais tem ampliado significativamente a superfície de ataque das infraestruturas digitais. Diversos incidentes de segurança demonstraram que vulnerabilidades em firmware e configurações inseguras podem ser exploradas em larga escala para comprometer redes inteiras.

Um dos casos mais emblemáticos foi o malware Mirai, identificado em 2016. O Mirai explorava dispositivos IoT com credenciais padrão ou fracas, como roteadores, câmeras IP e gravadores digitais. Após

comprometer os dispositivos, o malware os incorporava a uma botnet capaz de realizar ataques distribuídos de negação de serviço (DDoS) em grande escala. Esse incidente demonstrou como dispositivos aparentemente simples podem ser instrumentalizados para gerar impactos significativos na infraestrutura da internet [19].

Outro exemplo relevante é o malware Reaper (também conhecido como IoTroop), identificado em 2017. Diferentemente do Mirai, que explorava principalmente credenciais padrão, o Reaper utilizava vulnerabilidades conhecidas em firmware para comprometer dispositivos IoT. Esse comportamento evidenciou a importância da gestão de vulnerabilidades e da atualização contínua de firmware em dispositivos conectados.

Além desses casos, campanhas como VPNFilter demonstraram que dispositivos de rede, especialmente roteadores domésticos e corporativos de pequeno porte, podem ser alvo de ataques sofisticados. O VPNFilter possuía múltiplos estágios de infecção e era capaz de interceptar tráfego, roubar credenciais e até inutilizar dispositivos comprometidos.

Esses incidentes reforçam que vulnerabilidades em firmware representam um vetor crítico de ataque em ambientes de dispositivos conectados, incluindo equipamentos de rede sem fio. A exploração dessas fragilidades frequentemente está associada a práticas inadequadas de desenvolvimento, ausência de mecanismos robustos de atualização e falta de monitoramento contínuo de vulnerabilidades. Assim, abordagens sistemáticas de auditoria de firmware e governança de segurança tornam-se fundamentais para reduzir riscos em infraestruturas baseadas em dispositivos conectados.

A Tabela 4 sintetiza exemplos representativos de botnets e campanhas de malware que afetaram dispositivos conectados e equipamentos de rede, destacando o ano de ocorrência, o principal vetor de ataque explorado e os impactos observados. Os casos apresentados ilustram como fragilidades em firmware, credenciais inseguras e ausência de mecanismos adequados de atualização podem contribuir para comprometimentos em larga escala, reforçando a relevância da auditabilidade e da gestão contínua de vulnerabilidades em dispositivos conectados.

Tabela 4: Exemplos de botnets e campanhas de malware que afetaram dispositivos conectados e equipamentos de rede

Malware	**Ano**	**Principal vetor de ataque**	**Impacto observado**
Mirai	2016	Credenciais padrão e serviços expostos em dispositivos IoT	Formação de grandes botnets utilizadas em ataques DDoS globais
Reaper (IoTroop)	2017	Exploração de vulnerabilidades em firmware de dispositivos	Botnet mais sofisticada com capacidade de expansão automatizada
VPNFilter	2018	Comprometimento de roteadores e dispositivos de rede	Interceptação de tráfego, roubo de credenciais e sabotagem de dispositivos

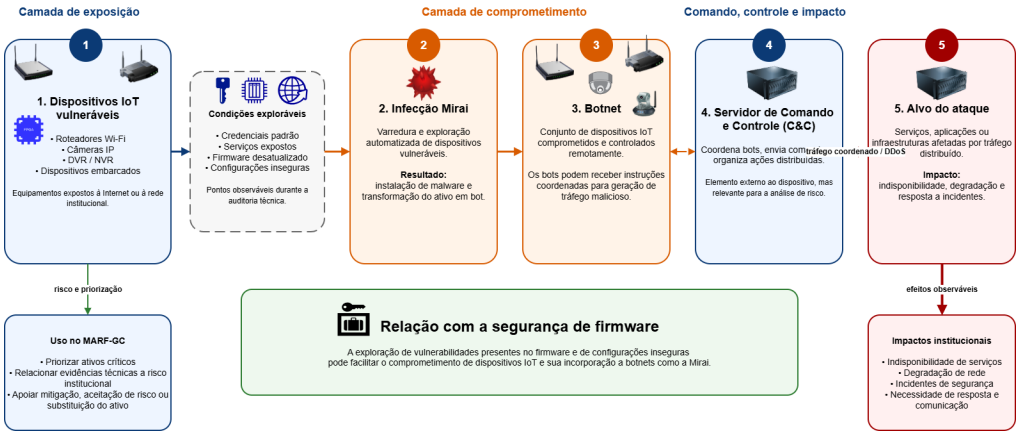

Figura 5: Modelo simplificado do funcionamento da botnet Mirai explorando dispositivos IoT comprometidos.

Fonte: Elaborado pelo autor (2026).

A Figura 5 ilustra esse funcionamento em cinco camadas, desde a exploração de dispositivos vulneráveis até o impacto final sobre os alvos de ataque, evidenciando como falhas de firmware discutidas ao longo deste capítulo podem ser encadeadas em uma cadeia de comprometimento em larga escala.

2.17 AUDITORIA E REPRODUTIBILIDADE NA ANÁLISE DE FIRMWARE

A análise de firmware também possui relevância sob a perspectiva de auditoria e reprodutibilidade científica. Em ambientes institucionais, a capacidade de reproduzir análises e verificar resultados é essencial para garantir transparência na avaliação de riscos tecnológicos.

A análise estática contribui para esse objetivo ao permitir a inspeção de imagens de firmware sem necessidade de execução direta em hardware físico. Isso possibilita que diferentes pesquisadores ou equipes técnicas reproduzam o mesmo processo de análise, utilizando ferramentas semelhantes e validando os resultados obtidos.

Ferramentas como Binwalk, analisadores de bibliotecas e scanners de vulnerabilidades permitem extrair e examinar o conteúdo interno do firmware, identificar dependências de software e correlacionar componentes com vulnerabilidades conhecidas em bases públicas de segurança.

Essa abordagem favorece a construção de evidências técnicas auditáveis, permitindo que organizações documentem seus processos de avaliação de risco e fundamentem decisões relacionadas à adoção ou substituição de tecnologias.

2.18 TRABALHOS RELACIONADOS

A literatura recente apresenta diversos estudos voltados à análise de segurança de firmware em dispositivos conectados, sistemas embarcados e equipamentos de rede, com foco em identificação de vulnerabi-

lidades, técnicas de auditoria, reutilização de componentes de terceiros e implicações para a segurança de sistemas embarcados.

Para a seleção dos trabalhos relacionados, foram considerados estudos publicados majoritariamente entre 2020 e 2024, priorizando surveys, revisões sistemáticas, estudos empíricos e propostas diretamente associadas à análise de firmware, segurança de dispositivos conectados e avaliação de vulnerabilidades em sistemas embarcados. Trabalhos clássicos anteriores a esse período foram mantidos quando apresentaram relevância metodológica ou histórica para a consolidação do campo. Foram também incluídos estudos voltados à governança de cibersegurança, à gestão de riscos e à governança de TI em ambientes de ensino superior, uma vez que a articulação entre análise técnica e processos institucionais constitui o eixo central desta dissertação.

A Tabela 5 apresenta uma síntese comparativa dos trabalhos selecionados, destacando foco, abordagem, limitações e relação com a proposta desta dissertação.

Tabela 5: Comparação de trabalhos relacionados em segurança de firmware e governança de cibersegurança

Autor	Foco	Abordagem	Limitação	Relação com esta dissertação
Costin et al. (2014)	Segurança de firmware em larga escala	Análise empírica de imagens de firmware	Não aborda governança institucional nem auditabilidade como eixo central	Referência metodológica para análise de firmware em larga escala
Feng et al. (2023)	Detecção de vulnerabilidades em firmware IoT	Survey técnico sobre técnicas de detecção	Foco predominantemente técnico, com pouca discussão institucional	Apoia a sistematização das técnicas de análise de firmware
Haq et al. (2023)	Segurança em firmware de dispositivos IoT	Revisão sobre arquitetura, extração e análise de vulnerabilidades	Pouca articulação com governança e gestão de riscos	Contribui para a fundamentação sobre arquitetura e análise de firmware
Zhao et al. (2023)	Componentes de terceiros em firmware IoT	Detecção de reutilização e violações em componentes de software	Foco específico na cadeia de suprimentos, sem discussão institucional ampliada	Reforça a importância da rastreabilidade de componentes em firmware
Bakhshi et al. (2024)	Vulnerabilidades e auditoria de firmware IoT	Revisão de vulnerabilidades e técnicas de auditoria	Não aprofunda a integração entre auditoria técnica e governança institucional	Fundamenta a discussão sobre auditabilidade e técnicas de avaliação
Chen et al. (2024)	Identificação automatizada de bibliotecas reutilizadas	Análise automatizada em larga escala	Foco na detecção técnica de bibliotecas, sem tratar implicações de governança	Apoia a discussão sobre riscos associados a bibliotecas desatualizadas e terceiros
Melaku (2023)	Governança de cibersegurança em organizações	Proposta de framework dinâmico e adaptativo de governança	Não aborda especificamente firmware IoT ou dispositivos embarcados	Fornece o referencial de governança utilizado para articular os achados técnicos desta dissertação
Savas e Karatas (2022)	Panorama de estudos em governança de cibersegurança	Revisão teórica sobre frameworks e modelos de governança	Não trata de IoT ou firmware; abordagem institucional genérica	Sustenta a discussão sobre governança como dimensão estratégica complementar à análise técnica
Bianchi e Sousa (2016); Khouja et al. (2018)	Governança de TI em instituições de ensino superior	Revisão sistemática sobre mecanismos de governança em IES	Foco em governança geral de TI, sem tratar segurança de firmware	Ancora o contexto institucional desta dissertação em ambientes de ensino superior
Esta dissertação	Firmware, auditabilidade e governança	Análise reproduzível, revisão crítica e discussão institucional	Não realiza validação dinâmica, exploração ou testes em hardware; incorpora reprodução estática direcionada para recomposição documental.	Integra análise técnica de firmware à governança de cibersegurança em ambientes institucionais

De forma geral, os trabalhos analisados podem ser agrupados em três categorias principais: (i) estudos de análise de vulnerabilidades em firmware; (ii) propostas de técnicas automatizadas de auditoria; e (iii)

abordagens voltadas à gestão de riscos e governança de segurança em ambientes de dispositivos conectados e institucionais. Os trabalhos analisados foram selecionados com base em sua relevância, número de citações e aderência ao tema de segurança de firmware em dispositivos conectados e governança de cibersegurança no período recente.

Observa-se que, apesar da diversidade de abordagens técnicas, a maioria dos trabalhos não considera explicitamente o contexto institucional no qual dispositivos conectados e equipamentos de rede estão inseridos. Da mesma forma, os estudos de governança de cibersegurança e governança de TI em IES tendem a tratar a segurança de forma genérica, sem aprofundar a camada de firmware como objeto de avaliação.

2.18.1 Lacuna Identificada

A literatura técnica oferece métodos para extração, análise estática, identificação de componentes, emulação, fuzzing e correlação com bases públicas. As práticas operacionais de segurança, por sua vez, incluem gestão de vulnerabilidades, scanners, testes de intrusão, Red Team, Blue Team e Purple Team. Esses mecanismos produzem evidências importantes, mas cada um observa apenas parte do problema: scanners privilegiam a superfície exposta; análise estática privilegia o conteúdo interno do artefato; testes ofensivos validam caminhos de exploração e impacto; e equipes defensivas transformam evidências em controles e detecções.

Os referenciais de governança e gestão de riscos, como NIST CSF, COBIT, ISO/IEC 27001 e PPSI, estabelecem funções, controles, responsabilidades e ciclos de melhoria, mas não detalham como preservar e interpretar evidências específicas da camada de firmware. Inversamente, os estudos técnicos de firmware normalmente encerram sua contribuição na detecção, correlação ou validação de falhas, sem definir responsável institucional, prazo, decisão, risco residual, aceitação formal ou reauditoria.

A lacuna desta dissertação situa-se, portanto, na ausência de uma estrutura específica que conecte: (i) evidências internas e reproduzíveis do firmware; (ii) validações técnicas complementares; (iii) contexto de exposição, criticidade e dependência operacional; (iv) controles defensivos; e (v) decisão institucional documentada. O MARF-GC não propõe uma nova técnica de detecção nem pretende substituir processos existentes. Sua contribuição está em organizar essa passagem entre camadas, com entregáveis, atores, critérios de confiança, classificação contextual do risco, tratamento, responsabilização e reavaliação.

2.19 SÍNTESE DO CAPÍTULO

A revisão apresentada neste capítulo evidenciou que a segurança de firmware constitui um elemento central na proteção de dispositivos de rede sem fio e outros sistemas embarcados e, consequentemente, na segurança de infraestruturas digitais mais amplas. A literatura demonstra que vulnerabilidades recorrentes, combinadas à baixa transparência de implementação e à complexidade arquitetural dos sistemas embarcados, tornam a análise de firmware uma atividade essencial para avaliação de risco e fortalecimento da postura de segurança institucional.

Além disso, verificou-se que métodos reproduzíveis de auditoria e análise estática desempenham papel

importante na produção de evidências técnicas que podem apoiar decisões organizacionais relacionadas à governança de cibersegurança. Entretanto, observou-se também que grande parte dos estudos concentra-se predominantemente na identificação técnica de vulnerabilidades, na extração de firmware ou na automação de mecanismos de análise, dedicando menor atenção à integração desses achados com práticas de governança, rastreabilidade e gestão institucional do risco cibernético.

Nesse contexto, é importante destacar que esta dissertação não pretende propor uma nova técnica de detecção de vulnerabilidades ou um novo mecanismo automatizado de auditoria de firmware. Sua contribuição está centrada na articulação entre análise reproduzível, auditabilidade, governança de cibersegurança e rastreabilidade técnica, buscando compreender como evidências oriundas da análise de firmware podem apoiar processos institucionais de avaliação de risco e tomada de decisão.

Assim, os elementos discutidos neste capítulo fornecem a base conceitual necessária para sustentar a proposta analítica desenvolvida nesta dissertação, posteriormente consolidada no MARF-GC (*Modelo Conceitual para Auditoria Reproduzível de Firmware para Governança de Cibersegurança*), concebido como instrumento de apoio à integração entre evidências técnicas, auditabilidade e governança institucional em ambientes dependentes de dispositivos de rede sem fio.

3 METODOLOGIA

3.1 CARACTERIZAÇÃO DA PESQUISA

Esta pesquisa caracteriza-se como aplicada, qualitativa, exploratória, descritiva e de natureza documental, com orientação analítico-interpretativa, apoiada em revisão orientada pelo problema, de caráter narrativo, e na reinterpretação analítica de resultados experimentais previamente publicados pelo autor em estudo anterior [1]. Sua natureza qualitativa decorre do fato de que o foco do estudo não está na mensuração estatística de variáveis ou na validação experimental de desempenho de ferramentas, mas na interpretação crítica de evidências técnicas e bibliográficas relacionadas à segurança de firmware em dispositivos de rede sem fio e sistemas embarcados [11, 10, 7]. A finalidade aplicada manifesta-se na intenção de produzir subsídios conceituais e práticos para a governança de cibersegurança em ambientes institucionais dependentes de dispositivos de rede sem fio e equipamentos embarcados [44, 25, 26]. A expressão revisão sistematizada não é adotada, pois não foram preservados registros suficientes para caracterizar uma revisão sistemática com protocolo completo, fluxo de seleção e avaliação formal de qualidade.

Do ponto de vista dos objetivos, trata-se de uma pesquisa exploratória e descritiva. É exploratória porque busca compreender, articular e reinterpretar um problema ainda pouco consolidado na interseção entre auditoria de firmware, gestão de riscos e governança institucional. É também descritiva porque sistematiza vulnerabilidades recorrentes, técnicas de auditoria, limitações de firmware proprietário e elementos de auditabilidade presentes na literatura e na base empírica utilizada [4, 5, 6, 1]. A pesquisa adota uma estratégia de consolidação crítica do conhecimento, reinterpretação institucional de evidências previamente produzidas e reprodução técnica direcionada para recomposição documental, sem validação dinâmica ou experimentação ofensiva.

3.2 ESTRATÉGIA METODOLÓGICA

A estratégia metodológica desta dissertação foi estruturada em quatro camadas complementares. A primeira consistiu em uma revisão analítica da literatura especializada e de referenciais normativos relacionados à segurança de firmware, dispositivos de rede sem fio, sistemas embarcados, análise estática, auditabilidade, engenharia de segurança, governança de cibersegurança e gestão de riscos [21, 43, 11, 7]. Essa etapa teve como objetivo consolidar conceitos, identificar vulnerabilidades recorrentes, mapear abordagens de auditoria e reunir elementos teóricos capazes de sustentar a discussão institucional proposta no trabalho.

A análise documental contemplou referenciais técnicos, normativos e de governança relacionados à segurança de firmware, dispositivos de rede sem fio, sistemas embarcados, gestão de vulnerabilidades, rastreabilidade de componentes, gestão de riscos e governança de cibersegurança. Foram considerados, de modo especial, o NIST Cybersecurity Framework 2.0, a NIST SP 800-53, a NIST SP 800-193, os CIS Critical Security Controls, o COBIT, a ISO/IEC 27001, a ETSI EN 303 645, a IEC 62443, a ISO/IEC 27402

e referenciais associados a SBOM, como SPDX e CycloneDX [23, 24, 31, 29, 30, 32, 33, 34, 35, 36, 37]. Esses documentos foram utilizados não como objeto jurídico de análise, mas como base conceitual para interpretar como evidências técnicas de firmware podem ser convertidas em critérios de governança, gestão de riscos e tomada de decisão institucional.

A segunda camada metodológica consistiu na retomada crítica de uma base empírica previamente produzida em estudo anterior sobre segurança de firmware em roteadores Wi-Fi [1]. Sem buscar repetir integralmente a campanha experimental original, esta dissertação incorpora os resultados desse estudo como corpus empírico de referência, reinterpretando seus achados à luz da literatura recente e dos referenciais de governança e engenharia de segurança [25, 26, 43]. Essa decisão metodológica permitiu preservar o vínculo com evidências técnicas concretas e, ao mesmo tempo, distinguir a campanha original da reprodução técnica complementar e direcionada descrita nesta dissertação.

A terceira camada correspondeu à síntese conceitual dos achados bibliográficos, documentais e empíricos, com o objetivo de construir uma interpretação institucionalmente orientada da segurança de firmware. Foi nessa etapa que se estruturou o MARF-GC, concebido como um modelo analítico para articular aquisição de firmware, auditoria reproduzível, produção de evidências, classificação de riscos e governança de cibersegurança. A partir dessa síntese, também foram formuladas diretrizes institucionais voltadas à gestão de firmware em equipamentos de rede sem fio.

A quarta camada consistiu em uma reprodução técnica complementar e direcionada das quatro imagens recuperadas. Seu propósito foi recompor a trilha documental, registrar hashes, versões de ferramentas, comandos, escopo efetivamente analisado, relatórios e critérios de triagem. Essa reprodução não foi utilizada para forçar a repetição das contagens 13, 7, 11 e 3 do estudo de base. Os resultados foram tratados como uma execução documentalmente independente, condicionada às versões atuais das ferramentas e das bases consultadas.

Em conjunto, essas quatro camadas permitiram que a pesquisa não se limitasse à descrição técnica de vulnerabilidades, mas avançasse na interpretação de como evidências produzidas por auditoria de firmware podem apoiar processos de avaliação de risco, definição de prioridades e tomada de decisão em organizações dependentes de infraestrutura conectada [44, 45, 46, 47].

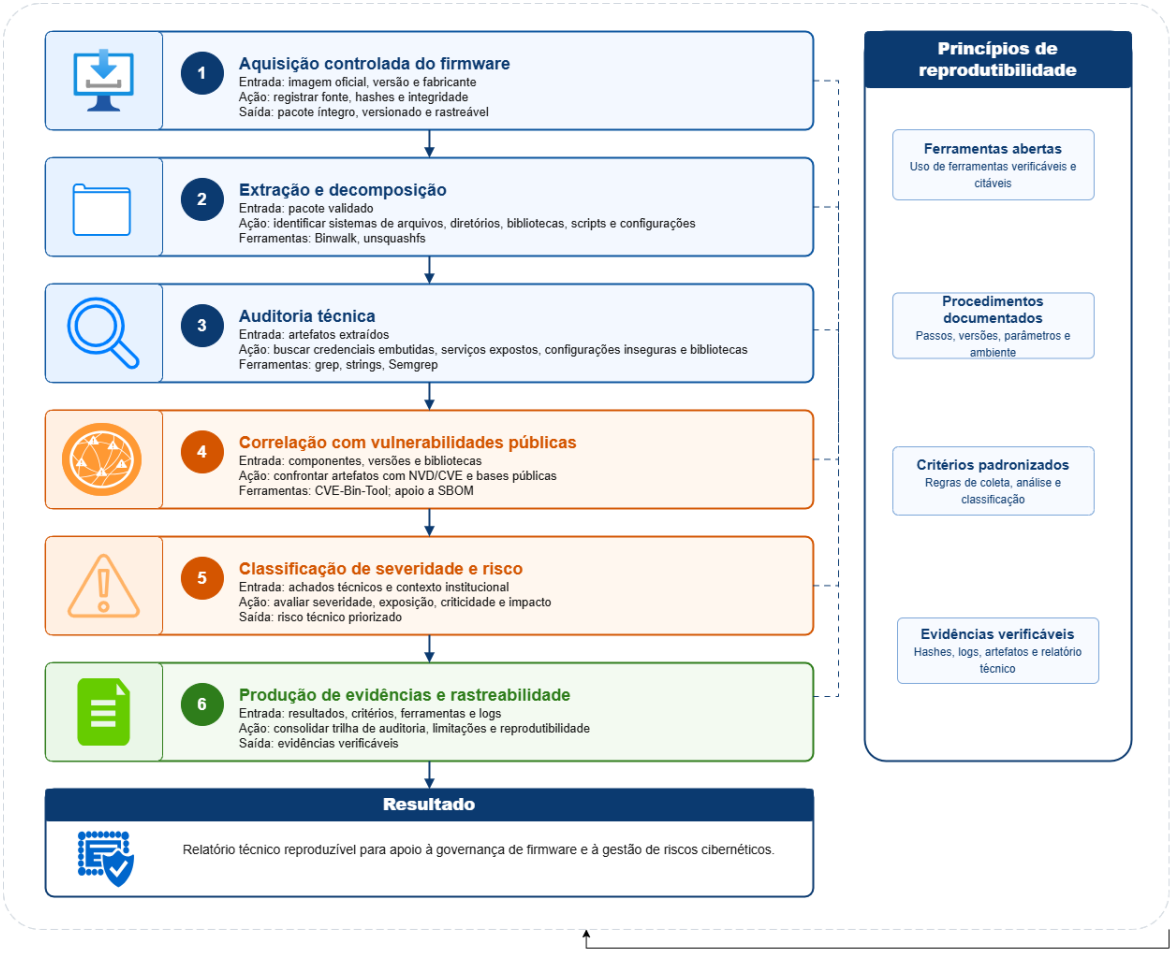

Figura 6: Pipeline metodológico utilizado na auditoria reproduzível de firmware realizada no estudo anterior [1].

Fonte: Elaborado pelo autor (2026).

A Figura 6 apresenta o pipeline metodológico adotado no estudo de base para a auditoria de firmware. O processo combina extração de sistemas de arquivos, inspeção estática de componentes e correlação com bases públicas de vulnerabilidades, permitindo identificar fragilidades presentes em dispositivos de rede sem fio e sistemas embarcados de forma reproduzível [4, 48, 21].

Tabela 6: Ferramentas relevantes para análise de firmware em dispositivos de rede sem fio e sistemas embarcados

Ferramenta	Tipo	Finalidade principal
Binwalk	Extração / engenharia reversa	Identificação e extração de sistemas de arquivos, assinaturas e componentes internos de imagens de firmware.
Firmware Mod Kit	Manipulação / extração	Extração e reconstrução de firmwares baseados em Linux embarcado.
cve-bin-tool	Vulnerabilidades	Identificação de bibliotecas conhecidas e correlação com vulnerabilidades públicas.
Semgrep	Análise estática	Identificação de padrões inseguros em código-fonte e scripts.
grep / strings	Inspeção textual	Busca de credenciais embutidas, parâmetros sensíveis e artefatos de configuração.
Firmadyne	Emulação	Execução de firmware em ambiente controlado para análise dinâmica e observação de comportamento.

A Tabela 6 sintetiza ferramentas comumente empregadas em processos de análise de firmware. Embora esta dissertação enfatize a análise estática e a produção de evidências auditáveis, a comparação entre ferramentas mostra que diferentes abordagens podem ser complementares, especialmente quando se deseja combinar inspeção estrutural, identificação de componentes vulneráveis e validação dinâmica.

No contexto desta dissertação, o termo evidências técnicas refere-se a artefatos observáveis, verificáveis e documentáveis obtidos ou derivados da análise de firmware, tais como versões de componentes, bibliotecas identificadas, arquivos de configuração, serviços expostos, credenciais embutidas, mecanismos de atualização, resultados de ferramentas de análise, hashes de integridade e registros de vulnerabilidades correlacionados a bases públicas. Essas evidências não são tratadas apenas como achados técnicos isolados, mas como insumos analíticos capazes de apoiar a avaliação de riscos, a rastreabilidade de decisões e a governança de cibersegurança em ambientes institucionais [1, 21, 25].

3.2.1 Escopo e Limitações do Semgrep e da Correlação com CVEs

O Semgrep 1.171.0 foi executado em modo genérico sobre um corpus textual construído a partir dos sistemas de arquivos extraídos. Foram copiados arquivos menores que 2 MB reconhecidos por tipo MIME como texto, scripts de shell, JavaScript, JSON, XML, YAML, Python, Perl, PHP e arquivos de configuração quando classificados nessas categorias. As cinco regras empregadas eram expressões genéricas para triagem de possíveis credenciais, marcadores de chave privada, referências a serviços inseguros, usuários administrativos padrão e associação de serviço HTTP a todas as interfaces. Não foram aplicadas regras semânticas específicas por linguagem. Seu escopo não abrangeu, de forma equivalente, todos os binários compilados presentes nos sistemas de arquivos. Portanto, a menção à análise estática não significa que todo o firmware tenha sido analisado semanticamente pelo Semgrep. Binários, bibliotecas e executáveis foram principalmente identificados por extração, assinaturas, metadados, inspeção textual, dependências e correlação de componentes; engenharia reversa profunda e análise de comportamento ficaram fora do escopo desta etapa.

Da mesma forma, o cve-bin-tool não gera novas CVEs nem comprova automaticamente que uma vulnerabilidade seja explorável. A ferramenta identifica componentes e versões e os correlaciona com registros públicos. Uma correspondência pode indicar um componente potencialmente vulnerável, mas deve ser avaliada quanto a uso efetivo, configuração, exposição, correções retroportadas, opções de compilação e condições de exploração. Nesta dissertação, os resultados são diferenciados pelas seguintes categorias:

1. **CVE correlacionada**: correspondência automatizada entre componente/versão e registro público;
2. **componente potencialmente vulnerável**: correlação considerada tecnicamente plausível após inspeção do artefato;
3. **achado validado por inspeção**: presença do componente, arquivo, configuração ou padrão confirmada no sistema extraído;
4. **vulnerabilidade com exposição identificada**: serviço ou condição de alcance observada por técnica dinâmica ou verificação do equipamento;

5. **vulnerabilidade com exploração confirmada**: exploração controlada e documentada em ambiente autorizado.

A base retomada nesta dissertação sustenta contagens agregadas de correlações e achados estáticos, mas não permite classificar todas as ocorrências nas duas últimas categorias. Por isso, o texto evita tratar toda correspondência como vulnerabilidade comprovadamente explorável.

3.2.2 Arquitetura do Ambiente de Análise

A base empírica utilizada nesta dissertação foi produzida em estudo anterior conduzido em ambiente controlado, o que permite compreender a dinâmica de análise de firmware em dispositivos de rede sem fio e sustentar a discussão institucional proposta neste trabalho.

O estudo de base documenta a execução dos experimentos em uma máquina virtual Kali Linux 2025.2, configurada com quatro vCPUs e 8 GB de memória RAM [1]. A figura do ambiente possui caráter conceitual e representa os componentes e fluxos necessários à análise; ela não deve ser interpretada como inventário exaustivo de todos os recursos efetivamente utilizados em cada execução.

No estudo anterior [1], os firmwares foram obtidos em repositórios oficiais e verificados por checksums MD5 e SHA-256. O fluxo combinou Binwalk, Semgrep, cve-bin-tool, inspeção textual e o script `collect_evidence.sh`, responsável por orquestrar extração, varredura e coleta de artefatos. A publicação de base documenta o método e as contagens agregadas, mas não reproduz em seu corpo os hashes, URLs, versões exatas das ferramentas, comandos, regras e relatórios individualizados. Essa distinção é relevante porque a reprodutibilidade plena exige tanto a descrição do fluxo quanto a preservação dos artefatos específicos de cada execução.

A Figura 7 ilustra a organização conceitual do ambiente utilizado, destacando a interação entre os componentes de análise e os dispositivos avaliados.

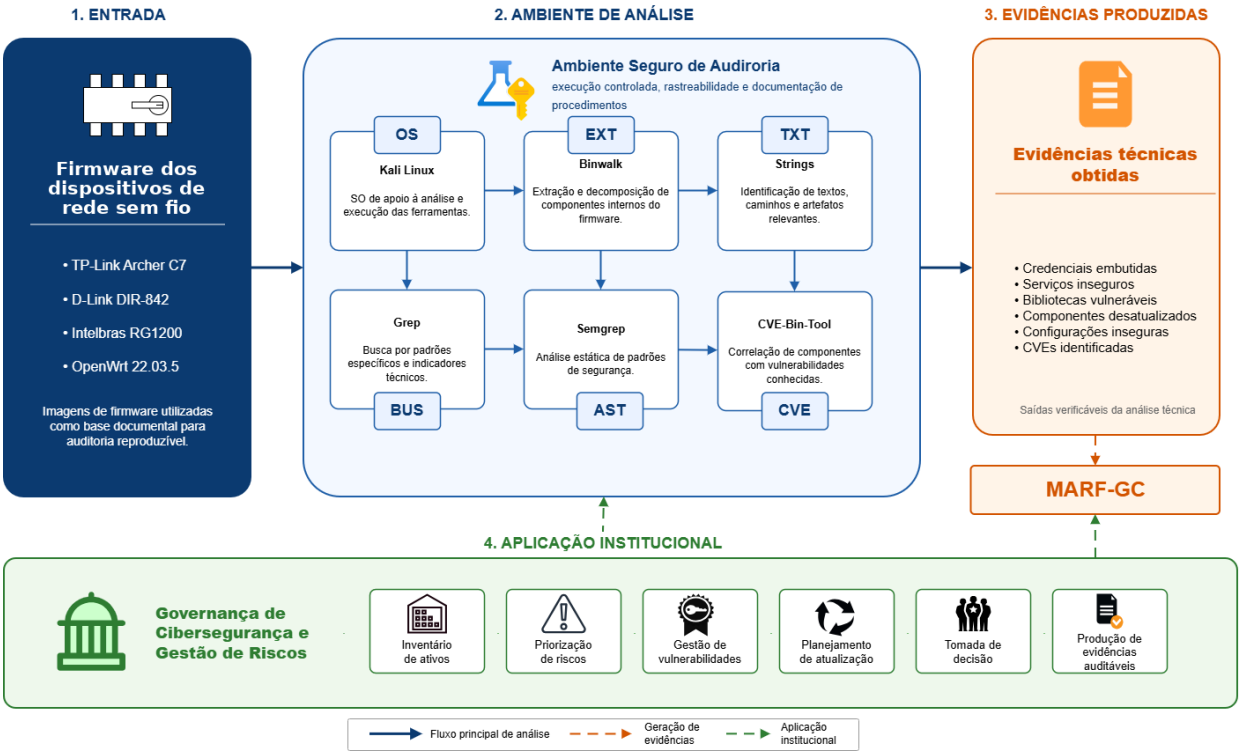

Figura 7: Arquitetura conceitual do ambiente de análise de firmware utilizado no estudo anterior [1], retomado nesta dissertação.

Fonte: Elaborado pelo autor (2026).

3.2.3 Reprodução Direcionada para Recomposição da Trilha Documental

Em 23 de julho de 2026, foi realizada uma reprodução técnica complementar e direcionada em máquina virtual isolada, com a finalidade de recompor a trilha documental e ampliar a rastreabilidade da análise. O procedimento teve natureza documental e estática. Não foram executados os firmwares, conduzidos testes de intrusão, exploradas vulnerabilidades ou realizadas medições de exposição em rede.

A máquina virtual utilizou Kali Linux 2025.2, quatro vCPUs, 8 GB de memória RAM e disco virtual de 500 GB. Foram registradas as versões Binwalk3 3.1.0, cve-bin-tool 3.4, Semgrep 1.171.0, Python 3.13.14, squashfs-tools 4.7.5 e u-boot-tools 2025.01. As imagens originais foram mantidas em compartilhamento somente leitura e copiadas para diretório de trabalho após conferência de integridade.

Tabela 7: Hashes SHA-256 confirmados na reprodução direcionada

Imagem	Versão	SHA-256
TP-Link Archer C7 v5	20220715	14bab8d9cfe2062205ec6a3975d83b8dc1f770688008b8024a8bf214bfc7fcaa
D-Link DIR-842 R1	3.0.3	afd9276c1c08109d12c90b97d07e126848c642d514f936d8388577286f6f07bc
Intelbras RG1200	2.1.8	62817ba78ee8f2a2f0349f6bed012a5141349853bab15436c5954394a69659b2
OpenWrt para Archer C7 v5	22.03.5	db4409c8ca0c60efe0dbcd066a069b45bd72e7d3b3ae42808a7de3e672f109ba

Fonte: Elaborado pelo autor (2026), a partir da reprodução direcionada.

Após a extração, foram criadas cópias de análise sem links simbólicos, preservando-se inventários separados dos links removidos. Essa medida evitou que ferramentas de busca textual seguissem referências para caminhos externos ao sistema de arquivos extraído. As quatro raízes seguras continham, respectivamente, 1.000 arquivos no D-Link, 646 no Intelbras, 1.046 no OpenWrt e 2.090 no TP-Link.

A base local do cve-bin-tool foi atualizada uma única vez e reutilizada em modo offline para as quatro varreduras. A fonte OSV foi desabilitada porque a tentativa inicial exigiu o utilitário externo `gsutil`, indisponível no ambiente. Essa decisão foi registrada como limitação metodológica. O Semgrep foi executado somente sobre arquivos textuais reconhecidos por tipo MIME, menores que 2 MB, utilizando cinco regras genéricas para triagem de possíveis credenciais, marcadores de chave privada, referências a serviços inseguros, usuários administrativos padrão e associação de serviço HTTP a todas as interfaces. Os resultados brutos foram submetidos a inspeção, exclusão de arquivos de tradução e interface, eliminação de falsos positivos em binários e consolidação por causa técnica.

A trilha foi preservada por snapshots sucessivos da máquina virtual, relatórios em CSV, JSON e texto, hashes de resultados, scripts e regras. O pacote final de evidências recebeu o SHA-256 `24d8013ce625a66bb8bf3544312138cf3b5c148920c0f5f9ff6977f352b3f8ce`. A existência desse pacote comprova a preservação documental da execução, mas não substitui a disponibilização pública dos artefatos nem demonstra explorabilidade dos achados.

3.2.4 Cenário Institucional de Referência

A análise desenvolvida nesta dissertação considera como referência um cenário institucional real, baseado na infraestrutura de rede de uma IES e representado de forma anonimizada e conceitual. O objetivo da utilização desse cenário não é expor detalhes operacionais sensíveis da infraestrutura, mas representar um ambiente institucional típico no qual dispositivos de rede, segmentos lógicos, serviços de apoio e equipamentos embarcados coexistem e sustentam atividades acadêmicas, administrativas e laboratoriais.

Nesse ambiente, a rede é composta por múltiplos segmentos interconectados, organizados a partir de uma camada de distribuição, switches de acesso, VLANs, serviços institucionais e dispositivos embarcados distribuídos. A infraestrutura contempla redes administrativas, segmentos destinados a periféricos e uma zona associada a dispositivos conectados e equipamentos embarcados, como roteadores, pontos de acesso, câmeras, DVR/NVR e equipamentos legados. Essa configuração evidencia que dispositivos baseados em

firmware não operam de forma isolada, mas integrados a uma arquitetura de rede mais ampla, na qual podem influenciar conectividade, autenticação, segmentação lógica, disponibilidade de serviços e exposição institucional.

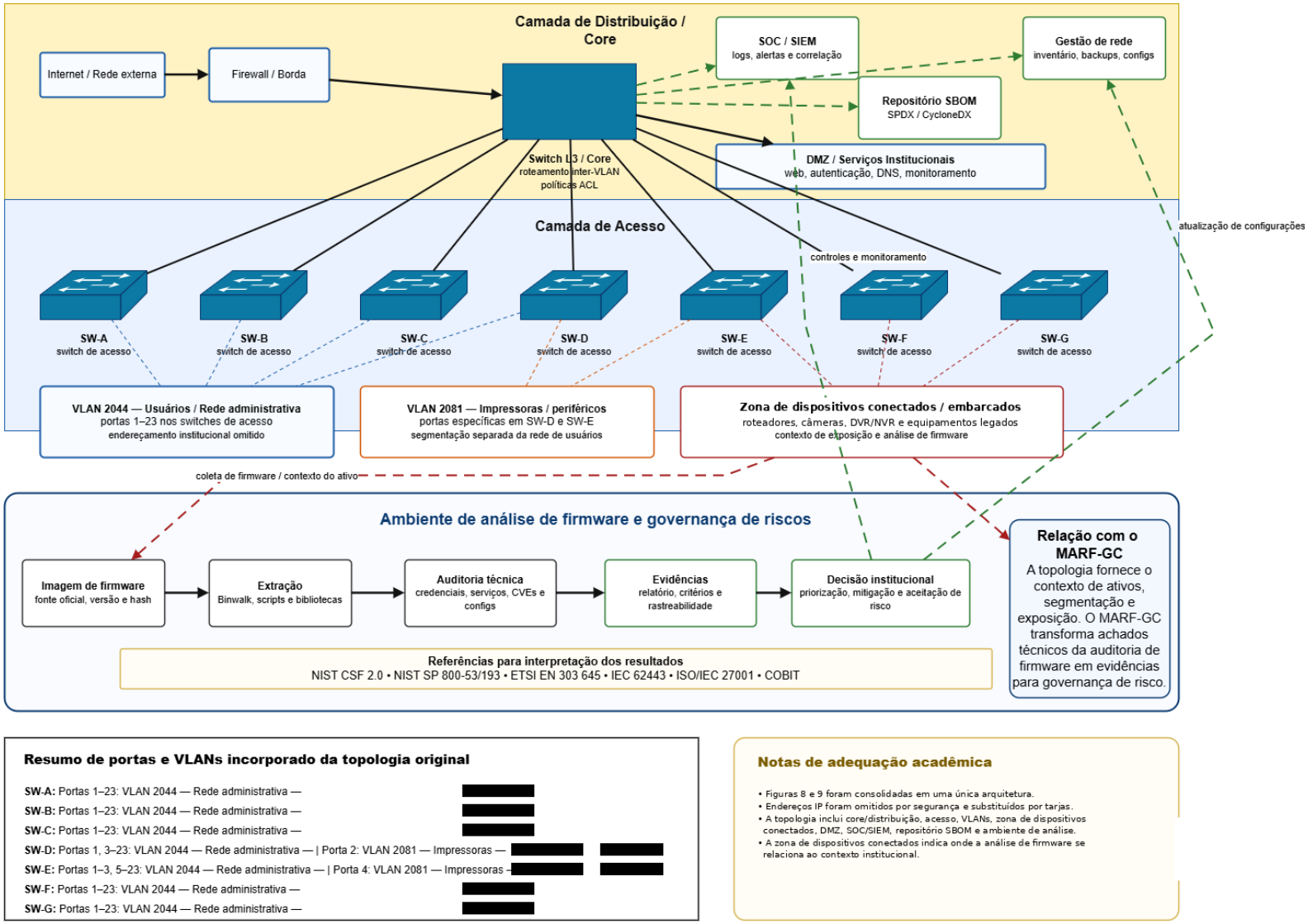

Figura 8: Topologia institucional unificada para análise de firmware de dispositivos de rede sem fio e governança de riscos.

Fonte: Elaborado pelo autor (2026), a partir de topologia institucional anonimizada.

A Figura 8 combina dois níveis de representação. A camada de rede, com segmentos, switches, VLANs, serviços e dispositivos embarcados, corresponde a um cenário institucional anonimizado de referência. Elementos como SOC/SIEM, repositório de SBOM, fluxo formal de aceitação de risco e integração contínua entre equipes são apresentados como componentes conceituais ou desejáveis da arquitetura proposta, e não como afirmação de que estejam integralmente implantados no ambiente estudado. Para fins de segurança e adequação acadêmica, endereços IP, nomes internos e informações sensíveis foram omitidos ou substituídos por marcações genéricas.

Tabela 8: Delimitação entre cenário institucional de referência e arquitetura proposta

Elemento	**Cenário de referência**	**Componente proposto pelo MARF-GC**
Segmentos de rede, switches, VLANs e dispositivos embarcados	Representação anonimizada de características típicas observadas em infraestrutura institucional	Utilizados como contexto para exposição, criticidade e dependências
Gestão de rede e equipes técnicas	Funções institucionais existentes em diferentes níveis de formalização	Recebem responsabilidades explícitas no fluxo de evidências e tratamento
SOC/SIEM e casos de uso de detecção	Não são afirmados como componentes plenamente implantados no cenário estudado	Representam capacidade defensiva desejável para integrar achados a monitoramento e resposta
Repositório de SBOM e evidências	Não é afirmado como repositório institucional já existente	Representa mecanismo proposto para preservar componentes, versões, hashes e relatórios
Comitê, aceitação formal de risco e reauditoria	Podem existir de forma genérica em políticas institucionais, sem confirmação de fluxo específico para firmware	São requisitos de governança do modelo para decisão, prazo, risco residual e acompanhamento

Fonte: Elaborado pelo autor (2026).

A presença de VLANs e de segmentos distintos demonstra a importância da separação lógica entre usuários, periféricos, serviços institucionais e dispositivos embarcados. Embora essa segmentação contribua para reduzir riscos de exposição direta e movimentação lateral, ela não elimina a necessidade de avaliar a segurança dos firmwares utilizados nos equipamentos que compõem a infraestrutura. Roteadores, pontos de acesso e demais dispositivos embarcados podem conter bibliotecas desatualizadas, serviços inseguros, credenciais embutidas ou mecanismos frágeis de atualização, tornando-se potenciais vetores de comprometimento em ambientes institucionais.

A relevância desse cenário para a presente dissertação reside no fato de que os firmwares analisados: TP-Link Archer C7, D-Link DIR-842, Intelbras RG1200 e OpenWrt 22.03.5, correspondem a soluções representativas de dispositivos de rede amplamente utilizados em ambientes acadêmicos, administrativos e institucionais. Essa correspondência entre os firmwares estudados e o cenário de referência confere relevância prática aos achados da dissertação, pois permite discutir como vulnerabilidades identificadas em firmware podem afetar redes reais compostas por múltiplos segmentos, switches de acesso, serviços distribuídos e equipamentos embarcados.

A parte inferior da Figura 8 explicita a conexão entre o cenário institucional e o ambiente de análise de firmware. Nesse fluxo, a imagem de firmware é obtida a partir de fonte oficial, submetida a procedimentos de extração, analisada tecnicamente e convertida em evidências que podem apoiar decisões institucionais.

Essa representação reforça a lógica central da dissertação: a auditoria de firmware não se limita à identificação de vulnerabilidades técnicas, mas produz evidências úteis para classificação de risco, priorização de mitigação, atualização de equipamentos, segmentação de rede e aceitação ou tratamento institucional do risco.

Do ponto de vista normativo, políticas institucionais de segurança da informação, programas governamentais e frameworks de privacidade e segurança, como o PPSI, estabelecem diretrizes gerais para proteção de ativos digitais, governança, maturidade, controles, gestão de riscos, segurança da informação e continuidade das ações institucionais [39, 40, 41]. Entretanto, tais referenciais tendem a operar em nível organizacional amplo, sem detalhar procedimentos específicos para inventário, auditoria, rastreabilidade, atualização e classificação de risco de firmware em dispositivos de rede sem fio e sistemas embarcados.

Essa lacuna é relevante para o cenário analisado nesta dissertação, uma vez que roteadores, pontos de acesso e demais equipamentos embarcados podem sustentar serviços críticos de conectividade, autenticação, segmentação lógica e monitoramento. Assim, vulnerabilidades presentes na camada de firmware podem permanecer pouco visíveis nos processos tradicionais de gestão de ativos e segurança da informação. Nesse contexto, o MARF-GC é proposto como uma estrutura analítica complementar, voltada a aproximar a auditoria reproduzível de firmware dos processos institucionais de governança, gestão de riscos e tomada de decisão.

3.3 BASE EMPÍRICA UTILIZADA

A base empírica deriva do estudo anterior do autor [1], que examinou quatro imagens de firmware: TP-Link Archer C7 (US) v5.0, D-Link DIR-842 R1, Intelbras RG1200 e OpenWrt 22.03.5. Para o recorte desta dissertação, esses equipamentos são tratados como dispositivos de rede sem fio com software embarcado, com ênfase em pontos de acesso e funções de roteamento, sem generalização para outras categorias de dispositivos conectados.

O procedimento publicado incluiu aquisição em fontes oficiais, verificação por MD5 e SHA-256, extração com Binwalk, inspeção de arquivos e padrões sensíveis, análise de código e scripts com Semgrep, correlação de componentes e versões com registros públicos por meio do cve-bin-tool e classificação agregada conforme CVSS v3.1. O script `collect_evidence.sh` foi desenvolvido para automatizar etapas de extração, varredura e coleta de artefatos [1].

É necessário distinguir os resultados do estudo de base daqueles obtidos na reprodução direcionada. As contagens 13, 7, 11 e 3 pertencem à publicação anterior e são preservadas como resultados históricos agregados. A reprodução de 2026 utilizou as mesmas quatro imagens confirmadas por hash, porém versões atuais das ferramentas e da base de vulnerabilidades; por isso, produziu uma matriz diferente, com 31 candidatos a CVE associados ao curl/libcurl 7.79.1 no TP-Link e 11 achados estáticos consolidados. As duas execuções não são somadas nem utilizadas para alegar repetibilidade numérica.

A Tabela 9 apresenta o estado atualizado da documentação após a reprodução direcionada.

Tabela 9: Estado atualizado da trilha de reprodutibilidade

Elemento	Situação após a reprodução	Observação
Modelos, versões e quatro imagens	Documentado	Identificados na publicação e conferidos por SHA-256 na reprodução
Ambiente de execução	Documentado	Kali Linux 2025.2, quatro vCPUs, 8 GB de RAM e disco virtual de 500 GB
Ferramentas e versões	Documentado	Binwalk3 3.1.0, cve-bin-tool 3.4, Semgrep 1.171.0 e ferramentas auxiliares
Comandos, parâmetros e scripts	Preservado	Scripts específicos para raízes seguras, varredura offline e consolidação
Escopo do Semgrep	Documentado	Arquivos textuais por MIME, menores que 2 MB; contagens por firmware registradas
Base de vulnerabilidades	Documentado com limitação	Atualização em 23/07/2026; execução offline; fonte OSV desabilitada
Relação de achados	Incorporada	Os 11 achados estáticos e os 31 candidatos a CVE estão individualizados no Apêndice A; relatórios integrais permanecem no pacote técnico
Evidências e integridade	Preservado	Relatórios, hashes, snapshots e manifesto com 3.275 arquivos
Origem, data original e situação de suporte	Limitação registrada	A publicação de base registra repositórios oficiais; URLs, data exata de obtenção e situação de suporte naquele momento não foram integralmente recuperadas e não são inferidas nesta dissertação

Fonte: Elaborado pelo autor (2026).

3.4 PROCEDIMENTOS DE REVISÃO

A revisão adotada possui caráter narrativo e orientado pelo problema. Seu objetivo foi consolidar conceitos e referenciais necessários à articulação entre segurança de firmware, auditabilidade, análise reproduzível, práticas operacionais de segurança e governança de cibersegurança. Foram utilizadas combinações de termos relacionados a firmware de dispositivos de rede sem fio, sistemas embarcados, análise estática, vulnerabilidades, componentes de terceiros, SBOM, reprodutibilidade, governança, gestão de riscos, testes de segurança e equipes Red, Blue e Purple Team.

Foram priorizados surveys, estudos empíricos, trabalhos de referência em análise de firmware, documentos normativos e publicações diretamente aderentes ao problema de pesquisa. Trabalhos clássicos foram mantidos quando apresentaram relevância metodológica ou histórica. A seleção foi orientada por aderência temática, atualidade, relevância para a construção do MARF-GC e capacidade de sustentar pelo menos um dos seguintes eixos: identificação de componentes e fragilidades; auditabilidade e reprodução; validação técnica complementar; classificação contextual do risco; ou governança institucional.

Como não foram preservados registros completos de bases consultadas, datas de busca, strings finais, quantitativos de inclusão e exclusão e avaliação formal da qualidade, a revisão não é apresentada como sistemática. Essa delimitação evita atribuir ao procedimento um nível de formalização que não foi documentado.

3.5 CRITÉRIOS DE ANÁLISE

A análise do material bibliográfico e documental foi orientada pelas seguintes perguntas:

1. Quais vulnerabilidades e fragilidades são mais recorrentes em firmware de dispositivos de rede sem fio e sistemas embarcados segundo a literatura recente?
2. Como métodos reproduzíveis de análise e auditoria de firmware podem contribuir para avaliação de segurança?
3. Quais implicações esses achados trazem para a governança de cibersegurança em ambientes institucionais?

Essas perguntas orientaram a organização do capítulo de fundamentação, a retomada do estudo empírico e a discussão final da dissertação.

3.6 LIMITAÇÕES DA PESQUISA

A pesquisa não realizou análise dinâmica, emulação funcional, fuzzing, exploração controlada ou validação em hardware real. A base empírica concentra-se em quatro imagens de pontos de acesso sem fio e roteadores e não permite generalização estatística para outros fabricantes, versões ou categorias de dispositivos conectados. A reprodução direcionada recompôs a trilha documental e confirmou arquivos, componentes e padrões, mas não demonstrou inicialização automática, exposição em rede ou explorabilidade.

A correlação com CVEs depende das fontes e da data de atualização da base. A fonte OSV foi desabilitada por dependência externa não planejada, e os resultados podem divergir de execuções futuras. As regras genéricas do Semgrep geraram muitos falsos positivos, especialmente em páginas web, traduções e binários contendo apenas marcadores textuais; por isso, as contagens brutas não foram interpretadas como vulnerabilidades. A matriz consolidada preserva 42 registros documentais. Os 11 achados estáticos e os 31 candidatos a CVE estão individualizados no Apêndice A, enquanto descrições extensas, vetores, saídas brutas e hashes permanecem no pacote técnico.

A validação prospectiva do MARF-GC permanece necessária. A aplicação apresentada é retrospectiva e ilustrativa, não uma comprovação experimental de efetividade.

3.7 AMEAÇAS À VALIDADE

Como esta pesquisa possui natureza qualitativa, documental e analítico-interpretativa, algumas ameaças à validade devem ser consideradas na interpretação dos resultados. A explicitação dessas limitações contribui para delimitar o alcance das conclusões e reforçar a coerência metodológica da dissertação.

Quanto à validade interna, a principal ameaça decorre do fato de a base empírica retomada derivar de um conjunto específico de firmwares de roteadores Wi-Fi, analisados previamente em estudo anterior do autor. Assim, os achados discutidos refletem evidências produzidas em um contexto delimitado, influenciadas pelas características dos dispositivos investigados, das versões analisadas e das ferramentas utilizadas.

Para mitigar essa limitação, os resultados foram reinterpretados em diálogo com literatura especializada, referenciais normativos e discussão institucional de governança de cibersegurança.

Quanto à validade externa, os resultados não devem ser generalizados estatisticamente para toda a diversidade de dispositivos conectados ou equipamentos de rede. A análise concentra-se em quatro firmwares de dispositivos de rede sem fio utilizados como referência para ambientes institucionais, especialmente em contextos acadêmicos e organizacionais. Dessa forma, as conclusões devem ser compreendidas como evidências analíticas contextualizadas, potencialmente úteis para ambientes com características semelhantes, mas não como afirmações universais sobre todos os sistemas embarcados ou dispositivos conectados.

Quanto à validade de construção, reconhece-se que conceitos como auditabilidade, governança de firmware, reprodutibilidade e risco institucional possuem natureza multidimensional. Para reduzir ambiguidades conceituais, esta dissertação definiu evidências técnicas como artefatos observáveis, verificáveis e documentáveis produzidos ou derivados da análise de firmware, tais como versões de componentes, bibliotecas identificadas, arquivos de configuração, serviços expostos, credenciais embutidas, hashes, resultados de ferramentas e CVEs correlacionadas. Além disso, o MARF-GC foi estruturado com base em entradas, saídas, atores, etapas, indicadores e integração com referenciais como NIST CSF, COBIT e PPSI.

Quanto à validade de conclusão, a principal limitação está relacionada ao caráter interpretativo dos achados. Embora tenha sido realizada reprodução estática direcionada para recomposição documental, não foram conduzidos testes dinâmicos, fuzzing, emulação avançada, exploração controlada ou validação em hardware real; portanto, as conclusões não devem ser lidas como comprovação experimental de efetividade do MARF-GC. Em vez disso, devem ser compreendidas como uma síntese conceitual sustentada por literatura, referenciais normativos e evidências empíricas previamente publicadas. Essa delimitação é coerente com o objetivo da dissertação, centrado na articulação entre auditoria reproduzível, produção de evidências e governança institucional.

Por fim, buscou-se reduzir vieses metodológicos por meio da triangulação entre literatura especializada, referenciais normativos, resultados empíricos previamente publicados, reprodução direcionada e documentação técnica associada aos firmwares analisados. Essa estratégia contribui para fortalecer a consistência interpretativa da pesquisa e delimitar adequadamente o alcance das contribuições apresentadas.

4 RESULTADOS E DISCUSSÃO

4.1 SEGURANÇA DE FIRMWARE COMO PROBLEMA INSTITUCIONAL

A análise da literatura e os resultados empíricos discutidos nesta dissertação evidenciam que a segurança de firmware se configura como uma camada crítica e sistematicamente subavaliada na proteção de dispositivos de rede sem fio e sistemas embarcados. Em ambientes institucionais, essa constatação assume caráter estratégico, uma vez que roteadores, gateways e outros dispositivos embarcados desempenham funções estruturais na conectividade e no funcionamento cotidiano das infraestruturas digitais.

O firmware, nesses dispositivos, é tipicamente organizado em múltiplas camadas, incluindo bootloader, kernel do sistema operacional, bibliotecas de suporte e aplicações responsáveis pela lógica operacional. Essa arquitetura modular, embora favoreça a flexibilidade e a reutilização de componentes, amplia significativamente a superfície de ataque. Vulnerabilidades em qualquer uma dessas camadas podem comprometer não apenas o dispositivo isolado, mas também o comportamento sistêmico da rede.

Tabela 10: Padrões recorrentes de vulnerabilidades em firmware

Categoria	**Descrição**	**Impacto institucional**
Credenciais embutidas	Usuários, senhas ou chaves fixas em arquivos, scripts ou binários	Acesso não autorizado e comprometimento administrativo
Bibliotecas desatualizadas	Componentes com vulnerabilidades conhecidas em bases públicas	Exploração remota e aumento da superfície de ataque
Serviços inseguros	Protocolos ou interfaces expostos sem proteção adequada	Interceptação, abuso de serviços e movimentação lateral
Componentes de terceiros	Reutilização de módulos externos sem rastreabilidade adequada	Risco de cadeia de suprimentos e baixa visibilidade técnica
Configurações inseguras	Permissões frágeis, parâmetros padrão e ausência de endurecimento	Escalada de privilégios e exposição indevida de recursos

A Tabela 10 sintetiza padrões recorrentes de vulnerabilidades discutidos ao longo da literatura e retomados nesta dissertação. Essa sistematização reforça que as falhas em firmware não se limitam a erros pontuais de implementação, mas podem produzir impactos institucionais relevantes quando associadas a dispositivos críticos de rede.

Dessa forma, a segurança de firmware não pode ser tratada como uma questão técnica restrita ao nível do dispositivo. Ela deve ser compreendida como um problema institucional, com implicações diretas para a disponibilidade de serviços, a segmentação lógica da rede, o controle de acesso e a integridade dos fluxos de comunicação. Essa perspectiva está alinhada com estudos recentes que tratam a segurança de dispositivos conectados como um problema sistêmico, no qual vulnerabilidades em componentes específicos podem impactar diretamente a gestão de riscos organizacional e a continuidade de serviços críticos [44].

Além disso, a dificuldade de inspeção e validação de firmware em muitos dispositivos de rede sem fio, especialmente em soluções proprietárias, introduz limitações relevantes na capacidade de avaliação de risco por parte das organizações. Esse cenário cria dependência de fornecedores e reduz a autonomia institucional na tomada de decisões relacionadas à segurança da infraestrutura.

Nesse contexto, reconhecer a segurança de firmware como um problema institucional representa um passo fundamental para a evolução da governança de cibersegurança. Essa mudança de perspectiva permite incorporar a análise de firmware aos processos de gestão de riscos, auditoria e definição de políticas tecnológicas, ampliando a capacidade das organizações de identificar vulnerabilidades críticas e responder de forma mais eficaz a ameaças emergentes.

4.2 RESULTADOS DA ANÁLISE ESTÁTICA DOS FIRMWARES

A análise dos resultados é organizada em dois conjuntos que não devem ser confundidos: as contagens agregadas publicadas no estudo de base e os registros obtidos na reprodução direcionada de 2026. A separação é necessária porque as versões das ferramentas, a base de vulnerabilidades e os critérios de triagem não são idênticos.

4.2.1 Resultados Agregados do Estudo de Base

Foram considerados três firmwares proprietários e uma solução de código aberto, conforme a Tabela 11.

Tabela 11: Firmwares considerados na análise empírica

Firmware	**Fabricante / Projeto**	**Modelo / Versão**	**Tipo**
TP-Link Archer C7	TP-Link	Archer C7 (US) v5.0	Proprietário
D-Link DIR-842	D-Link	DIR-842 R1	Proprietário
Intelbras RG1200	Intelbras	RG1200	Proprietário
OpenWrt	OpenWrt Project	22.03.5	Código aberto

O estudo de base utilizou Binwalk, Semgrep, cve-bin-tool e inspeção textual. O cve-bin-tool identificou componentes e versões e os associou a registros existentes de CVE; portanto, não se afirma que a ferramenta tenha gerado CVEs nem que cada correspondência represente exploração comprovada. Os resultados históricos são apresentados na Tabela 12.

Tabela 12: Ocorrências correlacionadas a registros de CVE no estudo de base

Firmware	Quantidade	Interpretação permitida pelo corpus
TP-Link Archer C7	13	Contagem agregada da execução original; requer validação por ocorrência
D-Link DIR-842	7	Contagem agregada da execução original
Intelbras RG1200	11	Contagem agregada da execução original
OpenWrt 22.03.5	3	Menor quantidade relativa naquela execução específica

4.2.2 Resultados da Reprodução Direcionada

A reprodução confirmou as quatro imagens por SHA-256 e concluiu a extração de quatro raízes seguras sem links simbólicos. O cve-bin-tool 3.4, utilizando a mesma base local em modo offline, não manteve correlações para D-Link, Intelbras e OpenWrt nessa execução. Para o TP-Link, identificou o componente curl/libcurl 7.79.1 e o correlacionou a 31 registros públicos: duas ocorrências classificadas como críticas pelas fontes do relatório, oito altas, 17 médias e quatro baixas. A presença e a versão foram confirmadas em `/usr/bin/curl` e `/usr/lib/libcurl.so.4.7.0`. As 31 linhas são candidatos a CVE associados a um único componente, não 31 explorações confirmadas.

A inspeção das dependências mostrou que o libcurl estava ligado a OpenSSL, e não a NSS. Não foram encontradas dependências dinâmicas de nghttp2, libidn, NSS ou LDAP no libcurl. Os scripts observados utilizavam curl principalmente em rotinas de DDNS por HTTP, sem evidência textual de SOCKS5 com resolução remota, HSTS, HTTP/2, OAuth2 ou proxy. Essa triagem permitiu marcar algumas condições como não identificadas ou não aplicáveis ao build observado, preservando as demais como condicionais.

O Semgrep 1.171.0 processou 749 arquivos textuais no D-Link, 337 no Intelbras, 841 no OpenWrt e 1.238 no TP-Link. As cinco regras genéricas produziram 1.516 ocorrências brutas. Após exclusão de traduções e páginas de interface, validação dos arquivos reais, eliminação de marcadores presentes apenas em binários e consolidação por causa técnica, permaneceram 11 achados estáticos, conforme a Tabela 13.

Tabela 13: Síntese dos registros mantidos após a reprodução direcionada

Firmware	Registros	Composição
D-Link DIR-842 R1	3	Duas chaves privadas RSA de 1.024 bits associadas ao servidor `anweb`; uma chave TR-069 com certificado expirado em 2015
Intelbras RG1200	4	Uma chave privada RSA de 2.048 bits associada ao `httpd`; três campos de credencial padrão com valores literais não vazios
OpenWrt 22.03.5	0	Nenhuma ocorrência bruta foi mantida como achado consolidado nesta triagem; isso não comprova ausência de vulnerabilidades
TP-Link Archer C7	35	31 candidatos a CVE do curl/libcurl 7.79.1 e quatro achados consolidados de possível exposição de credenciais em logs ou console

Fonte: Elaborado pelo autor (2026), a partir da reprodução direcionada.

As quatro chaves privadas reais eram legíveis sem senha, possuíam certificados correspondentes e eram referenciadas por executáveis do firmware. No D-Link, os pares `server.key/server.pem` e `intercept_server.key/intercept_server.pem` eram referenciados por `anweb`; o par

`tr069_key.pem/tr069_cert.pem` era referenciado pelo executável `tr069`. No Intelbras, `privkeySrv.pem/certSrv.crt` era referenciado por `httpd`. A integração ao executável foi confirmada, mas inicialização automática e exposição de rede não foram demonstradas.

Os três campos de credencial padrão do Intelbras estavam em `webroot_ro/default.cfg` e foram registrados sem divulgação dos valores. No TP-Link, foram identificadas rotinas ativas que encaminhavam variáveis de senha para syslog, console ou arquivo de log em `ncm.sh`, `pppshare.sh`, `getisp.sh` e `checkpsw.sh`. Esses registros foram consolidados por arquivo e causa técnica, em vez de contabilizados por repetição textual.

A matriz documental final reuniu 42 registros: 31 candidatos a CVE e 11 achados estáticos consolidados. O Apêndice A individualiza os 42 registros, apresenta a triagem dos candidatos prioritários e inclui uma ficha MARF-GC preenchida; os relatórios integrais permanecem preservados no pacote de evidências.

Tabela 14: Categorias de validação aplicáveis aos achados de firmware

Categoria	Critério	Cobertura na reprodução
CVE correlacionada	Correspondência automatizada entre componente/versão e registro público	31 registros do curl/libcurl
Componente potencialmente vulnerável	Presença e versão confirmadas, com aplicabilidade ainda condicionada	Confirmado para curl/-libcurl 7.79.1
Achado validado por inspeção	Arquivo, configuração ou padrão confirmado no sistema extraído	11 achados consolidados
Exposição identificada	Serviço ou condição de alcance verificada no equipamento em execução	Não demonstrada
Exploração confirmada	Exploração controlada, autorizada e documentada	Fora do escopo

4.2.3 Interpretação Comparativa dos Achados

As contagens do estudo original e da reprodução não são diretamente comparáveis. A execução de 2026 evidencia como mudanças de ferramenta, base e regras podem alterar o número de correlações. Assim, a quantidade de ocorrências não constitui medida absoluta de segurança.

No conjunto original, os firmwares proprietários apresentaram maior quantidade agregada de correlações, enquanto o OpenWrt 22.03.5 apresentou menor quantidade relativa e melhores condições de transparência, inspeção e rastreabilidade. Na reprodução direcionada, nenhum achado do OpenWrt foi mantido após a triagem específica, mas isso não autoriza inferir segurança universal. A idade da versão, situação de suporte, quantidade de componentes, exposição de serviços, criticidade, controles compensatórios e capacidade de atualização devem ser considerados.

A Tabela 15 aplica esses cuidados aos quatro artefatos, evitando utilizar a contagem isolada como ranking de segurança.

Tabela 15: Comparação aplicada aos quatro firmwares analisados

Firmware	Arquivos na raiz segura	Resultado histórico	Resultado da reprodução	Condição de comparação	Limitação decisória
D-Link DIR-842 R1 3.0.3	1.000	7 ocorrências agregadas	3 achados criptográficos validados	Chaves e certificados integrados a executáveis; suporte histórico e exposição não recompostos	Confirmar ativação, alcance, reutilização entre unidades e correção disponível
Intelbras RG1200 2.1.8	646	11 ocorrências agregadas	1 chave privada e 3 credenciais padrão	Presença em arquivos e referência no `httpd`; sem validação dinâmica	Confirmar serviços ativos, alteração dos padrões e política de atualização
OpenWrt 22.03.5	1.046	3 ocorrências agregadas	0 achado mantido na triagem específica	Maior transparência do artefato; zero mantido não equivale a ausência de falhas	Versão antiga, suporte e superfície executada precisam ser avaliados separadamente
TP-Link Archer C7 v5 20220715	2.090	13 ocorrências agregadas	31 candidatos do curl/libcurl e 4 achados de logging	Os 31 registros pertencem a um único componente confirmado; aplicabilidade varia por função e compilação	Verificar backports, uso das funções afetadas, exposição e tratamento dos logs

Fonte: Elaborado pelo autor (2026), a partir do estudo de base e da reprodução direcionada.

A análise estática revela conteúdo interno que scanners de rede podem não observar. Em contrapartida, scanners, testes de intrusão, emulação e Red Team verificam exposição, comportamento, encadeamento e impacto que a inspeção estática não comprova. O valor do MARF-GC está em organizar essa complementaridade, registrar o nível de confiança e indicar validações adicionais.

4.3 MARF-GC: MODELO CONCEITUAL PARA AUDITORIA REPRODUZÍVEL DE FIRMWARE PARA GOVERNANÇA DE CIBERSEGURANÇA

A discussão desenvolvida até aqui evidencia que a segurança de firmware em dispositivos de rede sem fio e sistemas embarcados não pode ser tratada apenas como um problema pontual de detecção de vulnerabilidades. Os achados retomados nesta dissertação, articulados à literatura analisada, indicam que a exposição ao risco também depende da capacidade institucional de inspecionar componentes embarcados, produzir evidências auditáveis, acompanhar atualizações e reduzir assimetrias de informação em relação aos fornecedores.

Nesse contexto, propõe-se o MARF-GC (Modelo Conceitual para Auditoria Reproduzível de Firmware para Governança de Cibersegurança), concebido como uma estrutura analítica voltada à articulação entre auditoria reproduzível de firmware, auditabilidade técnica e governança de cibersegurança em ambientes institucionais. A proposta busca organizar a análise de firmware em um processo tecnicamente reproduzível, documentalmente auditável e orientado à tomada de decisão organizacional.

Em ambientes acadêmicos, administrativos, laboratoriais e corporativos, dispositivos embarcados como roteadores, gateways, pontos de acesso e equipamentos de rede desempenham funções críticas para a conectividade, a autenticação, a segmentação lógica e a continuidade operacional. Nesses contextos, fragilidades na camada de firmware podem produzir impactos que ultrapassam o dispositivo isolado, afetando serviços, ampliando dependências tecnológicas e dificultando a avaliação institucional de risco. Assim, o modelo proposto busca deslocar a análise de firmware de uma atividade estritamente técnica para um instrumento de apoio à governança de cibersegurança.

O MARF-GC está organizado em seis etapas complementares: (i) aquisição do firmware; (ii) extração e decomposição; (iii) auditoria técnica; (iv) classificação de risco; (v) integração com a governança; e (vi) reprodutibilidade e produção de evidências. A Figura 9 apresenta a estrutura conceitual do modelo.

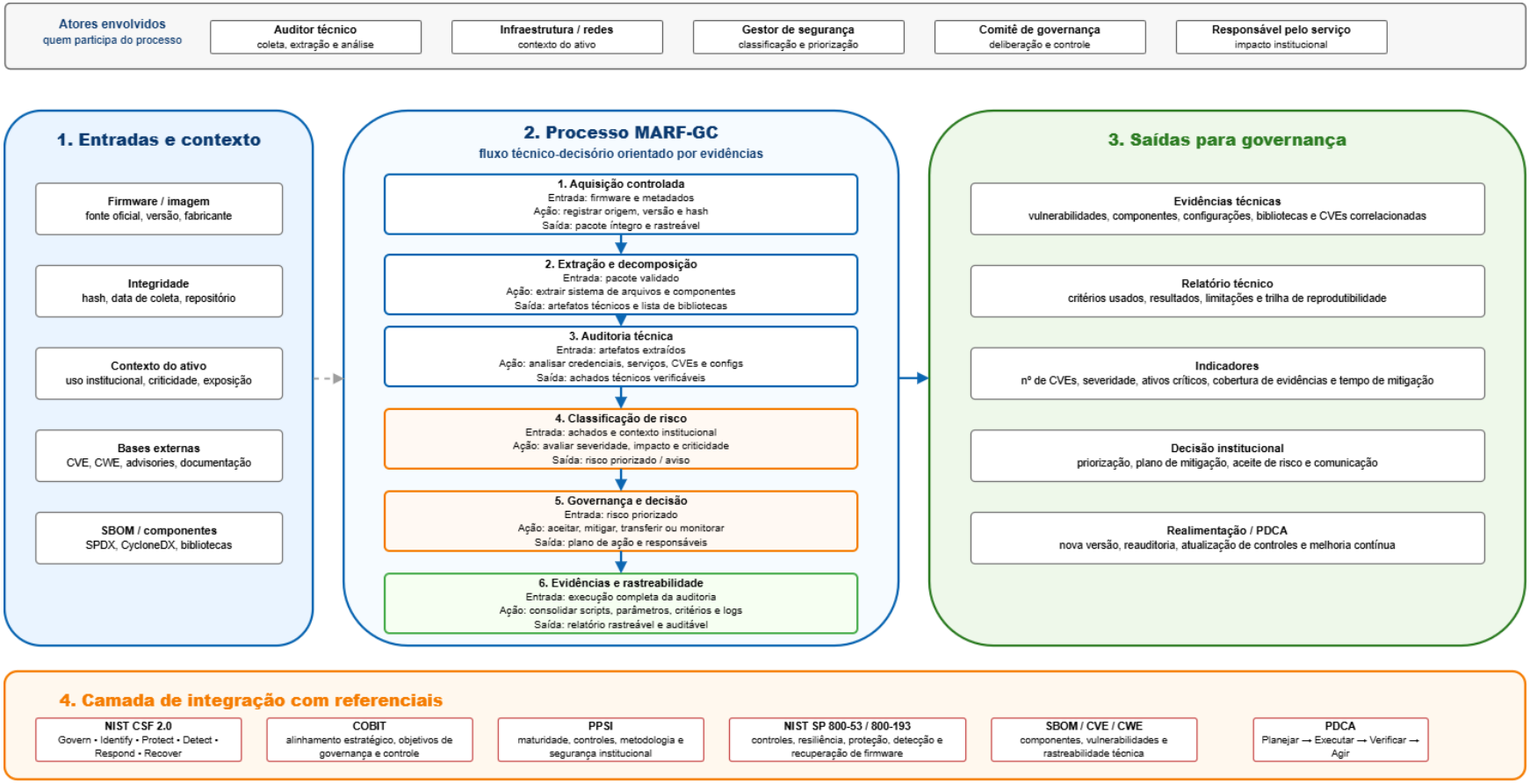

Figura 9: MARF-GC: Modelo para Auditoria Reproduzível de Firmware para Governança de Cibersegurança.

Fonte: Elaborado pelo autor (2026).

As etapas técnicas do MARF-GC (aquisição, extração, auditoria técnica e produção de evidências) retomam deliberadamente a mesma lógica de análise estática apresentada na Figura 4 (Seção 2.9) e no pipeline metodológico da Figura 6 (Seção 3.2), pois essas etapas constituem a base técnica necessária de qualquer auditoria reproduzível de firmware. A contribuição do MARF-GC em relação a esses dois fluxos anteriores está nas camadas adicionadas: atores institucionais, saídas voltadas à governança (Tabela 16) e integração explícita com referenciais normativos (Tabela 17), detalhadas na Seção 4.3.2.

A primeira etapa corresponde à aquisição do firmware a partir de fontes oficiais dos fabricantes ou de projetos de código aberto. Nessa fase, devem ser registrados a origem do arquivo, a versão analisada e, sempre que possível, mecanismos de verificação de integridade, como *hashes* ou *checksums*. Esse procedimento contribui para reduzir o risco de análise de imagens adulteradas e fortalece a rastreabilidade do processo.

A segunda etapa envolve a extração e a decomposição do firmware. Nessa fase, ferramentas como o Binwalk permitem identificar a estrutura interna da imagem, incluindo sistemas de arquivos embarcados, bibliotecas compartilhadas, scripts de inicialização, arquivos de configuração e componentes executáveis. Essa decomposição fornece a base técnica necessária para a inspeção dos elementos que compõem o firmware.

A terceira etapa consiste na auditoria técnica propriamente dita. Nela são investigados padrões recorrentes de fragilidade, como credenciais embutidas, bibliotecas desatualizadas, serviços inseguros, permissões frágeis, configurações padrão e componentes de terceiros sem rastreabilidade adequada. Essa etapa se conecta diretamente aos achados observados no estudo empírico retomado nesta dissertação, especialmente no que se refere à presença de componentes vulneráveis e à baixa visibilidade sobre dependências internas.

A quarta etapa corresponde à classificação de risco. Nesse ponto, os achados deixam de ser tratados apenas como falhas técnicas isoladas e passam a ser interpretados à luz de sua criticidade, possibilidade de exploração, impacto operacional e relevância institucional. Em ambientes conectados, uma vulnerabilidade em firmware pode afetar não apenas o dispositivo analisado, mas também a disponibilidade de serviços, a segmentação da rede, a integridade das comunicações e a exposição de outros ativos interdependentes.

A quinta etapa trata da integração dos achados com a governança de cibersegurança. Os resultados da auditoria devem ser convertidos em subsídios para decisões institucionais, como atualização de firmware, substituição de equipamentos sem suporte, segmentação de dispositivos críticos, restrição de serviços inseguros e definição de critérios para aquisição de novas tecnologias. Essa etapa aproxima a análise técnica da tomada de decisão organizacional e reforça o papel do firmware como elemento relevante da gestão de riscos.

Por fim, a sexta etapa enfatiza a reprodutibilidade da análise e a produção de evidências auditáveis. O processo deve registrar ferramentas utilizadas, parâmetros de execução, versões analisadas, resultados obtidos e critérios de interpretação. Com isso, a auditoria pode ser repetida, revisada e comparada em ciclos futuros, fortalecendo a transparência, a verificabilidade e a confiabilidade da avaliação.

A principal contribuição do MARF-GC está na articulação entre análise técnica de firmware, auditabilidade, rastreabilidade e governança institucional. Nessa perspectiva, a auditoria reproduzível deixa de ser

compreendida apenas como prática operacional de segurança e passa a atuar como instrumento conceitual de apoio à gestão de riscos em ambientes dependentes de dispositivos de rede sem fio.

4.3.1 Contribuição Específica e Entregáveis Obrigatórios

O MARF-GC não propõe uma nova técnica de detecção, exploração ou análise binária. Sua contribuição específica consiste em estruturar a passagem entre evidências internas do firmware, validações técnicas complementares, classificação contextual do risco e decisão institucional documentada. Um processo convencional de gestão de vulnerabilidades pode registrar uma CVE e acompanhar sua correção; o MARF-GC exige, adicionalmente, a origem e a integridade da imagem, o contexto do ativo, o grau de confiança do achado, a distinção entre correlação e explorabilidade, a responsabilidade decisória, o tratamento, o risco residual e o gatilho de reauditoria.

Os produtos mínimos do modelo são:

1. inventário do ativo e do firmware, com fabricante, modelo, versão, suporte e criticidade;
2. registro de origem e integridade da imagem;
3. inventário de componentes e escopo efetivamente analisado;
4. relação individualizada de achados, evidências e grau de confiança;
5. classificação técnica e avaliação do contexto institucional;
6. decisão de tratamento, responsável, prazo e risco residual;
7. controles defensivos ou validações complementares requeridas;
8. trilha preservada de ferramentas, parâmetros, limitações e resultados;
9. data ou condição de nova auditoria.

Sem esses entregáveis, o modelo pode ser reduzido a um fluxograma genérico. Com eles, torna-se uma estrutura de rastreabilidade entre análise, operação de segurança e governança.

4.3.2 Entradas, Saídas, Atores e Integração com Referenciais de Governança

Para fortalecer sua aplicabilidade institucional, o MARF-GC pode ser descrito a partir de quatro dimensões complementares: entradas, saídas, atores e integração com referenciais de governança. Essa estrutura permite explicitar que o modelo não se limita à execução de ferramentas de análise estática, mas organiza um processo decisório orientado por evidências técnicas, critérios de risco e responsabilidades institucionais.

As entradas do modelo correspondem aos elementos necessários para iniciar a auditoria reproduzível de firmware, incluindo imagem de firmware, fonte de obtenção, versão, fabricante, modelo do dispositivo,

hash de integridade, contexto do ativo, criticidade institucional, documentação técnica disponível e bases públicas de vulnerabilidades. As saídas correspondem aos artefatos produzidos ao longo do processo, como componentes identificados, bibliotecas analisadas, CVEs correlacionadas, serviços expostos, configurações inseguras, classificação de risco, relatório técnico, recomendações de mitigação e registros de rastreabilidade.

Tomando como referência o cenário institucional descrito na Seção 3.2.4, os atores do MARF-GC podem ser mapeados, a título de exemplo, da seguinte forma: o auditor técnico corresponderia a um servidor técnico-administrativo ou bolsista de TI lotado no Departamento, responsável pela execução da análise; a equipe de infraestrutura de redes corresponderia ao setor de suporte técnico do Departamento, responsável pelo contexto operacional dos ativos; o gestor de segurança da informação corresponderia ao Núcleo de Tecnologia da Informação (NTI) central da instituição, responsável pela priorização de riscos entre múltiplas unidades; e o comitê de governança corresponderia a uma instância colegiada de segurança da informação, compatível com estruturas institucionais de governança previstas em referenciais como o PPSI (Seção 2.12.1), responsável por deliberar sobre mitigação, aceitação ou transferência dos riscos identificados.

Tabela 16: Mapeamento entre etapas do MARF-GC, evidências e referenciais de governança

Etapa do MARF-GC	**Entradas principais**	**Saídas / evidências**	**Atores envolvidos**	**Referenciais relacionados**
Aquisição do firmware	Fonte oficial, versão, fabricante, modelo, hash e documentação disponível.	Registro de origem, versão analisada e integridade da imagem.	Auditor técnico e equipe de infraestrutura.	NIST CSF 2.0 – Identify; NIST SP 800-53; ISO/IEC 27001.
Extração e decomposição	Imagem de firmware e ferramentas de extração.	Sistema de arquivos extraído, bibliotecas, scripts, binários e arquivos de configuração.	Auditor técnico.	SBOM, SPDX, CycloneDX; NIST SP 800-53; ISO/IEC 27402.
Auditoria técnica	Componentes extraídos, bases CVE, regras de análise e padrões sensíveis.	Credenciais embutidas, bibliotecas vulneráveis, serviços inseguros e configurações frágeis.	Auditor técnico e analista de segurança.	CIS Controls; NIST SP 800-53; ETSI EN 303 645.
Classificação de risco	Achados técnicos, criticidade do ativo, exposição e impacto institucional.	Severidade, impacto, prioridade e recomendação preliminar de tratamento.	Gestor de segurança, equipe de infraestrutura e responsável pelo serviço.	NIST CSF 2.0 – Govern e Identify; COBIT; ISO/IEC 27001.
Governança e decisão	Relatório técnico, classificação de risco, contexto operacional e restrições institucionais.	Decisão sobre atualização, substituição, segmentação, mitigação, aceitação ou monitoramento do risco.	Gestor de segurança, comitê de governança e responsável pelo ativo.	COBIT; NIST CSF 2.0 – Govern, Protect e Respond; ISO/IEC 27001.
Evidências e reprodutibilidade	Ferramentas, parâmetros, versões, critérios utilizados e resultados da análise.	Relatório auditável, trilha de evidências, indicadores e base para reauditorias.	Auditor técnico, gestão de segurança e auditoria interna.	NIST SP 800-53; NIST SP 800-193; SBOM; PDCA; COBIT.

Fonte: Elaborado pelo autor (2026).

Esse mapeamento evidencia que o MARF-GC não substitui frameworks consolidados como NIST CSF, COBIT, CIS Controls ou ISO/IEC 27001. Sua função é complementar esses referenciais, oferecendo uma camada analítica específica para firmware de dispositivos de rede sem fio e sistemas embarcados.

Enquanto os frameworks indicam objetivos de governança, controle, identificação de riscos, proteção e monitoramento, o MARF-GC organiza como evidências técnicas extraídas de firmware podem alimentar esses processos institucionais.

Tabela 17: Contribuição específica do MARF-GC em relação aos referenciais de governança (NIST CSF 2.0, COBIT e PPSI já detalhados na Tabela 2)

Dimensão do MARF-GC	**Contribuição específica do MARF-GC**
Inventário e contexto do ativo	Detalha informações específicas de firmware, como fabricante, modelo, versão, hash, suporte e criticidade do dispositivo de rede ou sistema embarcado.
Aquisição e verificação do firmware	Define evidências mínimas para comprovar origem, integridade e reprodutibilidade da análise de firmware.
Extração e análise técnica	Operacionaliza a coleta de evidências técnicas na camada de firmware, normalmente pouco detalhada em frameworks amplos.
Classificação de risco	Traduz vulnerabilidades técnicas em critérios institucionais de severidade, impacto e prioridade de tratamento.
Decisão institucional	Estrutura decisões sobre atualização, substituição, segmentação, endurecimento, monitoramento ou aceitação temporária do risco.
Evidências e melhoria contínua	Preserva trilha auditável de ferramentas, versões, parâmetros, achados, limitações e recomendações para reauditorias.

Fonte: Elaborado pelo autor (2026).

A Tabela 17 evidencia a função complementar do MARF-GC em relação a referenciais consolidados de governança e segurança da informação. Enquanto o NIST CSF 2.0 oferece uma estrutura ampla para governar, identificar, proteger, detectar, responder e recuperar, o COBIT contribui para a governança, responsabilização, controle e alinhamento institucional da tecnologia da informação. O PPSI, por sua vez, fornece um referencial brasileiro voltado à maturidade, à metodologia, à governança e aos controles de privacidade e segurança da informação em instituições públicas [23, 30, 39, 40].

A contribuição específica do MARF-GC está em preencher a lacuna operacional existente entre esses referenciais amplos e a necessidade prática de auditar firmware em dispositivos de rede sem fio e sistemas embarcados. O modelo organiza como evidências técnicas, tais como versões de firmware, bibliotecas, serviços expostos, CVEs, arquivos de configuração, hashes e trilhas de análise, podem ser convertidas em informações úteis para gestão de riscos, priorização de mitigação e tomada de decisão institucional. Dessa forma, o MARF-GC atua como uma ponte entre a camada técnica da segurança de firmware e a camada decisória da governança de cibersegurança.

O fluxo decisório associado ao MARF-GC pode ser compreendido de forma cíclica. Inicialmente, a organização identifica o ativo e coleta a imagem de firmware. Em seguida, realiza a análise técnica, documenta os achados e classifica os riscos. A partir dessa classificação, os atores institucionais decidem entre atualizar o firmware, substituir o equipamento, segmentar o ativo, restringir serviços expostos, aceitar temporariamente o risco ou programar nova auditoria. Após a decisão, os resultados devem ser registrados e realimentar o inventário, as políticas de atualização, os critérios de aquisição e os ciclos futuros de monitoramento.

Essa lógica aproxima o MARF-GC do ciclo PDCA (*Plan, Do, Check, Act*). Na etapa de planejamento, são definidos ativos, escopo, critérios e responsabilidades. Na execução, ocorre a auditoria técnica do

firmware. Na verificação, os achados são avaliados quanto à severidade, impacto e aderência a políticas institucionais. Na ação, são implementadas medidas de mitigação, atualização, substituição ou melhoria de controles. Dessa forma, o modelo favorece uma governança contínua, documentada e orientada por evidências.

Também é possível associar indicadores ao modelo, tais como: percentual de dispositivos de rede sem fio inventariados; percentual de firmwares com versão documentada; quantidade de correlações com CVEs por dispositivo e respectivo estado de validação; percentual de ativos com firmware atualizado; tempo médio entre identificação e tratamento de vulnerabilidades; quantidade de dispositivos sem suporte do fabricante; percentual de análises com trilha de evidências completa; e número de recomendações de mitigação efetivamente implementadas. Esses indicadores ampliam a utilidade institucional do MARF-GC, permitindo acompanhar a evolução da maturidade da governança de firmware ao longo do tempo.

4.3.3 Lógica de Classificação do Risco Institucional

O estudo de base classificou as ocorrências agregadas segundo o CVSS v3.1. O CVSS comunica características técnicas de uma vulnerabilidade, mas não representa sozinho o risco para uma instituição. Para a aplicação atual do MARF-GC, a severidade técnica deve ser complementada por informações de ameaça e ambiente, em consonância com a separação entre métricas técnicas e contexto organizacional prevista nas versões atuais do CVSS. O modelo utiliza uma lógica contextual inspirada em avaliação de riscos, separando *probabilidade* e *impacto* e preservando o grau de confiança do achado [45, 49, 50].

A probabilidade é classificada como baixa, média ou alta a partir da combinação entre: exposição do serviço; evidência de uso do componente; existência de código de exploração ou registro de exploração conhecida; condições de autenticação e acesso; e presença de controles compensatórios. O impacto é classificado como baixo, médio ou alto considerando: criticidade do ativo; dependência de serviços; sensibilidade dos dados; possibilidade de interrupção, alteração de tráfego ou movimentação lateral; e capacidade institucional de recuperação.

Tabela 18: Matriz qualitativa de risco do MARF-GC

Probabilidade / Impacto	**Baixo**	**Médio**	**Alto**
Baixa	Baixo	Baixo	Médio
Média	Baixo	Médio	Alto
Alta	Médio	Alto	Crítico

A matriz é aplicada somente depois da classificação da evidência. Uma CVE apenas correlacionada, sem confirmação de componente ativo, não recebe o mesmo grau de confiança de uma exposição observada ou exploração confirmada. A decisão também considera suporte e capacidade de tratamento: um equipamento crítico, sem atualização e sem telemetria, pode exigir substituição mesmo sem exploração pública conhecida; inversamente, uma correlação de severidade alta em biblioteca não utilizada pode ser rebaixada após validação técnica.

Tabela 19: Critérios de contexto utilizados na passagem de severidade técnica para risco institucional

Critério	Pergunta de avaliação	Efeito esperado
Confiança da evidência	O componente, a configuração ou a exposição foram confirmados?	Define o peso atribuído ao achado
Exposição	O serviço é externo, interno, restrito ou desabilitado?	Altera a probabilidade
Exploração conhecida	Há exploração observada, prova de conceito ou registro em catálogo de exploração conhecida?	Eleva a prioridade de validação e tratamento
Criticidade do ativo	O dispositivo sustenta serviço acadêmico, administrativo ou laboratorial essencial?	Altera o impacto
Dependências e movimento lateral	O comprometimento pode afetar outros segmentos ou serviços?	Eleva o impacto potencial
Atualização e suporte	Existe correção, suporte do fabricante ou alternativa viável?	Orienta atualizar, mitigar ou substituir
Controles compensatórios	Segmentação, firewall, autenticação e monitoramento reduzem a exposição?	Reduz probabilidade e risco residual
Capacidade de detecção e resposta	Há logs, telemetria e responsáveis definidos?	Afeta tempo de resposta e risco residual

A classificação final deve registrar a justificativa, o responsável, a data, as fontes de evidência e o risco residual. O modelo não impõe pesos universais porque instituições possuem critérios distintos; ele exige, contudo, que a regra adotada seja explícita, repetível e aprovada pela governança.

4.3.4 Integração com Red Team, Blue Team e Purple Team

A auditoria estática pode iniciar um ciclo operacional: um componente ou configuração potencialmente vulnerável é identificado; o teste de intrusão ou Red Team verifica, quando autorizado e necessário, a exposição e o caminho de exploração; o Blue Team avalia a capacidade de bloquear, detectar e responder; e uma dinâmica Purple Team ajusta controles e valida novamente o cenário. Os resultados são então encaminhados à governança, que decide entre atualizar, mitigar, segmentar, aceitar temporariamente ou substituir o ativo.

Tabela 20: Papel das equipes no ciclo do MARF-GC

Ator	Contribuição	Saída para o modelo
Auditor de firmware	Extrai, identifica, correlaciona e preserva evidências	Registro técnico, confiança e limitações
Gestão de vulnerabilidades	Consolida boletins, suporte, prazos e exposição	Prioridade preliminar e acompanhamento
Red Team / teste de intrusão	Valida caminho de ataque, explorabilidade e impacto	Evidência de exposição ou exploração
Blue Team / SOC	Define segmentação, regras, telemetria e detecções	Controles, casos de uso e risco residual
Purple Team	Integra teste e defesa em ciclos controlados	Evidência de eficácia dos controles
Gestor do ativo e governança	Avaliam criticidade, custo, continuidade e responsabilidade	Decisão, prazo, aceitação e reauditoria

4.3.5 Aplicação Ilustrativa do MARF-GC aos Achados da Reprodução

A aplicação permanece retrospectiva e ilustrativa, mas passa a utilizar evidências concretas da reprodução direcionada. Três exemplos demonstram a passagem entre achado técnico, confiança, contexto, tratamento e decisão.

Componente curl/libcurl 7.79.1 no TP-Link. A correlação automática produziu 31 candidatos a CVE. A presença do componente foi confirmada em dois binários MIPS e as dependências foram inspecionadas. A ausência de NSS permitiu afastar a aplicabilidade da CVE-2022-27781 ao build observado, enquanto a ausência de evidência de IDN, HTTP/2 server push e SOCKS5 com resolução remota reduziu a confiança em outras correlações prioritárias. No MARF-GC, o resultado não seria convertido automaticamente em risco crítico: a gestão de vulnerabilidades verificaria backports e suporte; o Red Team ou teste de intrusão validaria os fluxos relevantes; o Blue Team revisaria segmentação e telemetria; e a governança decidiria entre atualizar, mitigar ou substituir o equipamento.

Chaves privadas embarcadas no D-Link. A inspeção confirmou quatro pares criptográficos no conjunto analisado, três deles no D-Link. Os arquivos possuíam chaves privadas legíveis sem senha, certificados correspondentes e referências em executáveis. O certificado TR-069 estava expirado desde 2015. O estado de validação é superior ao de uma simples ocorrência textual, pois a presença, a validade criptográfica e a integração ao componente foram confirmadas. Ainda assim, a exposição em rede não foi demonstrada. O tratamento recomendado inclui verificar reutilização entre unidades, substituir materiais compartilhados, restringir serviços e programar reauditoria.

Credenciais padrão e logging sensível. No Intelbras, três campos continham valores literais não vazios; no TP-Link, quatro arquivos possuíam código ativo de registro de variáveis de senha. O Blue Team poderia restringir os serviços, revisar permissões de logs, remover dados sensíveis da telemetria e monitorar tentativas de autenticação. A governança precisaria definir responsável, prazo, risco residual e critério de substituição caso não exista correção do fabricante.

Esses exemplos não validam empiricamente a efetividade do MARF-GC, mas demonstram que o modelo acrescenta uma trilha explícita entre evidência, grau de confiança, validação complementar, controle defensivo e decisão institucional. O Apêndice A apresenta uma ficha preenchida para o achado CRYPTO-03, explicitando risco, responsáveis, prazos e gatilho de reauditoria em caráter ilustrativo.

4.3.6 Aplicabilidade Institucional do MARF-GC

A aplicabilidade institucional do MARF-GC decorre da necessidade crescente de mecanismos estruturados para avaliação da segurança de dispositivos de rede sem fio e outros sistemas embarcados empregados em ambientes organizacionais. Em universidades, órgãos públicos, laboratórios, centros de pesquisa e outras infraestruturas conectadas, roteadores, gateways, pontos de acesso, câmeras, controladores e equipamentos embarcados frequentemente sustentam serviços essenciais de conectividade, autenticação, monitoramento e operação administrativa. Apesar disso, a camada de firmware costuma receber menor atenção do que sistemas operacionais, aplicações e controles de perímetro, o que pode ampliar a exposição a riscos pouco visíveis nos processos tradicionais de gestão de segurança.

Nesse contexto, o MARF-GC pode ser compreendido como um instrumento analítico de apoio à avaliação institucional de dispositivos conectados, especialmente em situações de aquisição, implantação, manutenção, substituição ou revisão de equipamentos já em uso. Em vez de se restringir à identificação pontual de falhas técnicas, o modelo favorece a incorporação de critérios relacionados à auditabilidade, à rastreabilidade de componentes, à transparência do ciclo de atualização, à dependência de fornecedores e à verificabilidade do firmware.

Essa aplicabilidade é particularmente relevante em organizações que operam com parque tecnológico heterogêneo, múltiplos fabricantes e restrições de pessoal, orçamento ou visibilidade técnica. Nesses cenários, decisões sobre permanência, substituição ou segmentação de dispositivos nem sempre podem ser baseadas apenas em desempenho, custo ou compatibilidade funcional. A presença de bibliotecas vulneráveis, a ausência de documentação técnica, a opacidade sobre componentes embarcados e a inexistência de políticas claras de atualização podem representar fatores relevantes de risco institucional, ainda que não sejam imediatamente perceptíveis em processos convencionais de aquisição ou inventário.

Sob essa perspectiva, o MARF-GC pode apoiar ao menos quatro frentes institucionais. A primeira diz respeito à avaliação prévia de dispositivos antes de sua adoção, permitindo incorporar critérios de segurança e auditabilidade ao processo de seleção tecnológica. A segunda envolve a revisão de ativos já implantados, com foco em identificação de equipamentos sem suporte, componentes vulneráveis e dependência excessiva de fornecedores. A terceira refere-se à priorização de medidas de mitigação, como segmentação de rede, substituição de dispositivos críticos, endurecimento de configuração e atualização de firmware. A quarta está relacionada à produção de evidências técnicas para subsidiar auditorias internas, processos de prestação de contas, documentação de risco e tomada de decisão em segurança da informação.

Além disso, a proposta apresenta potencial de articulação com práticas organizacionais já consolidadas em gestão de riscos e segurança da informação, especialmente aquelas alinhadas a referenciais como ISO/IEC 27001, ISO/IEC 27005 e NIST Cybersecurity Framework. Nessa perspectiva, o MARF-GC não substitui controles tradicionais de segurança, inventário de ativos, gestão de vulnerabilidades ou processos formais de governança. Seu papel é complementar esses mecanismos, introduzindo uma lente analítica voltada especificamente à camada de firmware, frequentemente negligenciada nas avaliações institucionais de risco.

Do ponto de vista da engenharia de segurança, a principal contribuição do modelo está em aproximar evidências técnicas produzidas na análise de firmware de processos institucionais de decisão. Isso permite ampliar a visibilidade sobre riscos associados a componentes embarcados, favorecendo discussões mais robustas sobre atualização, substituição de equipamentos, critérios de aquisição, segmentação de rede e continuidade operacional.

Embora o modelo tenha sido estruturado a partir de evidências derivadas da análise de roteadores Wi-Fi e firmware de dispositivos de rede, sua lógica analítica pode ser adaptada a outros cenários envolvendo sensores, dispositivos industriais, equipamentos de automação e diferentes infraestruturas conectadas. Essa possibilidade de adaptação não implica generalização irrestrita, mas indica que os princípios de auditabilidade, rastreabilidade, classificação de risco e produção de evidências podem oferecer utilidade em contextos organizacionais mais amplos.

Dessa forma, o MARF-GC contribui para reduzir a distância entre achados técnicos especializados e

processos institucionais de governança de cibersegurança, favorecendo maior integração entre análise de firmware, gestão de riscos, segurança da informação e continuidade operacional.

4.4 CONTRIBUIÇÕES DA ENGENHARIA DE SEGURANÇA

A perspectiva da engenharia de segurança permite compreender que vulnerabilidades em firmware não devem ser interpretadas apenas como falhas técnicas isoladas, mas como elementos capazes de impactar diretamente a confiabilidade, a disponibilidade e a resiliência de sistemas conectados. Em ambientes institucionais, dispositivos de rede sem fio frequentemente desempenham funções críticas na infraestrutura de comunicação, tornando sua proteção um componente estratégico da segurança operacional.

Sob essa ótica, a principal contribuição analítica desta dissertação consiste em articular segurança de firmware, auditabilidade técnica e governança de cibersegurança em uma abordagem integrada de avaliação de risco. Diferentemente de estudos predominantemente orientados à detecção técnica de vulnerabilidades, este trabalho busca ampliar a interpretação dos achados, considerando implicações institucionais relacionadas à rastreabilidade, dependência tecnológica, continuidade de serviços e capacidade organizacional de mitigação.

A contribuição da engenharia de segurança manifesta-se também na proposição do MARF-GC, concebido como um modelo conceitual voltado à organização de critérios reprodutíveis para análise de firmware em contextos institucionais. Mais do que estabelecer um procedimento técnico rígido, a proposta busca favorecer a articulação entre evidências técnicas, auditabilidade e processos institucionais de tomada de decisão, contribuindo para ampliar a compreensão sobre riscos associados a dispositivos embarcados.

Além disso, ao retomar resultados empíricos previamente obtidos e reinterpretá-los à luz da governança de cibersegurança, esta dissertação contribui para aproximar análise técnica e contexto organizacional, favorecendo uma visão mais abrangente sobre segurança em dispositivos de rede sem fio e sistemas embarcados. Essa integração amplia o potencial interpretativo dos achados em cenários institucionais, nos quais decisões relacionadas à infraestrutura digital precisam considerar simultaneamente desempenho, continuidade operacional e exposição a riscos cibernéticos.

Cabe destacar, ainda, que os resultados desta pesquisa devem ser compreendidos como evidências analíticas contextualizadas, derivadas de um escopo específico de análise e interpretadas sob uma perspectiva predominantemente qualitativa e interpretativa. Assim, os achados não pretendem estabelecer generalizações estatísticas para toda a diversidade de dispositivos conectados, mas oferecer subsídios analíticos relevantes para contextos institucionais semelhantes.

Dessa forma, entende-se que a engenharia de segurança possui papel central na construção de infraestruturas digitais mais resilientes, especialmente diante da crescente adoção de dispositivos conectados e equipamentos de rede sem fio em organizações públicas e privadas. Nesse contexto, a segurança de firmware deixa de ocupar posição periférica e passa a integrar dimensões estratégicas relacionadas à governança tecnológica, à gestão de riscos e à continuidade operacional.

4.5 O PAPEL DA AUDITABILIDADE

Um dos pontos centrais observados ao longo desta pesquisa é a relevância da auditabilidade como elemento estruturante da segurança de firmware e da governança de cibersegurança. Métodos de análise reproduzíveis, baseados em ferramentas abertas e procedimentos documentados, favorecem a rastreabilidade dos resultados, a transparência dos processos e a possibilidade de revisão técnica independente [1, 21]. A literatura também enfatiza a importância da reprodutibilidade em análises de segurança como elemento essencial para validação científica e construção de confiança em ambientes institucionais, especialmente quando decisões técnicas dependem de evidências verificáveis [1, 21].

Diferentemente de abordagens opacas ou dependentes exclusivamente de fornecedores, a auditabilidade permite que evidências técnicas sejam verificadas, reproduzidas e comparadas por diferentes atores. Essa característica é especialmente importante no contexto de dispositivos conectados, nos quais a complexidade do firmware e a reutilização de componentes de terceiros dificultam a avaliação direta de segurança.

Em ambientes acadêmicos e institucionais, a auditabilidade assume papel ainda mais relevante, pois a legitimidade das decisões técnicas frequentemente depende da capacidade de demonstrar evidências, justificar critérios adotados e comparar alternativas tecnológicas de forma sistemática. Nesse cenário, a ausência de mecanismos auditáveis pode gerar assimetrias de informação, limitando a capacidade institucional de avaliar riscos de forma independente.

Além disso, a auditabilidade contribui para reduzir a dependência de avaliações exclusivamente baseadas em fabricantes, permitindo que organizações desenvolvam maior autonomia na análise de sua própria infraestrutura. Essa autonomia é fundamental em contextos onde dispositivos de rede desempenham funções críticas e onde vulnerabilidades podem impactar diretamente a continuidade dos serviços.

Dessa forma, a incorporação de práticas auditáveis na análise de firmware não apenas fortalece a identificação de vulnerabilidades, mas também amplia a capacidade de governança, ao fornecer subsídios técnicos confiáveis para processos de gestão de riscos e tomada de decisão. Assim, a auditabilidade emerge como um elemento essencial na construção de infraestruturas digitais mais seguras, transparentes e resilientes.

4.6 FIRMWARE PROPRIETÁRIO E FIRMWARE DE CÓDIGO ABERTO

No conjunto específico analisado, o OpenWrt 22.03.5 apresentou menor quantidade de ocorrências correlacionadas e melhores condições de transparência, inspeção e rastreabilidade em comparação com os firmwares proprietários avaliados [1]. Esse resultado não autoriza concluir que software de código aberto seja universalmente mais seguro. Código disponível facilita revisão e verificação, mas não garante manutenção, atualização, qualidade de implementação ou ausência de vulnerabilidades.

Da mesma forma, firmware proprietário não é necessariamente pouco seguro. Fabricantes podem manter processos robustos de desenvolvimento, suporte, testes, assinatura e resposta a vulnerabilidades, mesmo sem disponibilizar o código-fonte. O problema institucional surge quando a organização não recebe informação suficiente sobre componentes, suporte, atualizações, correções e mecanismos de verificação.

Tabela 21: Critérios institucionais de comparação entre firmwares proprietários e de código aberto

Critério	Questão para avaliação	Evidência desejável
Transparência de componentes	A composição do firmware pode ser conhecida e atualizada?	SBOM, versões, dependências e boletins
Auditabilidade	É possível inspecionar ou verificar independentemente o artefato?	Código, documentação, hashes, interfaces de teste ou auditoria por terceiro
Suporte e atualização	Há prazo de suporte e correções tempestivas?	Política de ciclo de vida, canal de atualização e histórico
Resposta a vulnerabilidades	Existe processo de recebimento, triagem e divulgação?	PSIRT, política de divulgação e avisos de segurança
Integridade e recuperação	O dispositivo verifica e recupera firmware confiável?	Assinatura, secure boot, rollback seguro e recuperação
Adequação institucional	O risco pode ser monitorado, mitigado e justificado?	Telemetria, segmentação, suporte e documentação contratual

A auditabilidade deve ser tratada como um critério de governança e aquisição, não como sinônimo de segurança. Em processos institucionais, pode ser exigida por meio de SBOM, documentação técnica, política de suporte, mecanismos seguros de atualização, evidências de integridade, resposta a vulnerabilidades e possibilidade de verificação independente.

4.7 GOVERNANÇA DE CIBERSEGURANÇA E GESTÃO DE RISCOS

A governança de cibersegurança pressupõe a capacidade organizacional de identificar riscos, priorizar ações e definir mecanismos de mitigação de forma estruturada e contínua. Nesse contexto, a efetividade da governança está diretamente relacionada à visibilidade e à auditabilidade dos componentes que compõem a infraestrutura tecnológica. Quando camadas críticas, como o firmware de dispositivos de rede sem fio e sistemas embarcados, são opacas, desatualizadas ou de difícil análise, a própria governança institucional torna-se limitada, reduzindo a capacidade de avaliação de risco e comprometendo a tomada de decisão baseada em evidências [25, 26, 27, 28]. Abordagens contemporâneas de governança de cibersegurança reforçam a necessidade de visibilidade contínua sobre componentes críticos da infraestrutura, incluindo firmware, como forma de apoiar estratégias eficazes de gestão de riscos em ambientes de dispositivos conectados [23, 45].

Retomando a distinção estabelecida na Seção 2.11, os trabalhos citados a seguir, voltados à rotina operacional do ONS e à auditoria interna em instituições financeiras, situam-se predominantemente no nível de gestão de riscos e controle operacional. Isso não reduz sua relevância, mas reforça que a produção de evidências técnicas (gestão) é insumo necessário, porém não suficiente, para a governança propriamente dita, que exige também definição de política, autoridade decisória e prestação de contas, dimensão que o MARF-GC endereça explicitamente em sua etapa 5 (Seção 4.3).

No contexto do PPEE/UnB, estudos recentes também têm abordado a cibersegurança sob perspectivas relacionadas à governança, gestão de riscos e controles institucionais e tomada de decisão. [46], ao ana-

lisar a gestão de riscos cibernéticos no setor elétrico brasileiro sob a ótica da rotina operacional do ONS, evidencia a importância de controles mínimos, estruturas regulatórias e mecanismos de avaliação para ambientes críticos. De forma complementar, [47] discute o papel da auditoria interna na gestão de riscos cibernéticos em instituições financeiras brasileiras, destacando a relevância da avaliação independente, da governança e da integração entre controles técnicos e processos organizacionais. Esses trabalhos reforçam que a cibersegurança, no contexto do PPEE, vem sendo abordada não apenas como questão técnica, mas como dimensão estratégica de governança, risco e continuidade institucional.

Essa limitação é particularmente relevante em ambientes institucionais, nos quais dispositivos de rede sem fio desempenham papel estrutural na conectividade e na operação de serviços. Vulnerabilidades em firmware podem impactar não apenas dispositivos isolados, mas também a disponibilidade de serviços, a segmentação da rede e a integridade dos fluxos de comunicação. Dessa forma, a ausência de mecanismos sistemáticos de avaliação de firmware introduz um ponto cego na gestão de riscos, fragilizando a governança de cibersegurança.

Nesse cenário, a segurança de firmware deve ser incorporada de forma explícita às práticas de gestão de riscos, padronização tecnológica e monitoramento da infraestrutura. Isso envolve a definição de critérios para seleção de dispositivos, exigência de políticas de atualização seguras, priorização de tecnologias auditáveis e adoção de mecanismos de segmentação e controle de serviços expostos. Mais do que uma prática técnica, trata-se de um elemento estratégico que amplia a capacidade institucional de antecipar vulnerabilidades e reduzir a dependência de avaliações exclusivamente baseadas em fornecedores.

Além disso, a ausência de visibilidade sobre o firmware compromete a capacidade institucional de realizar avaliações independentes de segurança, criando dependência de fornecedores e reduzindo a autonomia na tomada de decisão. Esse cenário é particularmente crítico em ambientes acadêmicos e governamentais, nos quais a transparência, a auditabilidade e a justificativa técnica das decisões são elementos fundamentais para a governança de cibersegurança. Com base nos achados deste estudo, propõe-se um modelo conceitual de governança de firmware para ambientes institucionais, integrando práticas de inventário, monitoramento de vulnerabilidades, políticas de atualização e produção de evidências auditáveis.

Figura 10: Modelo conceitual de governança para gestão de firmware em dispositivos de rede sem fio em ambientes institucionais.

Fonte: Elaborado pelo autor (2026).

A Figura 10 sintetiza um modelo conceitual de governança de firmware em ambientes institucionais. Nesse modelo, inventário de dispositivos, monitoramento de vulnerabilidades, políticas de atualização segura, gestão de riscos e auditoria são integrados como componentes interdependentes. Essa integração permite não apenas a identificação de vulnerabilidades, mas também a produção de evidências técnicas que sustentam decisões organizacionais.

Assim, a incorporação da análise de firmware à governança de cibersegurança contribui para reduzir assimetrias de informação, aumentar a rastreabilidade das decisões e fortalecer a capacidade institucional de resposta a incidentes. Em ambientes cada vez mais dependentes de dispositivos de rede sem fio e sistemas embarcados, essa abordagem representa um avanço na maturidade da gestão de riscos e na construção de infraestruturas digitais mais seguras e resilientes [25, 26, 27, 28].

4.8 SÍNTESE DOS ACHADOS E IMPLICAÇÕES INSTITUCIONAIS

A análise desenvolvida neste capítulo evidencia que a segurança de firmware em dispositivos de rede sem fio deve ser compreendida como um problema técnico e institucional. Os achados retomados a partir do estudo empírico indicam a presença de vulnerabilidades associadas a bibliotecas desatualizadas, serviços expostos, credenciais embutidas e componentes de terceiros com baixa rastreabilidade. Embora tais fragilidades sejam inicialmente identificadas na camada técnica, seus efeitos podem alcançar a disponibilidade dos serviços, a segmentação da rede, a continuidade operacional e a capacidade institucional de

gestão de riscos.

A comparação entre firmwares proprietários e de código aberto reforçou que a quantidade de ocorrências correlacionadas não deve ser interpretada isoladamente como medida absoluta de segurança. O ponto central observado está na diferença de condições de auditabilidade, transparência e rastreabilidade dos componentes internos. Em ambientes proprietários, a menor visibilidade sobre bibliotecas, versões, correções e dependências pode ampliar a assimetria de informação entre instituições e fornecedores, dificultando processos de verificação independente e tomada de decisão baseada em evidências.

Nesse contexto, a auditoria reproduzível de firmware assume papel relevante ao permitir que procedimentos de aquisição, extração, inspeção, classificação e documentação sejam registrados e repetidos. Essa característica amplia a confiabilidade dos achados técnicos e favorece sua utilização em processos institucionais de governança, como gestão de vulnerabilidades, definição de critérios de aquisição, priorização de atualizações, substituição de ativos obsoletos e segmentação de dispositivos críticos.

Dessa forma, os achados discutidos neste capítulo sustentam a necessidade de integrar a análise de firmware às estratégias institucionais de cibersegurança. A principal implicação é que a segurança de dispositivos de rede sem fio não pode depender apenas de controles perimetrais ou de atualizações fornecidas pelos fabricantes, exigindo mecanismos internos de avaliação, rastreabilidade e produção de evidências. É nesse ponto que o MARF-GC se apresenta como uma proposta conceitual para aproximar auditoria técnica, auditabilidade e governança de cibersegurança em ambientes organizacionais.

4.9 DIRETRIZES INSTITUCIONAIS PARA GOVERNANÇA DE FIRMWARE EM DISPOSITIVOS DE REDE SEM FIO

A partir dos achados discutidos nesta dissertação, é possível identificar um conjunto de diretrizes institucionais voltadas à governança de firmware em dispositivos de rede sem fio e equipamentos embarcados. Essas diretrizes não têm como finalidade substituir normas, políticas ou referenciais consolidados de segurança da informação, mas oferecer subsídios analíticos que possam apoiar instituições na avaliação, aquisição, implantação e manutenção de dispositivos embarcados conectados.

A primeira diretriz refere-se à manutenção de um inventário atualizado de dispositivos de rede sem fio e seus respectivos firmwares. Esse inventário pode contemplar informações como fabricante, modelo, versão do firmware, data da última atualização, finalidade do dispositivo, segmento de rede e criticidade operacional. A ausência desse tipo de controle tende a dificultar a compreensão sobre exposição a vulnerabilidades conhecidas e a priorização de ações de mitigação.

A segunda diretriz relaciona-se à definição de políticas mínimas de atualização de firmware. Em contextos institucionais, torna-se relevante acompanhar boletins de segurança, identificar dispositivos sem suporte, observar versões desatualizadas e estabelecer procedimentos compatíveis com a continuidade operacional dos serviços. Essa prática pode favorecer uma melhor compreensão dos riscos associados à permanência de versões vulneráveis em ambientes produtivos.

A terceira diretriz envolve a consideração de critérios de segurança na aquisição de dispositivos de rede

sem fio e equipamentos embarcados. Além de aspectos relacionados a desempenho, custo e compatibilidade, os achados discutidos nesta pesquisa sugerem a relevância de considerar fatores como suporte do fabricante, frequência de atualizações, disponibilidade de documentação técnica, mecanismos de atualização segura e possibilidades de verificação independente do firmware.

A quarta diretriz refere-se à segmentação lógica de dispositivos de rede sem fio e outros equipamentos embarcados em domínios de rede apropriados. Equipamentos embarcados, especialmente aqueles com baixa transparência técnica ou suporte limitado, podem representar vetores de risco adicionais quando posicionados em segmentos compartilhados com serviços administrativos, sistemas críticos ou ambientes sensíveis. Nesse sentido, estratégias de segmentação podem contribuir para reduzir potenciais impactos decorrentes de comprometimentos.

A quinta diretriz consiste na realização periódica de procedimentos de auditoria de firmware, particularmente em dispositivos críticos ou amplamente distribuídos na infraestrutura institucional. Tais procedimentos podem ser organizados com base nos elementos conceituais propostos pelo MARF-GC, incluindo aquisição da imagem, verificação de integridade, extração, análise estática, identificação de componentes vulneráveis e documentação dos achados.

A sexta diretriz enfatiza a importância da produção e preservação de evidências auditáveis. Registros relacionados às análises realizadas, versões avaliadas, ferramentas empregadas, parâmetros utilizados e decisões técnicas adotadas podem contribuir para ampliar a rastreabilidade, apoiar processos de governança e fortalecer mecanismos institucionais de prestação de contas e gestão de riscos.

Tabela 22: Diretrizes institucionais para governança de firmware em dispositivos de rede sem fio

Diretriz	**Descrição**	**Potencial contribuição institucional**
Inventário de dispositivos	Registro de fabricante, modelo, versão de firmware, localização lógica e criticidade	Favorece maior visibilidade sobre ativos e apoio à priorização de riscos
Política de atualização	Acompanhamento, validação e aplicação de atualizações conforme contexto operacional	Contribui para redução da exposição a vulnerabilidades conhecidas
Critérios de aquisição	Consideração de suporte, documentação, atualização segura e auditabilidade	Favorece decisões mais informadas sobre dependência tecnológica e transparência
Segmentação de rede	Organização de dispositivos de rede sem fio em domínios compatíveis com criticidade operacional	Pode reduzir impactos associados à movimentação lateral e comprometimentos
Auditoria periódica	Aplicação recorrente de análise estática e verificação de componentes	Contribui para compreensão contínua de fragilidades e evolução do risco
Evidências auditáveis	Registro de ferramentas, versões, parâmetros, achados e decisões técnicas	Fortalece rastreabilidade, transparência e suporte à governança

A Tabela 22 sintetiza diretrizes institucionais derivadas da discussão desenvolvida nesta dissertação. Em conjunto, tais elementos sugerem possibilidades para aproximar a análise de firmware de práticas organizacionais relacionadas à governança, gestão de riscos e tomada de decisão em cibersegurança.

Em ambientes acadêmicos, administrativos e governamentais, essas diretrizes podem oferecer subsí-

dios para reflexão sobre políticas institucionais voltadas à segurança de dispositivos de rede sem fio e sistemas embarcados. Além disso, a adoção de práticas relacionadas à rastreabilidade técnica e à auditabilidade tende a favorecer maior compreensão institucional sobre dependências tecnológicas e riscos associados ao ciclo de vida dos firmwares.

Dessa forma, a governança de firmware em dispositivos de rede sem fio pode ser compreendida como um processo contínuo e contextualizado, cuja maturidade depende da articulação entre inventário, atualização, segmentação, auditabilidade e produção de evidências técnicas. Contudo, tais diretrizes devem ser interpretadas como contribuições analíticas derivadas do escopo desta pesquisa, de caráter predominantemente qualitativo e interpretativo, e não como prescrições normativas universalmente aplicáveis.

5 CONCLUSÃO

Esta dissertação analisou a segurança de firmware em pontos de acesso sem fio, considerando também as funções de roteamento presentes nos equipamentos do corpus, e discutiu suas implicações para a governança de cibersegurança em ambientes institucionais. A partir da articulação entre revisão da literatura, análise documental de referenciais normativos e retomada crítica de evidências empíricas previamente produzidas, o estudo permitiu examinar a segurança de firmware não apenas sob a ótica da identificação de vulnerabilidades, mas também como elemento relevante para a gestão de riscos, a auditabilidade e a tomada de decisão organizacional.

Os resultados discutidos ao longo da pesquisa indicam que o firmware deve ser compreendido como uma camada crítica da infraestrutura digital contemporânea, especialmente em dispositivos responsáveis por funções estruturais de conectividade, autenticação e controle de tráfego. Nesses contextos, vulnerabilidades em firmware não se restringem ao equipamento isolado, podendo afetar a disponibilidade de serviços, a segmentação lógica da rede, a integridade dos fluxos de comunicação e a continuidade operacional de ambientes acadêmicos, administrativos e governamentais.

A retomada analítica das evidências empíricas previamente obtidas evidenciou a recorrência de fragilidades como bibliotecas desatualizadas, credenciais embutidas, serviços inseguros e reutilização de componentes de terceiros sem rastreabilidade adequada. Embora tais vulnerabilidades possuam naturezas técnicas distintas, elas convergem para um mesmo problema institucional: a ampliação da superfície de ataque e a redução da capacidade de controle sobre ativos de rede que, em muitos casos, são essenciais ao funcionamento cotidiano das organizações.

Outro aspecto central da dissertação refere-se à relação entre segurança de firmware e auditabilidade. A análise desenvolvida sugere que a identificação de vulnerabilidades, por si só, não é suficiente para sustentar decisões institucionais consistentes em matéria de cibersegurança. Em ambientes organizacionais complexos, a possibilidade de reproduzir análises, verificar evidências, documentar procedimentos e interpretar achados à luz do contexto institucional fortalece a transparência, reduz assimetrias de informação e amplia a autonomia técnica das organizações diante da dependência de fornecedores e soluções fechadas.

Nesse sentido, a comparação entre firmwares proprietários e de código aberto permitiu observar diferenças relevantes sob a ótica da rastreabilidade e da inspeção independente. Ainda que não se sustente uma superioridade absoluta entre modelos proprietários e abertos, os resultados indicam que ecossistemas com maior transparência técnica e maior capacidade de auditoria tendem a oferecer melhores condições para processos institucionais de avaliação de risco, atualização, correção e governança operacional.

Como principal contribuição conceitual da dissertação, foi proposto o MARF-GC (Modelo para Auditoria Reproduzível de Firmware para Governança de Cibersegurança). O modelo foi concebido como uma estrutura analítica voltada à articulação entre auditoria técnica, reprodutibilidade analítica e governança institucional, organizando dimensões relacionadas à aquisição de firmware, extração, inspeção técnica, classificação de risco, integração com processos de governança e produção de evidências auditáveis. Mais do que um fluxo técnico de análise, o MARF-GC representa uma tentativa de aproximar a segurança de

firmware de práticas institucionais de gestão de riscos, priorização de ativos, definição de critérios de aquisição e fortalecimento da resiliência operacional.

Adicionalmente, a dissertação fortaleceu a relação entre o MARF-GC e referenciais consolidados de governança e segurança, como NIST CSF 2.0, NIST SP 800-53, NIST SP 800-193, CIS Controls, COBIT, ISO/IEC 27001, ETSI EN 303 645, IEC 62443, ISO/IEC 27402 e padrões de SBOM como SPDX e CycloneDX. Essa articulação permitiu posicionar o modelo proposto não como substituto de normas existentes, mas como uma camada analítica complementar voltada à operacionalização da governança de firmware em dispositivos de rede sem fio por meio de evidências técnicas auditáveis.

Além do modelo proposto, a dissertação sistematizou diretrizes institucionais para governança de firmware em dispositivos de rede sem fio, contemplando aspectos como inventário de dispositivos, políticas de atualização, critérios de aquisição, segmentação de rede, auditoria periódica e produção de evidências técnicas. Tais diretrizes não devem ser interpretadas como prescrições normativas universalmente aplicáveis, mas como subsídios analíticos derivados do escopo desta pesquisa, úteis para apoiar a reflexão e a formulação de práticas de governança em contextos institucionais semelhantes.

Do ponto de vista metodológico, o trabalho explorou o potencial de uma abordagem baseada na consolidação crítica de evidências previamente produzidas, reinterpretadas à luz da literatura recente e de referenciais de governança e engenharia de segurança. Essa estratégia permitiu produzir uma leitura institucionalmente orientada, mas sua adequação e efetividade ainda precisam ser avaliadas prospectivamente em aplicação real, com participação de equipes técnicas e gestores.

Como contribuição documental adicional, a reprodução direcionada confirmou as quatro imagens por hash, registrou o ambiente e as ferramentas, delimitou o escopo textual do Semgrep, individualizou 11 achados estáticos e organizou 31 candidatos a CVE do curl/libcurl 7.79.1 em uma matriz de 42 registros. Esse resultado fortalece a rastreabilidade da dissertação, mas não altera o caráter retrospectivo e ilustrativo da aplicação do modelo.

Outro resultado relevante da pesquisa foi o posicionamento do MARF-GC em relação a referenciais consolidados de governança e segurança da informação. Ao relacionar o modelo com NIST CSF 2.0, COBIT, CIS Controls, ISO/IEC 27001, ETSI EN 303 645, IEC 62443, ISO/IEC 27402, SBOM e PPSI, a dissertação evidenciou que sua proposta não busca substituir normas, frameworks ou políticas institucionais existentes. Sua contribuição consiste em oferecer uma camada analítica específica para firmware de dispositivos de rede sem fio e sistemas embarcados, capaz de transformar achados técnicos em evidências auditáveis, critérios de risco, indicadores e subsídios para decisão institucional.

O modelo também foi delimitado em relação às práticas operacionais. Análise estática, scanners, emulação, testes de intrusão, Red Team e Blue Team observam dimensões distintas e complementares. O MARF-GC organiza seus resultados, registra o grau de confiança e conecta validação técnica, controles defensivos, responsabilização e reauditoria.

Como limitações, reconhece-se que a pesquisa concentrou-se em análise estática e em resultados agregados de quatro firmwares, sem validação dinâmica, fuzzing, exploração controlada ou experimentação em hardware real. A reprodução direcionada recompôs hashes, ferramentas, comandos, regras e relatórios, individualizou os 11 achados estáticos e incorporou ao Apêndice A a relação integral dos 31 candidatos

a CVE. As saídas brutas, os hashes e os demais artefatos técnicos permanecem preservados no pacote de evidências. Não houve validação dinâmica de exposição ou explorabilidade, e os resultados não devem ser generalizados estatisticamente para toda a diversidade de dispositivos conectados e equipamentos de rede.

Por fim, conclui-se que a segurança de firmware em dispositivos de rede sem fio não deve ser tratada apenas como um problema técnico de atualização ou correção de vulnerabilidades, mas como componente estratégico da governança de cibersegurança em organizações intensivamente dependentes de conectividade. Em ambientes como universidades, centros de pesquisa e órgãos públicos, onde múltiplos dispositivos, redes e serviços coexistem de forma interdependente, a incorporação de práticas de auditoria reproduzível pode fortalecer a capacidade institucional de compreender riscos, produzir evidências, reduzir dependências opacas e apoiar decisões mais robustas sobre aquisição, manutenção e proteção de infraestruturas digitais.

Em síntese, a principal defesa desta dissertação é que a segurança de firmware deve ser incorporada à governança de cibersegurança como um objeto legítimo de avaliação institucional, e não apenas como um problema técnico restrito ao fabricante ou ao dispositivo isolado. Ao aproximar evidências técnicas, auditabilidade e gestão de riscos, o estudo busca contribuir para que organizações dependentes de dispositivos de rede sem fio ampliem sua capacidade de compreender vulnerabilidades, produzir evidências e fundamentar decisões relacionadas à atualização, substituição e proteção de ativos conectados.

5.1 CONTRIBUIÇÕES DA DISSERTAÇÃO

As contribuições desta dissertação concentram-se na articulação entre segurança de firmware, auditabilidade e governança de cibersegurança em ambientes institucionais dependentes de dispositivos de rede sem fio, organizadas a seguir em cinco dimensões complementares.

Contribuição científica. A dissertação sistematiza literatura recente sobre segurança de firmware, vulnerabilidades recorrentes em pontos de acesso sem fio e equipamentos de rede embarcados, cadeia de suprimentos de software, auditabilidade e reprodutibilidade, ao mesmo tempo em que reinterpreta criticamente evidências empíricas previamente produzidas pelo autor [1]. Essa reinterpretação, e não a repetição do experimento original, constitui o núcleo do avanço científico proposto, deslocando o eixo analítico da detecção técnica de vulnerabilidades para sua articulação com processos institucionais de decisão.

Contribuição técnica. O MARF-GC organiza, de forma reproduzível, um fluxo técnico composto por aquisição do firmware, extração e decomposição, auditoria técnica e produção de evidências auditáveis, oferecendo uma estrutura sistemática para conduzir e documentar auditorias de firmware em equipamentos de rede sem fio.

Contribuição institucional. A dissertação formula diretrizes institucionais para governança de firmware em dispositivos de rede sem fio, contemplando inventário de dispositivos, políticas de atualização, critérios de aquisição, segmentação de rede e auditoria periódica, apresentadas como subsídios analíticos, não como prescrições normativas universais, mas capazes de apoiar instituições como universidades e órgãos públicos na reflexão sobre práticas de gestão de riscos.

Contribuição para a governança. Ao conectar explicitamente as etapas do MARF-GC a referenciais consolidados como NIST CSF 2.0, COBIT e PPSI (Seção 4.3.2), a dissertação demonstra como evidências técnicas de firmware podem ser traduzidas em critérios de decisão institucional, responsabilização e priorização orçamentária, deslocando a auditoria de firmware de uma atividade puramente técnica para um insumo de governança.

Contribuição para a segurança. Por fim, ao evidenciar que vulnerabilidades em firmware podem comprometer a disponibilidade de serviços, a segmentação lógica de rede e a integridade de fluxos de comunicação, a dissertação reforça a necessidade de tratar o firmware como componente estratégico da postura de segurança institucional, e não apenas como responsabilidade exclusiva do fabricante do dispositivo.

5.2 TRABALHOS FUTUROS

Como desdobramento desta pesquisa, recomenda-se ampliar o escopo empírico para outras categorias de dispositivos conectados e sistemas embarcados, como câmeras IP, gateways, controladores industriais, sensores e equipamentos de automação institucional. Essa ampliação permitiria avaliar se os padrões de vulnerabilidade, auditabilidade e dependência de fornecedores observados nos dispositivos de rede sem fio também se manifestam em outros tipos de equipamentos conectados.

Outra possibilidade de continuidade consiste na incorporação de técnicas complementares de análise, como emulação, fuzzing, análise dinâmica e validação em hardware real. Essas abordagens poderiam complementar os achados obtidos por análise estática, permitindo observar comportamentos de execução, interações entre processos e vulnerabilidades dependentes do ambiente operacional.

Também se recomenda a aplicação prática do MARF-GC em um ambiente institucional real, com o objetivo de avaliar sua utilidade em processos de inventário, classificação de risco, priorização de atualizações, definição de critérios de aquisição e documentação de evidências técnicas. Tal aplicação permitiria transformar o modelo conceitual proposto em instrumento de apoio à gestão institucional de firmware em dispositivos de rede sem fio e sistemas embarcados.

A validação prospectiva deve incluir um novo firmware, participação de auditores, infraestrutura, Red Team, Blue Team e gestores, comparação entre decisões com e sem o modelo, medição de tempo e esforço, concordância entre avaliadores, verificação dos controles implantados e reauditoria após o tratamento. Também se recomenda complementar a trilha com as URLs e datas originais de obtenção dos firmwares e disponibilizar publicamente, quando permitido, o pacote de evidências regenerado.

Por fim, trabalhos futuros podem explorar o desenvolvimento de ferramentas ou procedimentos semi-automatizados para apoiar a organização de evidências, a rastreabilidade de componentes e a integração entre auditoria técnica de firmware e processos de governança de cibersegurança.

Do ponto de vista tecnológico, futuras investigações podem explorar a integração do MARF-GC com mecanismos de *Supply Chain Security* e *Trusted Firmware*, incluindo geração e verificação automatizada de SBOM, correlação automática com bases de CVE em tempo real, e mecanismos de *remote attestation*

para verificação contínua da integridade do firmware em produção. A aplicação de princípios de *Zero Trust* a ambientes institucionais com dispositivos conectados também constitui uma direção promissora, especialmente para reduzir a confiança implícita historicamente depositada em dispositivos de rede.

Do ponto de vista operacional, trabalhos futuros podem investigar a integração do MARF-GC a plataformas de SOC e SIEM já existentes em ambientes institucionais, permitindo que evidências de auditoria de firmware alimentem processos contínuos de monitoramento e resposta a incidentes. Adicionalmente, a aplicação de técnicas de inteligência artificial para automatizar etapas da auditoria, como classificação de risco assistida e priorização de mitigação, e a criação de gêmeos digitais (*digital twins*) de ambientes de rede institucionais para simulação de cenários de comprometimento representam extensões naturais do modelo proposto nesta dissertação.

A TRILHA DE REPRODUTIBILIDADE E REGISTRO DOS ACHADOS

Este apêndice distingue os resultados históricos do estudo de base daqueles obtidos na reprodução direcionada realizada em 23 de julho de 2026. A reprodução teve por finalidade recompor a trilha documental e não buscar a repetição numérica da campanha original.

A.1 RESULTADOS HISTÓRICOS E REPRODUÇÃO DIRECIONADA

Tabela 23: Separação entre os dois conjuntos de resultados

Conjunto	Resultado	Uso permitido
Estudo de base	13 ocorrências no TP-Link, 7 no D-Link, 11 no Intelbras e 3 no OpenWrt	Contagens agregadas históricas publicadas; não equivalem a vulnerabilidades exploráveis
Reprodução direcionada	31 candidatos a CVE do curl/libcurl 7.79.1 e 11 achados estáticos consolidados	Reposição da trilha documental, validação de presença e organização de evidências; não comprova exposição ou exploração

Fonte: Elaborado pelo autor (2026).

A.2 ESCOPO EFETIVAMENTE ANALISADO

Tabela 24: Arquivos processados e ocorrências brutas do Semgrep

Firmware	Arquivos textuais	Ocorrências brutas	Achados consolidados
D-Link DIR-842 R1 3.0.3	749	129	3
Intelbras RG1200 2.1.8	337	75	4
OpenWrt 22.03.5	841	92	0
TP-Link Archer C7 v5 20220715	1.238	1.220	4
Total	**3.165**	**1.516**	**11**

Fonte: Elaborado pelo autor (2026).

As ocorrências brutas representam correspondências textuais. A redução para 11 achados envolveu exclusão de traduções e interfaces, confirmação do arquivo original, eliminação de marcadores presentes apenas em binários e consolidação de repetições.

A.3 ACHADOS ESTÁTICOS INDIVIDUALIZADOS

Tabela 25: Achados estáticos mantidos após validação

ID	Firmware	Categoria	Evidência principal	Estado
CRYPTO-01	D-Link DIR-842	Chave privada embarcada	<etc/intercept_server.key>; RSA 1.024 bits; certificado correspondente; referência em <anweb>	Confirmado por inspeção
CRYPTO-02	D-Link DIR-842	Chave privada embarcada	<etc/server.key>; RSA 1.024 bits; certificado correspondente; referência em <anweb> e <libdhal.so>	Confirmado por inspeção
CRYPTO-03	D-Link DIR-842	Material criptográfico obsoleto	etc/tr069_key.pem; RSA 8.192 bits; certificado expirado em 08/04/2015; referência em <tr069>	Confirmado por inspeção
CRYPTO-04	Intelbras RG1200	Chave privada embarcada	<webroot_ro/pem/privkeySrv.pem>; RSA 2.048 bits; certificado correspondente; referência em <httpd>	Confirmado por inspeção
CRED-01	Intelbras RG1200	Credencial padrão	<webroot_ro/default.cfg:693>; <usb.ftp.pwd> contém literal não vazio	Presença confirmada
CRED-02	Intelbras RG1200	Credencial padrão	<webroot_ro/default.cfg:701>; <usb.samba.pwd> contém literal não vazio	Presença confirmada
CRED-03	Intelbras RG1200	Credencial padrão	<webroot_ro/default.cfg:706>; <usb.samba.guest.pwd> contém literal não vazio	Presença confirmada
LOG-01	TP-Link Archer C7	Credencial em log	<lib/netifd/proto/ncm.sh:30>; variável de senha encaminhada ao syslog	Código ativo confirmado
LOG-02	TP-Link Archer C7	Credencial em console	<lib/netifd/proto/pppshare.sh:33>; variável de senha encaminhada a </dev/console>	Código ativo confirmado
LOG-03	TP-Link Archer C7	Credencial em log	<usr/lib/modem/getisp.sh>; chamadas ativas de log e syslog com variável de senha	Código ativo confirmado
LOG-04	TP-Link Archer C7	Credencial em arquivo de log	<usr/sbin/checkpsw.sh>; registro de usuário e variável de senha em <LOG_FILE>	Código ativo confirmado

Para os quatro achados criptográficos, a correspondência entre chave privada e certificado foi verificada pela impressão digital SHA-256 da chave pública. A inicialização automática e a exposição em rede dos serviços não foram comprovadas.

A.4 CANDIDATOS PRIORITÁRIOS ASSOCIADOS AO CURL/LIBCURL 7.79.1

A reprodução correlacionou o componente a 31 registros. A Tabela 26 apresenta as dez ocorrências classificadas como críticas ou altas pelas fontes utilizadas pelo cve-bin-tool. A severidade pode divergir da classificação do projeto curl, da NVD ou de outros fornecedores.

Tabela 26: Triagem das dez CVEs prioritárias

CVE	**Severidade da fonte**	**Score**	**Estado de triagem na reprodução**
CVE-2022-32207	Crítica	9,8	Versão no intervalo afetado; operações locais de arquivo associadas à condição não foram evidenciadas nos scripts examinados
CVE-2023-38545	Crítica	9,8	Condicional; suporte SOCKS5 textual presente, porém uso de `socks5h` ou resolução remota por proxy não foi localizado
CVE-2022-22576	Alta	8,1	Condicional; OAuth2 e reutilização de conexões em protocolos de correio ou LDAP não foram evidenciados
CVE-2022-27775	Alta	7,5	Condição de reutilização de conexão IPv6 local não foi evidenciada
CVE-2022-27781	Alta	7,5	Não aplicável ao build observado: libcurl vinculado a OpenSSL, sem backend NSS
CVE-2022-27782	Alta	7,5	Condicional; reutilização de conexão após alteração de opções TLS/SSH não foi demonstrada
CVE-2022-42915	Alta	7,5	Condicional; proxy HTTP combinado a protocolo não HTTP não foi evidenciado
CVE-2022-42916	Alta	7,5	Condição técnica não identificada: suporte IDN e uso de HSTS não foram demonstrados
CVE-2022-43551	Alta	7,5	Condição técnica não identificada: suporte IDN não foi demonstrado no build
CVE-2024-2398	Alta	7,5	Condição técnica não identificada: dependência ou símbolos de HTTP/2 server push não foram localizados

A Tabela 27 individualiza todos os 31 identificadores correlacionados na reprodução. Para manter a tabela legível, os scores e vetores completos permanecem nos relatórios CSV/JSON preservados; a Tabela

26 transcreve os scores das dez ocorrências críticas ou altas priorizadas. Para os 14 identificadores não incluídos na saída resumida preservada, utiliza-se a indicação “média/baixa (não priorizada)”, sem atribuir uma classe individual que não foi transcrita. O relatório CSV original preservado no pacote permanece como registro autoritativo dos campos completos.

Tabela 27: Relação integral dos 31 candidatos a CVE associados ao curl/libcurl 7.79.1

ID	CVE	Severidade da fonte	Componente e evidência	Situação de validação
CVE-001	CVE-2022-22576	Alta	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Prioritária; aplicabilidade condicionada ao protocolo e à reutilização de conexão
CVE-002	CVE-2022-27774	Média	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-003	CVE-2022-27775	Alta	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Prioritária; condição de reutilização IPv6 não evidenciada
CVE-004	CVE-2022-27776	Média	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-005	CVE-2022-27781	Alta	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Não aplicável ao build observado: backend NSS ausente
CVE-006	CVE-2022-27782	Alta	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Prioritária; condição de reutilização TLS/SSH não demonstrada
CVE-007	CVE-2022-32206	Média	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-008	CVE-2022-32207	Crítica	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Prioritária; versão no intervalo, condição operacional não evidenciada
CVE-009	CVE-2022-32208	Média	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-010	CVE-2022-32221	Média	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-011	CVE-2022-35252	Baixa	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-012	CVE-2022-42915	Alta	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Prioritária; uso combinado de proxy e protocolo não evidenciado

ID	CVE	Severidade da fonte	Componente e evidência	Situação de validação
CVE-013	CVE-2022-42916	Alta	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Condição técnica não identificada: IDN/HSTS não demonstrados
CVE-014	CVE-2022-43551	Alta	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Condição técnica não identificada: suporte IDN não demonstrado
CVE-015	CVE-2022-43552	Média	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-016	CVE-2023-23914	Média/baixa	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-017	CVE-2023-23915	Média/baixa	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-018	CVE-2023-23916	Média/baixa	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-019	CVE-2023-27533	Média/baixa	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-020	CVE-2023-27534	Média/baixa	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-021	CVE-2023-27535	Média/baixa	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-022	CVE-2023-27536	Média/baixa	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-023	CVE-2023-27538	Média/baixa	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-024	CVE-2023-28319	Média/baixa	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; intervalo e compilação requerem revisão, sem aplicação presumida

ID	CVE	Severidade da fonte	Componente e evidência	Situação de validação
CVE-025	CVE-2023-28320	Média/baixa	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-026	CVE-2023-28321	Média/baixa	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-027	CVE-2023-28322	Média/baixa	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-028	CVE-2023-38545	Crítica	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Prioritária; uso de SOCKS5 com resolução remota não localizado
CVE-029	CVE-2023-38546	Média/baixa	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-030	CVE-2023-46218	Média/baixa	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Candidato; aplicabilidade específica não confirmada
CVE-031	CVE-2024-2398	Alta	curl/libcurl 7.79.1; presença confirmada em dois artefatos MIPS	Condição técnica não identificada: HTTP/2 server push não localizado

Os 31 registros representam correlações de versão para um único componente confirmado. A decisão institucional deve considerar funcionalidade compilada, uso efetivo, backports, exposição, suporte e controles compensatórios. A relação também integra o arquivo `matriz_unificada_achados.csv` incluído no projeto e no pacote de evidências.

A.5 FICHA INDIVIDUAL E DECISÃO INSTITUCIONAL

Cada registro do MARF-GC deve conter, no mínimo: equipamento e firmware; origem e integridade; componente; caminho; ferramenta e comando; identificador externo; evidência; estado de validação; confiança; contexto institucional; risco; tratamento; responsável; prazo; risco residual; e gatilho de reauditoria.

A Tabela 28 apresenta o preenchimento ilustrativo para o achado CRYPTO-03. Os níveis, responsáveis e prazos demonstram a operacionalização do modelo e não constituem registro de uma decisão administrativa já aprovada pela instituição.

Tabela 28: Ficha MARF-GC preenchida para o achado CRYPTO-03

Campo	**Registro ilustrativo**
Ativo e firmware	D-Link DIR-842 R1, firmware 3.0.3; imagem confirmada pelo SHA-256 registrado na Tabela 7.
Achado e evidência	CRYPTO-03: `etc/tr069_key.pem`, chave privada RSA de 8.192 bits legível sem senha; certificado `etc/tr069_cert.pem` correspondente e expirado em 08/04/2015; caminhos referenciados pelo executável `sbin/tr069`.
Ferramentas e validação	Semgrep como triagem, inspeção do arquivo, OpenSSL para correspondência da chave pública, `strings`/busca textual para referência no executável. Presença, validade criptográfica e integração ao componente confirmadas.
Confiança e limites	Confiança alta quanto à presença do material; inicialização automática, exposição em rede, reutilização entre unidades e explorabilidade não demonstradas.
Probabilidade ilustrativa	Média, condicionada à ativação do TR-069, alcance do serviço, reutilização da chave e controles de rede.
Impacto ilustrativo	Alto, caso o material seja compartilhado ou utilizado por serviço acessível, devido ao risco de comprometimento de autenticação, confiança criptográfica e gestão remota.
Risco institucional	Alto na matriz qualitativa do MARF-GC (probabilidade média e impacto alto), com necessidade de revisão após validação operacional.
Tratamento recomendado	Verificar ativação e exposição do TR-069; confirmar reutilização do par entre dispositivos; substituir chave e certificado; restringir ou desabilitar o serviço; segmentar o ativo; solicitar atualização ao fabricante ou planejar substituição quando não houver correção.

Campo	Registro ilustrativo
Atores e responsabilidade	Equipe de redes executa a verificação e a mitigação; gestão de segurança prioriza e acompanha; responsável pelo ativo e instância de governança aprovam tratamento, exceção ou substituição.
Prazo ilustrativo	Até 30 dias para verificação técnica e até 90 dias para tratamento ou decisão formal, ajustáveis à criticidade e à política institucional.
Risco residual	Médio até que ativação, exposição e substituição do material sejam verificadas; deve ser reclassificado com as novas evidências.
Gatilho de reauditoria	Nova versão de firmware, troca do equipamento ou do certificado, alteração da exposição, boletim do fabricante, término do prazo de tratamento ou ocorrência de incidente relacionado.

A.6 INTEGRIDADE DO PACOTE DE EVIDÊNCIAS

O pacote final contém ambiente, scripts, regras, relatórios do cve-bin-tool, resultados do Semgrep, evidências criptográficas, matriz de 42 registros e manifesto com 3.275 arquivos. O arquivo `Reproducao_Firmware_Evidencias_2026.tar.gz` foi validado como arquivo TAR/GZIP e recebeu o SHA-256:

```
24d8013ce625a66bb8bf3544312138cf3b5c148920c0f5f9ff6977f352b3f8ce
```

O hash permite verificar a integridade do pacote específico, mas não implica publicação aberta, revisão por terceiro ou validação dinâmica dos achados.

REFERÊNCIAS BIBLIOGRÁFICAS

1 SOUZA, L. d. P.; ALBUQUERQUE, R. d. O.; VILLALBA, L. J. G.; MENDONÇA, F. L. L.; NZE, G. D. A. Auditable security assessment of proprietary and open-source wi-fi router firmware: A reproducible approach for academic infrastructures. *Engineering Proceedings*, v. 123, n. 1, p. 34, 2026. Disponível em: <https://doi.org/10.3390/engproc2026123034>.

2 ATZORI, L.; IERA, A.; MORABITO, G. The internet of things: A survey. *Computer Networks*, Elsevier, v. 54, n. 15, p. 2787–2805, 2010.

3 ZANELLA, A.; BUI, N.; CASTELLANI, A.; VANGELISTA, L.; ZORZI, M. Internet of things for smart cities. *IEEE Internet of Things Journal*, v. 1, n. 1, p. 22–32, 2014. Disponível em: <https://doi.org/10.1109/JIOT.2014.2306328>.

4 COSTIN, A.; ZADDACH, J.; FRANCILLON, A.; BALZAROTTI, D. A large-scale analysis of the security of embedded firmwares. In: *23rd USENIX Security Symposium (USENIX Security 14)*. San Diego, CA: USENIX Association, 2014. p. 95–110. Disponível em: <https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/costin>.

5 ZHAO, B.; JI, S.; ZHANG, X.; TIAN, Y.; WANG, Q.; PU, Y.; LYU, C.; BEYAH, R. UVSCAN: Detecting Third-Party component usage violations in IoT firmware. In: *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, 2023. p. 3421–3438. ISBN 978-1-939133-37-3. Disponível em: <https://www.usenix.org/conference/usenixsecurity23/presentation/zhao-binbin>.

6 CHEN, Y.; MA, F.; ZHANG, Y.; HE, Y.; WANG, H.; LI, Q. Autofirm: Automatically identifying reused libraries inside iot firmware at large-scale. *arXiv preprint arXiv:2406.12947*, 2024. Disponível em: <https://arxiv.org/abs/2406.12947>.

7 BAKHSHI, T.; GHITA, B.; KUZMINYKH, I. A review of iot firmware vulnerabilities and auditing techniques. *Sensors*, v. 24, n. 708, 2024.

8 ZHOU, X.; WANG, P.; ZHOU, L.; XUN, P.; LU, K. A survey of the security analysis of embedded devices. *Sensors*, v. 23, n. 22, p. 9221, 2023. Disponível em: <https://doi.org/10.3390/s23229221>.

9 NASCIMENTO, L. *Ataques a dispositivos IoT com origem brasileira chegam a 11 milhões de tentativas de ataques*. 2025. Crypto ID. Disponível em: <https://cryptoid.com.br/iot-internet-das-coisas/kaspersky-revela-11-milhoes-de-tentativas-de-ataques-no-brasil/>. Acesso em: 23 jun. 2026.

10 HAQ, S. U.; SINGH, Y.; SHARMA, A.; GUPTA, R.; GUPTA, D. A survey on IoT & embedded device firmware security: Architecture, extraction techniques, and vulnerability analysis frameworks. *Discover Internet of Things*, v. 3, p. 17, 2023. Article 17. Disponível em: <https://doi.org/10.1007/s43926-023-00045-2>.

11 FENG, X.; ZHU, X.; HAN, Q.-L.; ZHOU, W.; WEN, S.; XIANG, Y. Detecting vulnerability on IoT device firmware: A survey. *IEEE/CAA Journal of Automatica Sinica*, v. 10, n. 1, p. 25–41, 2023. Disponível em: <https://doi.org/10.1109/JAS.2022.105860>.

12 ROMAN, R.; ZHOU, J.; LOPEZ, J. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, v. 57, n. 10, p. 2266–2279, 2013. Disponível em: <https://doi.org/10.1016/j.comnet.2012.12.018>.

13 WEBER, R. H. Internet of things–new security and privacy challenges. *Computer Law & Security Review*, v. 26, n. 1, p. 23–30, 2010. Disponível em: <https://doi.org/10.1016/j.clsr.2009.11.008>.

14 SICARI, S.; RIZZARDI, A.; GRIECO, L. A.; COEN-PORISINI, A. Security, privacy and trust in internet of things: The road ahead. *Computer Networks*, Elsevier, v. 76, p. 146–164, 2015.

15 ZIMMERMANN, M. et al. Small world with high risks: A study of security threats in the npm ecosystem. *USENIX Security Symposium*, 2020.

16 ABIE, H.; BALASINGHAM, I. Iot security and privacy: Challenges and solutions. *Wireless Personal Communications*, v. 96, n. 1, p. 399–413, 2017.

17 REDINI, N.; MACHIRY, A.; WANG, R.; SPENSKY, C.; CONTINELLA, A.; SHOSHITAISHVILI, Y.; KRUEGEL, C.; VIGNA, G. Karonte: Detecting insecure multi-binary interactions in embedded firmware. In: *2020 IEEE Symposium on Security and Privacy (SP)*. [S.l.: s.n.], 2020. p. 1544–1561.

18 GAO, Z.; ZHANG, C.; LIU, H.; SUN, W.; TANG, Z.; JIANG, L.; CHEN, J.; XIE, Y. Faster and better: Detecting vulnerabilities in linux-based IoT firmware with optimized reaching definition analysis. In: *Proceedings of the 2024 Network and Distributed System Security Symposium (NDSS)*. San Diego, CA: Internet Society, 2024. Disponível em: <https://doi.org/10.14722/ndss.2024.24346>.

19 ANTONAKAKIS, M.; APRIL, T.; BAILEY, M.; BERNHARD, M.; BURSZTEIN, E.; COCHRAN, J.; DURUMERIC, Z.; HALDERMAN, J. A.; INVERNIZZI, L.; KALLITSIS, M.; KUMAR, D.; LEVER, C.; MA, Z.; MASON, J.; MENSCHER, D.; SEAMAN, C.; SULLIVAN, N.; THOMAS, K.; ZHOU, Y. Understanding the mirai botnet. In: *26th USENIX Security Symposium (USENIX Security 17)*. USENIX Association, 2017. p. 1093–1110. Disponível em: <https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis>.

20 KOLIAS, C. et al. Ddos in the iot: Mirai and other botnets. *Computer*, IEEE, v. 50, n. 7, p. 80–84, 2017.

21 SCARFONE, K.; SOUPPAYA, M.; CODY, A.; OREBAUGH, A. *Technical Guide to Information Security Testing and Assessment*. [S.l.], 2008. Disponível em: <https://doi.org/10.6028/NIST.SP.800-115>.

22 The MITRE Corporation. *MITRE ATT&CK: Adversary Emulation and Red Teaming*. 2026. Acesso em: 22 jul. 2026. Disponível em: <https://attack.mitre.org/resources/get-started/adversary-emulation-and-red-teaming/>.

23 National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0*. [S.l.], 2024. Disponível em: <https://doi.org/10.6028/NIST.CSWP.29>.

24 Joint Task Force. *Security and Privacy Controls for Information Systems and Organizations*. [S.l.], 2020. Disponível em: <https://doi.org/10.6028/NIST.SP.800-53r5>.

25 MELAKU, H. M. A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy*, v. 3, n. 3, p. 327–350, 2023. Disponível em: <https://doi.org/10.3390/jcp3030017>.

26 SAVAS, S.; KARATAS, S. Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. *International Cybersecurity Law Review*, v. 3, p. 7–34, 2022. Disponível em: <https://doi.org/10.1365/s43439-021-00045-4>.

27 BIANCHI, I. S.; SOUSA, R. D. IT governance mechanisms in higher education. *Procedia Computer Science*, v. 100, p. 941–946, 2016. Disponível em: <https://doi.org/10.1016/j.procs.2016.09.253>.

28 KHOUJA, M.; RODRIGUEZ, I. B.; HALIMA, Y. B.; MOALLA, S. IT governance in higher education institutions: A systematic literature review. *International Journal of Human Capital and Information Technology Professionals*, v. 9, n. 2, p. 52–67, 2018. Disponível em: <https://doi.org/10.4018/IJHCITP.2018040104>.

29 Center for Internet Security. *CIS Critical Security Controls Version 8.1*. 2024. Acesso em: 30 jun. 2026. Disponível em: <https://www.cisecurity.org/controls/v8>.

30 ISACA. *COBIT 2019 Framework: Governance and Management Objectives*. [S.l.], 2019. Disponível em: <https://www.isaca.org/resources/cobit>.

31 REGENSCHEID, A.; BUTTERFIELD, M.; MCBRIDE, C.; FELDMAN, D. *Platform Firmware Resiliency Guidelines*. [S.l.], 2018. Disponível em: <https://doi.org/10.6028/NIST.SP.800-193>.

32 International Organization for Standardization. *ISO/IEC 27001:2022 Information Security Management Systems*. 2022. Disponível em: <https://www.iso.org/standard/27001>.

33 European Telecommunications Standards Institute. *ETSI EN 303 645: Cyber Security for Consumer Internet of Things*. 2024. V3.1.3. Disponível em: <https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf>.

34 ISA Global Cybersecurity Alliance. *ISA/IEC 62443 Series of Standards*. 2024. Acesso em: 30 jun. 2026. Disponível em: <https://isagca.org/isa-iec-62443-standards>.

35 International Organization for Standardization. *ISO/IEC 27402:2023 Cybersecurity – IoT Security and Privacy – Device Baseline Requirements*. 2023. Disponível em: <https://www.iso.org/standard/80136.html>.

36 Linux Foundation. *System Package Data Exchange (SPDX): ISO/IEC 5962:2021*. 2021. Disponível em: <https://spdx.dev/>.

37 OWASP Foundation. *CycloneDX Bill of Materials Standard*. 2024. Disponível em: <https://cyclonedx.org/>.

38 European Union. *Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*. 2024. Disponível em: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>.

39 Secretaria de Governo Digital. *PPSI 2.0 – Programa de Privacidade e Segurança da Informação*. 2026. Portal Gov.br. Acesso em: 30 jun. 2026. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0>.

40 Secretaria de Governo Digital. *Guia do Framework de Privacidade e Segurança da Informação do PPSI 2.0*. 2026. Portal Gov.br. Versão 1.2. Acesso em: 30 jun. 2026. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/arquivos/guiafwppsi2-0-v1-2-30012026.pdf>.

41 Ministério da Gestão e da Inovação em Serviços Públicos. *Instrução Normativa SGD/MGI n. 4, de 14 de janeiro de 2026*. 2026. Portal Gov.br. Dispõe sobre o ciclo de implementação de 2026 do framework do PPSI. Acesso em: 30 jun. 2026. Disponível em: <https://www.gov.br/gestao/pt-br/acesso-a-informacao/institucional/atos-normativos/2026/2026-instrucao-normativa>.

42 European Union. *Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements*. 2024. Disponível em: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>.

43 ROSS, R.; MCEVILLEY, M.; OREN, J. C. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. [S.l.], 2022. Disponível em: <https://doi.org/10.6028/NIST.SP.800-160v1r1>.

44 LEE, I. Internet of things (iot) cybersecurity: Literature review and iot cyber risk management. *Future Internet*, v. 12, n. 9, p. 157, 2020.

45 Joint Task Force Transformation Initiative. *Guide for Conducting Risk Assessments*. [S.l.], 2012. Disponível em: <https://doi.org/10.6028/NIST.SP.800-30r1>.

46 LIMA, E. de O. *Gestão de Riscos Cibernéticos no Setor Elétrico Brasileiro: uma Proposta sob a Ótica da Rotina Operacional do Operador Nacional do Sistema Elétrico*. Dissertação (Dissertação de Mestrado Profissional em Engenharia Elétrica) — Universidade de Brasília, Brasília, DF, 2022.

47 FERREIRA, L. V. A. *O Papel da Auditoria Interna na Gestão de Riscos Cibernéticos em Instituições Financeiras Brasileiras: Estudo sob a Perspectiva das Três Linhas*. Dissertação (Dissertação de Mestrado Profissional em Engenharia Elétrica) — Universidade de Brasília, Brasília, DF, 2024.

48 CHEN, D. D.; EGELE, M.; WOO, M.; BRUMLEY, D. Towards automated dynamic analysis for linux-based embedded firmware. In: *Proceedings of the 2016 Network and Distributed System Security Symposium (NDSS)*. San Diego, CA: Internet Society, 2016. Disponível em: <https://doi.org/10.14722/ndss.2016.23415>.

49 Forum of Incident Response and Security Teams. *Common Vulnerability Scoring System Version 4.0: Specification Document*. 2023. Acesso em: 22 jul. 2026. Disponível em: <https://www.first.org/cvss/v4.0/specification-document>.

50 Cybersecurity and Infrastructure Security Agency. *Known Exploited Vulnerabilities Catalog*. 2026. Acesso em: 22 jul. 2026. Disponível em: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>.