FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Patricia Rodrigues da Silva

Proposta de Processo para a Gestão de Vulnerabilidades Técnicas

Americana, SP

2025

FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Patricia Rodrigues da Silva

Proposta de Processo para a Gestão de Vulnerabilidades Técnicas

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação sob a orientação Prof. Me. Edson Roberto Gaseta.

Área de concentração: Segurança da Informação

Americana, SP

2025

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi- CEETEPS Dados Internacionais de Catalogação-na-fonte

SILVA, Patricia Rodrigues

Proposta de processo para a gestão de vulnerabilidades técnicas. / Patricia Rodrigues Silva – Americana, 2025.

41f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Edson Roberto Gaseta

1. Redes de computadores 2. Segurança em sistemas de informação 3. Sistemas de informação – governança. I. SILVA, Patricia Rodrigues II. GASETA, Edson Roberto III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681519
681.518.5
681.518.3

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Patrícia Rodrigues da Silva

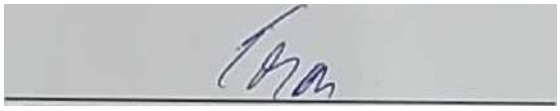
Proposta de processo para a gestão de vulnerabilidades técnicas

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza - FATEC Faculdade de Tecnologia de Americana Ministro Ralph Biasi.

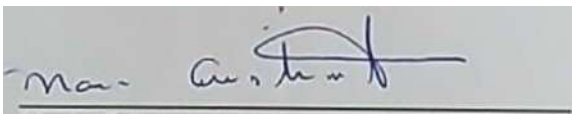
Área de concentração: Segurança da Informação

Americana, 26 de junho de 2025.

Banca Examinadora:



Edson Roberto Gaseta
Mestre
Fatec Americana "Ministro Ralph Biasi"



Maria Cristina Aranda
Doutora
Fatec Americana "Ministro Ralph Biasi"

Thiago da Silva Vie• a
Mestre
Fatec Americana "Ministro Ralph Biasi"

Dedico esse trabalho às mulheres que vieram antes de mim, a minha ancestralidade.

Agradeço ao professores que acreditaram no meu potencial e a minha família, que apoiou a minha decisão de cursar uma graduação após completar 50 anos de idade.

RESUMO

O aumento dos ataques cibernéticos tem gerado a necessidade de desenvolver aplicações e sistemas eficazes para monitoramento e prevenção de ameaças à segurança da informação. Este trabalho tem como objetivo estruturar o gerenciamento de vulnerabilidades em ativos críticos da organização, com foco na identificação de fragilidades técnicas e na implantação de um processo contínuo de mitigação. A pesquisa também destaca a importância de reduzir o ruído no julgamento, que pode interferir diretamente na tomada de decisão humana, prejudicando a eficácia das ações de segurança. O trabalho propõe a criação de um processo de monitoramento das vulnerabilidades, que seja de fácil implementação e de baixo custo, alinhada aos procedimentos de segurança da informação. A metodologia utilizada é teórico-prática e o objetivo central é demonstrar como o gerenciamento de vulnerabilidades pode ser estruturado para melhorar a segurança dos ativos organizacionais e contribuir para a proteção do ambiente corporativo.

Palavras-chave: vulnerabilidades técnicas; cibersegurança; detecção de vulnerabilidade técnica; ruído no julgamento.

ABSTRACT

The increase in cyberattacks has created the need to develop effective frameworks and systems for monitoring and preventing threats to information security. This study aims to structure vulnerability management in critical organizational assets, focusing on the identification of technical weaknesses and the implementation of a continuous mitigation process. The research also highlights the importance of reducing noise in judgment, which can directly affect human decision-making and compromise the effectiveness of security actions. This work proposes the creation of a vulnerability monitoring process that is easy to implement and low-cost, aligned with information security procedures. The methodology used is theory-based with practical application and the main objective is to demonstrate how vulnerability management can be structured to improve the security of organizational assets and contribute to the protection of the corporate environment.

Keywords: *technical vulnerabilities; cybersecurity; technical vulnerability detection; judgment noise.*

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE QUADROS

SUMÁRIO

INTRODUÇÃO

O aumento de ataques cibernéticos tem provocado constante desenvolvimento e oferta de aplicações e sistemas de monitoramento da informação em rede e de como detectar possíveis ameaças à sua segurança.

Torna-se imprescindível que a organização consiga detectar e prevenir tais ameaças, para manter seus ativos (informação, propriedade intelectual, equipamentos, softwares) protegidos e atingir seus objetivos de negócios. É necessário investir tanto na identificação de possíveis fragilidades técnicas e de processo, quanto na implantação e manutenção dessa análise.

É importante ressaltar que uma das fragilidades de processo, pode ser o ruído no julgamento, pois interfere diretamente na tomada de decisão humana.

A busca por um procedimento que possa atender a essa necessidade e seja de fácil implementação e utilização se mostra essencial uma vez que o volume de dados tratados tem aumentado exponencialmente.

O objetivo do trabalho é demonstrar a estruturação do gerenciamento de vulnerabilidades, de importantes ativos da organização.

Os objetivos específicos, com foco na segurança da informação, são: orientar a abrangência do escopo; estudar as fases de identificação de vulnerabilidades técnicas; analisar as recomendações de ações para os resultados encontrados; criar um processo para o monitoramento contínuo das vulnerabilidades.

A hipótese é mostrar atividades para prevenir incidentes de segurança da informação por meio da exploração de vulnerabilidades, através da rápida mitigação de fragilidades nos ativos da organização com um processo de simples implantação e baixo custo, para atendimento à política vigente.

O percurso metodológico deste trabalho é uma pesquisa teórico-prático.

O trabalho está organizado em três capítulos, sendo o capítulo I será a fundamentação teórica, capítulo II é o percurso metodológico e o capítulo III conterá os resultados, análise e discussão dos dados.

1 FUNDAMENTAÇÃO TEÓRICA

1.1 Conceito Segurança da Informação

A segurança da informação (S.I.) trata da proteção de um conjunto de informações, com o objetivo de preservar o valor que possuem para pessoas ou organizações. Seus principais aspectos são definidos pela tríade Confidencialidade, Integridade e Disponibilidade, garantindo que nenhuma dessas propriedades seja violada (Brasil, 2022):

- Confidencialidade: garante que somente pessoas autorizadas possam acessar as informações;
- Integridade: assegura que a informação é correta, íntegra, sem alterações ou fraudes; e
- Disponibilidade: assegura que a informação esteja acessível sempre que necessária.

Esses três princípios são fundamentais e atuam de forma conjunta para garantir a segurança da informação. A confidencialidade garante que o acesso e uso de uma informação sejam restritos somente às pessoas a quem ela é destinada; a integridade assegura que essas informações se mantenham consistentes e imunes a alterações não autorizadas; e a disponibilidade assegura que as informações estejam sempre acessíveis às pessoas autorizadas quando necessário (Brasil, 2022).

A proteção dessas informações pode ser quanto a vários tipos de ameaças, de modo a alinhar-se com os objetivos de negócio da organização, manter a continuidade de suas atividades, minimizar os riscos ao retorno dos investimentos, bem como às oportunidades e manter a sua reputação de mercado (Garcia, 2021).

Ela pode compreender a adoção de adequações técnicas, organizacionais e controles, boas práticas e mecanismos de melhoria contínua para os processos de negócios, com o objetivo de evitar perdas para a organização, e utiliza-se de outros princípios tão importantes quanto os citados anteriormente, que são: a autenticidade, a responsabilidade, o não repúdio e a confiabilidade (Brasil, 2022).

Em ambientes corporativos, a implementação de zonas de segurança permite que sistemas críticos convivam de forma controlada com segmentos inseguros. A segurança da informação é essencial para proteger dados empresariais e pessoais

contra ameaças como furto, destruição ou modificação, abrangendo procedimentos, regras de acesso e métodos para reagir a vulnerabilidades, com o suporte de ferramentas como antivírus e *firewalls* (Garcia, 2021).

Além disso, a segurança da informação viabiliza o uso confiável de recursos essenciais às atividades estratégicas, táticas e operacionais de uma organização, proporcionando proteção contra o mau uso intencional ou não de informações, seja por pessoas internas ou externas (Rezende; Abreu, 2019).

A inclusão de ferramentas de detecção de vulnerabilidades técnicas é um desses controles necessários para garantir a segurança da informação; com um ciclo contínuo de detecção e correção de vulnerabilidades, essencial para proteger dados e ativos digitais contra acessos não autorizados e outros incidentes de segurança (REZENDE; ABREU, 2019).

A norma ABNT NBR IS0/IEC 27002:2022 (ABNT, 2022), relaciona a gestão das vulnerabilidades técnicas com a segurança da informação, especificamente nos controles listados no Quadro 1.

Quadro 1 - Controles da ISO 27002/2022 relacionados às vulnerabilidades técnicas

Controle	Grupo de controle	Descrição
5.24	Organizacional	Planejamento e preparação da gestão de incidentes de segurança da informação
5.26	Organizacional	Resposta à Incidentes da Segurança da Informação
5.27	Organizacional	Aprendizados com incidentes da Segurança da Informação
8.8	Tecnológico	Gestão de Vulnerabilidades Técnicas

Fonte: ABNT NBR IS0/IEC 27002:2022

1.2 Vulnerabilidades técnicas

Vulnerabilidade é a característica de fraqueza de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças para causar danos. Essa fraqueza pode estar relacionada à configuração de uma senha fraca, à falta de adoção de proteções de rede, como um firewall, ou até a um controle tecnicamente instalado, porém mal gerenciado (Fernandes, 2021).

Essas fragilidades podem estar presentes em políticas, processos, equipamentos e pessoas, necessitando de um agente ou de uma condição desfavorável para resultar em incidentes (Fernandes, 2021).

Atualmente, as vulnerabilidades de Tecnologia da Informação (TI) são catalogadas e rastreadas sob a sigla inglesa CVE (Common Vulnerabilities and Exposures), em uma lista pública mantida pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST), denominada Banco de Dados Nacional de Vulnerabilidades (NVD) ((UNITED STATES, [s.d.]).

Ao serem registradas nesse banco de dados, as vulnerabilidades são analisadas qualitativamente quanto à sua severidade por meio do sistema denominado CVSS (Common Vulnerability Scoring System). Para essa pontuação, são considerados vários fatores que influenciam o impacto da exploração da vulnerabilidade, como a facilidade de exploração, os ambientes nos quais pode ocorrer e se são específicas de determinadas versões de *softwares*, sendo eliminadas com atualizações posteriores (NIAC, 2004).

As métricas da versão atual desse sistema de pontuação são: base, temporal e ambiental; seu resultado é utilizado para priorizar as atividades de remediação, com a aplicação de medidas e controles que estruturam a gestão das vulnerabilidades (NIAC, 2004).

1.3 Controles CIS (CIS Controls)

Os Controles CIS (CIS Controls) são um conjunto de salvaguardas práticas e priorizadas, projetadas para ajudar organizações a proteger seus sistemas e dados contra ameaças cibernéticas. Desenvolvidos inicialmente como os SANS Top 20, esses controles foram posteriormente assumidos e aprimorados pelo Center for Internet Security (CIS), que passou a mantê-los como parte de sua missão de promover boas práticas de segurança da informação em nível global (CENTER FOR INTERNET SECURITY, 2024).

O *framework* dos *CIS Controls* foi concebido a partir da colaboração de especialistas de segurança cibernética de diversas áreas e setores. Essa abordagem colaborativa garante que os controles sejam realistas, aplicáveis a diferentes contextos organizacionais e fundamentados na experiência prática de combate às ameaças reais do ambiente digital (CENTER FOR INTERNET SECURITY, 2024).

Esses conjunto está organizado em 18 controles críticos, que abrangem desde a identificação de ativos e gestão de vulnerabilidades até a proteção contra *malware* e resposta a incidentes. Esses controles seguem uma ordem de prioridade, permitindo que organizações iniciem sua jornada de segurança implementando primeiramente os controles mais essenciais.

Os controles são divididos em três grupos de implementação (*Implementation Groups - IGs*), que representam perfis diferentes de maturidade e recursos de segurança cibernética das organizações:

IG1 (Implementation Group 1): Focado em pequenas empresas ou organizações com recursos limitados. Inclui os controles mais básicos e fundamentais, que oferecem proteção contra ameaças comuns.

IG2 (Implementation Group 2): Indicado para organizações com departamentos de TI internos e maior complexidade operacional. Engloba práticas mais avançadas de controle e monitoramento.

IG3 (Implementation Group 3): Voltado a grandes organizações, com alta exposição a riscos e ameaças sofisticadas. Abrange controles detalhados e recursos técnicos robustos para defesa em profundidade (CENTER FOR INTERNET SECURITY, 2024).

Essa estrutura escalonada permite uma implementação progressiva e personalizada, baseada em avaliações de risco e na capacidade de investimento da organização. Além disso, os CIS Controls são compatíveis com outras estruturas

regulatórias, como o NIST Cybersecurity Framework, ISO/IEC 27001 e COBIT, o que facilita sua adoção como parte de programas integrados de conformidade e governança.

Os Controles CIS têm como principal objetivo reduzir a superfície de ataque, ajudando as organizações a protegerem seus ativos digitais com ações práticas e mensuráveis. A comunidade de segurança contribui ativamente para a evolução do *framework*, garantindo que ele permaneça atualizado frente às mudanças no cenário de ameaças (CENTER FOR INTERNET SECURITY, 2024).

Para apoiar sua implementação, o CIS oferece recursos como o CIS Controls Assessment Tool (CIS-CAT), uma ferramenta gratuita que permite avaliar o grau de conformidade da organização com os controles, priorizar ações corretivas e acompanhar o progresso da maturidade em segurança (CENTER FOR INTERNET SECURITY, 2024).

Além de oferecer uma abordagem ampla para a segurança cibernética, os CIS Controls também podem ser aplicados diretamente na detecção e gestão de vulnerabilidades técnicas, sendo especialmente úteis na identificação de falhas técnicas em sistemas, *softwares* e dispositivos conectados. Alguns dos controles priorizam ações como o inventário de ativos, análise contínua de segurança, correção de vulnerabilidades e monitoramento de anomalias. Esses controles são fundamentais para a prevenção de ataques exploratórios, pois ajudam as organizações a localizar pontos frágeis em sua infraestrutura antes que possam ser explorados por agentes maliciosos.

No Quadro 2, são apresentados alguns dos controles CIS mais relevantes quando se trata de detecção e resposta a vulnerabilidades:

Quadro 2 – Controles CIS relacionados à detecção de vulnerabilidades

Controle	**Grupo de Controle (IG)**	**Descrição**
CIS Control 1	IG1	Inventário e controle de ativos corporativos – Identifica e gerencia todos os ativos conectados à rede, etapa essencial para a detecção de vulnerabilidades.
CIS Control 2	IG1	Inventário e controle de ativos de software – Controla os softwares instalados para evitar o uso de versões desatualizadas ou não autorizadas.

Controle	Grupo de Controle (IG)	Descrição
CIS Control 3	IG1	Proteção de dados – Visa proteger dados sensíveis e críticos, abordando também aspectos de segurança que contribuem na identificação de falhas.
CIS Control 7	IG1	Gerenciamento de vulnerabilidades de segurança – Envolve a identificação, avaliação, priorização e correção de vulnerabilidades conhecidas.
CIS Control 8	IG2	Gerenciamento de logs de auditoria – Realiza a coleta e análise de registros de eventos para identificar comportamentos suspeitos ou anômalos.
CIS Control 17	IG2	Gerenciamento de resposta a incidentes – Estabelece processos para detectar e responder rapidamente a incidentes causados por vulnerabilidades exploradas.

Fonte: CIS CONTROLS – Center for Inernet Security

1.4 Ruído no julgamento

O ruído pode ser definido como variações imprevisíveis e indesejadas em julgamentos humanos que ocorrem mesmo quando as pessoas deveriam tomar decisões semelhantes sob as mesmas circunstâncias. Diferente do viés, que é um erro sistemático, o ruído é um erro aleatório (Kahneman; Sibony; Sunstein, 2021).

Podem ser identificados três tipos principais de ruído:

Ruído de nível – Diferença sistemática nas decisões entre indivíduos em um grupo. Exemplo: dois juízes dão penas muito diferentes para crimes semelhantes.

Ruído de padrão – Diferenças nas decisões do mesmo indivíduo dependendo do contexto. Exemplo: um médico pode diagnosticar a mesma condição de forma diferente dependendo do horário do dia.

Ruído ocasional – Variação imprevisível na decisão causada por fatores momentâneos, como humor, cansaço ou situações de pressão externa.

O ruído afeta decisões em todas as áreas, como justiça, medicina, contratações, seguros e tecnologia da informação, tornando os sistemas menos confiáveis e eficientes. Ao reduzir o ruído, as organizações podem melhorar a qualidade das decisões.

A criação de um processo auxilia na redução do ruído, utilizando uma estrutura baseada em critérios objetivos, além do uso de ferramentas como algoritmos e estatísticas, eliminando interferências humanas desnecessárias e trazendo respostas rápidas e direcionadas (Kahneman; Sibony; Sunstein, 2021).

Em seu clássico artigo ‘A Mathematical Theory of Communication’, Claude Shannon desenvolve o modelo matemático da comunicação, afirmando que o ruído introduz incertezas em quaisquer dos componentes básicos de um sistema de comunicação. Além disso, ele introduz o conceito de capacidade do canal, definido como a taxa máxima com a qual a informação pode ser transmitida de forma confiável, mesmo na presença de ruído (Shannon, 1948).

1.5 Ferramenta de Varredura

O objetivo da ferramenta é fazer a avaliação de vulnerabilidade, que é um processo que define, identifica e classifica falhas de segurança em um computador, rede ou infraestrutura de comunicação (Martins; Guimarães, 2021).

A ferramenta de varredura consiste em quatro módulos principais:

- interface do usuário;
- mecanismo de verificação;
- banco de dados de vulnerabilidades; e
- módulo de relatório.

Existem muitas ferramentas que realizam varreduras de vulnerabilidade (também conhecidas como *scanners*), algumas das quais são gratuitas e de código aberto (ou têm uma versão gratuita com limitações), enquanto outras podem ser muito caras.

Para ter eficácia na utilização da ferramenta, é fundamental que ela ofereça a capacidade de criar testes e relatórios personalizados, combinando os resultados com métricas e fórmulas próprias para gerar um resumo da segurança total da rede. Alternativamente, o relatório deve ser exportável de forma que os dados possam ser recuperados por um programa externo para gerar sinalizadores de segurança gerais e modelos estatísticos propostos externamente.

Essa análise de vulnerabilidade pode estimar a eficácia das contramedidas propostas e avaliar sua eficácia real depois de implementadas. Os resultados da atividade de avaliação de vulnerabilidade podem ser usados, por exemplo, para determinar o nível de maturidade de segurança de um *site* (Martins; Guimarães, 2021).

1.6 Nessus – Descoberta de vulnerabilidades

O Nessus é uma ferramenta de escaneamento de vulnerabilidades técnicas amplamente utilizada para identificar e avaliar falhas de segurança em sistemas operacionais, aplicativos e redes. De acordo com a Tenable Network Security (2024), empresa responsável pelo desenvolvimento da ferramenta, o Nessus permite detectar vulnerabilidades, configurações incorretas e outros riscos exploráveis por atacantes.

Entre suas principais funcionalidades está a varredura automática, que realiza verificações contínuas para identificar ameaças com rapidez e precisão (INOVATECHY, 2023). Além disso, a mesma empresa informa que a ferramenta realiza uma avaliação de risco, atribuindo pontuações com base na gravidade das falhas, o que permite priorizar as correções mais críticas.

Outra característica importante é a geração de relatórios personalizáveis, que facilitam a análise técnica e a comunicação dos riscos à equipe responsável (TENABLE NETWORK SECURITY, 2024).

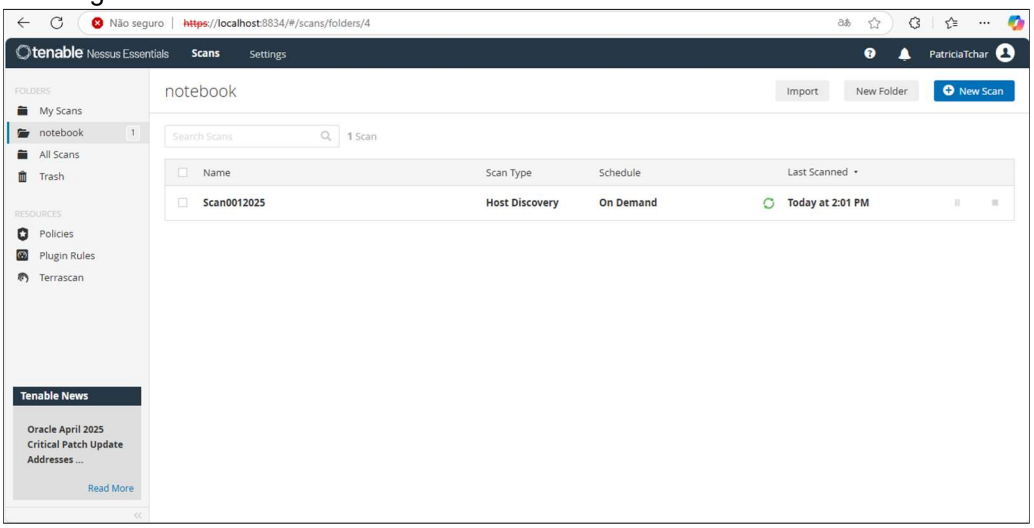
O Nessus está disponível em diferentes versões:

- Essentials: versão gratuita, voltada a estudantes, educadores e iniciantes, com suporte para até 16 endereços IP;
- Professional: voltada para consultores, analistas e equipes de segurança corporativas, com recursos de auditoria de conformidade e varreduras ilimitadas; e
- Expert: além das funcionalidades da versão Professional, oferece verificação de aplicações *web*, nuvem e infraestrutura como código (IaC).

Essa ferramenta é amplamente reconhecida por sua alta precisão, com uma das menores taxas de falso-positivos do setor, segundo informações da própria Tenable Network Security (2024).

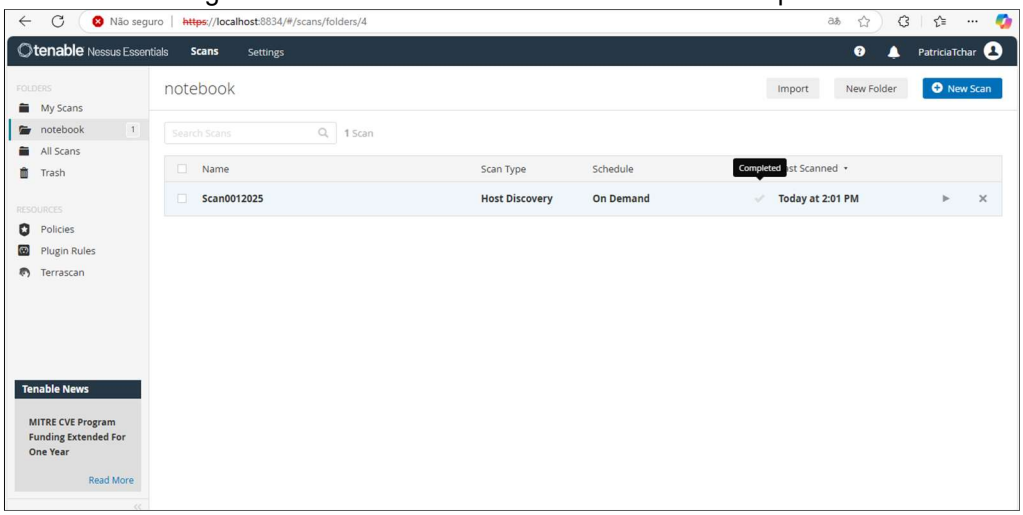
A Figura 1, Figura 2 e Figura 3 mostram um escaneamento de ativo, desde a descoberta em andamento e o resultado em tela :

Figura 1 - Escaneamento de vulnerabilidades em andamento na ferramenta



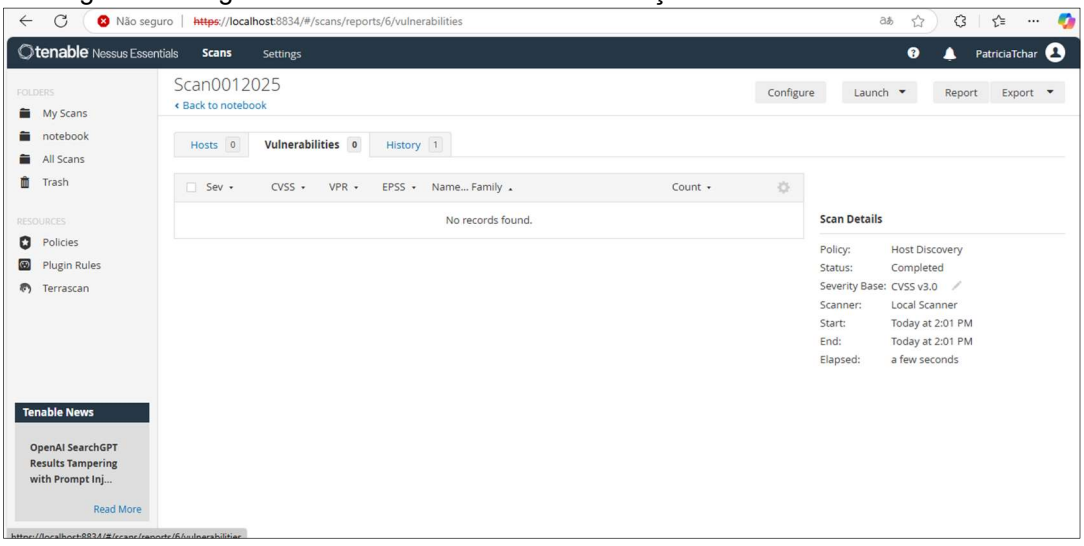
Fonte: Adaptado da ferramenta Nessus

Figura 2 - Escaneamento de vulnerabilidades completo.



Fonte: Adaptado da ferramenta Nessus

Figura 3 - Diagnóstico identificado com a identificação dos critérios estabelecidos.



Fonte: Adaptado da ferramenta Nessus

1.7 NMAP – Descoberta de vulnerabilidades

O Nmap (*Network Mapper*) é uma das ferramentas mais utilizadas em auditorias de redes e em atividades de teste de intrusão. Sua função primordial está na detecção de ativos conectados a uma rede, identificação de serviços ativos, descoberta de portas abertas e análise de possíveis vulnerabilidades técnicas. Por se tratar de uma ferramenta de código aberto, o Nmap tornou-se acessível e altamente customizável, sendo considerado fundamental no processo de avaliação da superfície de ataque de uma infraestrutura de TI (Lyon, 2022).

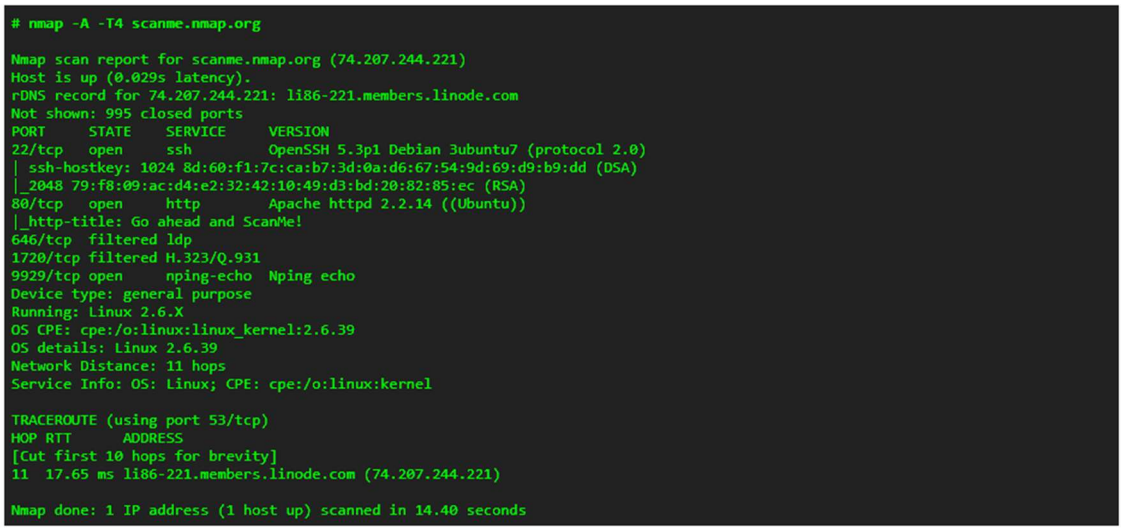
Desenvolvido por Gordon Lyon, o Nmap emprega técnicas de varredura que analisam pacotes TCP/IP para mapear a topologia da rede. Entre os tipos de varredura disponíveis, destaca-se a técnica *SYN scan* – também chamada de *half-open scan* – que permite realizar a sondagem de portas de forma furtiva, reduzindo a probabilidade de detecção por sistemas de defesa (Skoudis; Zelter, 2018). Essas funcionalidades tornam o Nmap altamente eficaz na identificação de potenciais brechas de segurança, especialmente quando utilizado em conjunto com outras ferramentas de análise.

Uma das grandes vantagens da ferramenta é o *Nmap Scripting Engine* (NSE), um mecanismo interno que possibilita a execução de *scripts* para automatizar a detecção de vulnerabilidades específicas. Por meio de scripts pré-configurados ou personalizados, é possível realizar análises mais profundas e identificar comportamentos suspeitos, vulnerabilidades conhecidas, serviços mal configurados, entre outras informações relevantes à segurança (Lyon, 2022).

No contexto do gerenciamento de vulnerabilidades técnicas, o Nmap se posiciona como ferramenta essencial para a etapa de identificação e mapeamento de ativos e serviços. Sua aplicação contribui para a criação de inventários precisos da rede, para a análise do cumprimento de políticas de segurança e para a realização de varreduras preventivas. Em ambientes corporativos, quando utilizado de forma ética e com a devida autorização, o Nmap apoia diretamente o aumento da resiliência cibernética e o fortalecimento da postura de segurança da organização (Stewart, 2020).

A figura 4 mostra a tela de interface (linha de comando) do escâner Nmap:

Figura 4 – Nmap pronto para uso através da linha de comando.



Fonte: Adaptado da ferramenta NMAP

1.8 OpenVAs – Descoberta de vulnerabilidades

O OpenVAS (*Open Vulnerability Assessment System*) é uma ferramenta de código aberto projetada para realizar varreduras em sistemas e redes em busca de vulnerabilidades de segurança. Originalmente um derivado do Nessus, o OpenVAS foi desenvolvido para fornecer uma alternativa gratuita e acessível a ferramentas de segurança comerciais. A manutenção e o desenvolvimento do OpenVAS são conduzidos pela Greenbone Networks, uma empresa especializada em soluções de segurança cibernética (Greenbone Networks, 2024).

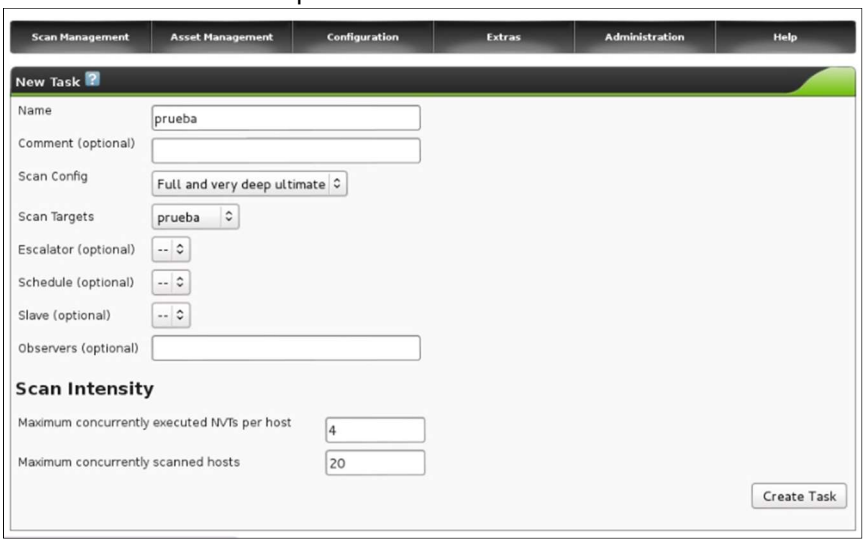
O OpenVAS realiza varreduras detalhadas em sistemas e redes para identificar vulnerabilidades conhecidas, utilizando uma base de dados chamada *Network Vulnerability Tests* (NVTs), que é constantemente atualizada. A ferramenta é capaz de analisar diversos protocolos e serviços, como HTTP, FTP, SMTP, SNMP e muitos outros, em busca de falhas de segurança. Após a execução da varredura, o OpenVAS gera relatórios detalhados que listam as vulnerabilidades encontradas, oferecendo recomendações para mitigação ou correção (Mendonza, 2019).

O OpenVAS é composto por três componentes principais: um escâner, responsável pela execução das varreduras de vulnerabilidades nos sistemas e redes; um painel de gerenciamento, que oferece a configuração das varreduras, e armazena os resultados; e uma interface *web* utilizada para visualizar os resultados das varreduras (Greenbone Networks, 2024).

Essa ferramenta é amplamente utilizada em diversos contextos de segurança cibernética, incluindo: auditoria de segurança, em que administradores de TI realizam verificações regulares em redes e sistemas; testes de penetração, com o objetivo de avaliar a segurança simulando ataques reais; e avaliações de riscos, em que as vulnerabilidades identificadas ajudam a priorizar ações corretivas de acordo com seu impacto potencial (Martins; Guimarães, 2021).

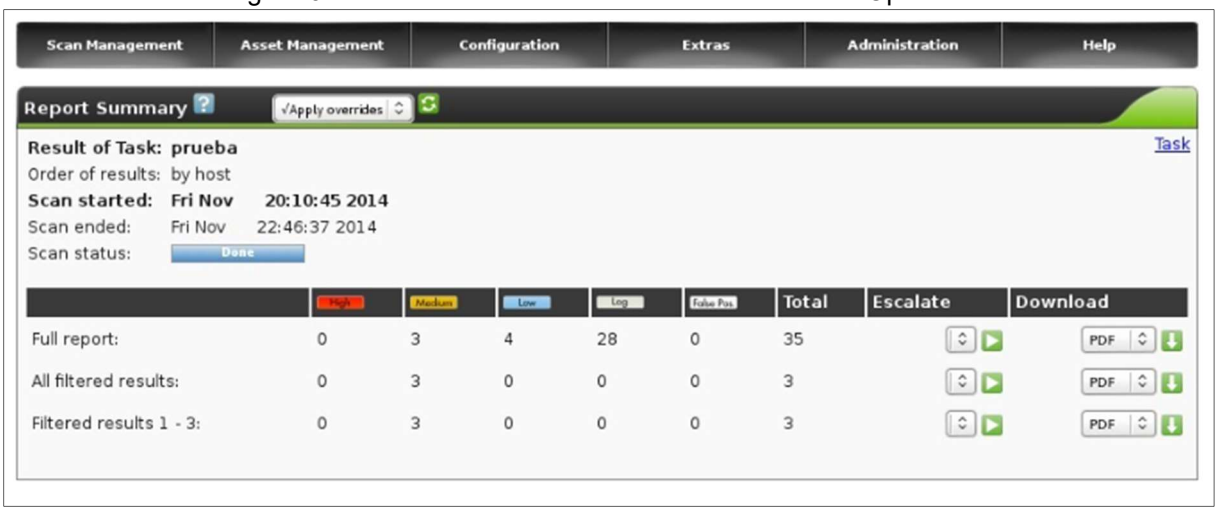
A Figura 5 e Figura 6 mostram respectivamente, a tela de interface gráfica do OpenVAS usada para iniciar o escaneamento de um ativo e a tela de resultados.

Figura 5 – Interface Gráfica do OpenVAS – tarefa de escaneamento de vulnerabilidades.



Fonte: Adaptado da ferramenta OpenVAS

Figura 6 – Tela de resultado do escaneamento com o OpenVAS



Fonte: Adaptado da ferramenta OpenVAS

2 METODOLOGIA

Este trabalho caracteriza-se como uma pesquisa de base teórica com aplicação prática, desenvolvida a partir da análise e interpretação de fontes bibliográficas, normativas e técnicas relacionadas à gestão de vulnerabilidades técnicas no contexto da segurança da informação. O objetivo da pesquisa foi estruturar um processo aplicável de gerenciamento de vulnerabilidades em ativos organizacionais críticos, com foco na consistência das decisões técnicas e na mitigação de vulnerabilidades técnicas.

A abordagem da pesquisa é qualitativa, pois busca compreender, organizar e propor soluções com base na interpretação crítica da literatura especializada. Não foram utilizados instrumentos empíricos, como entrevistas ou questionários, uma vez que o trabalho não possui caráter experimental ou de campo. Em vez disso, a construção do modelo proposto baseou-se na análise conceitual de documentos técnicos, normas internacionais, artigos acadêmicos e guias de boas práticas.

Entre as principais referências utilizadas, destaca-se o Guia de Gerenciamento de Vulnerabilidades, publicado pela Secretaria de Governo Digital do Governo Federal (BRASIL, 2023). Este documento foi central para a estruturação do processo sugerido, servindo como base para a definição de etapas como: escopo e priorização de ativos, identificação e categorização de vulnerabilidades, análise e tratamento dos achados técnicos, e planejamento de monitoramento contínuo. O guia fornece diretrizes práticas alinhadas às políticas públicas de segurança da informação, permitindo que o modelo proposto neste trabalho de conclusão de curso seja compatível com os referenciais adotados por órgãos públicos e organizações privadas brasileiras.

Além disso, foram incorporadas contribuições teóricas extraídas de normas como a ABNT NBR ISO/IEC 27002:2022, dos Controles CIS (Center for Internet Security) e de autores especializados em segurança da informação e gestão de vulnerabilidades. A pesquisa foi desenvolvida de forma individual, ao longo do semestre letivo, com apoio do professor orientador na validação da estrutura do trabalho e na adequação do conteúdo técnico à proposta acadêmica.

Embora a pesquisa tenha sido exclusivamente bibliográfica, e não exista amostra delimitada ou universo de aplicação empírica, foi possível desenvolver o modelo proposto, pensado para ser adaptável a organizações de diferentes tamanhos,

especialmente aquelas que lidam com ativos de tecnologia da informação e buscam elevar sua maturidade em segurança de forma objetiva e estruturada.

As etapas do trabalho seguiram uma sequência lógica: levantamento e revisão da literatura; identificação dos principais referenciais técnicos e normativos; análise crítica dos conceitos e práticas disponíveis; e, por fim, o desenvolvimento do processo de gestão de vulnerabilidades técnicas, apresentado no capítulo seguinte. Não foram utilizados métodos estatísticos ou técnicas de tabulação de dados, visto que o foco da pesquisa está na construção conceitual do processo.

Conclui-se, portanto, que a metodologia adotada foi adequada ao propósito do trabalho, permitindo a construção de um modelo coerente com os princípios da segurança da informação e fundamentado em fontes confiáveis e atualizadas.

3 Resultados, análise e discussão dos dados

3.1 Abrangência do escopo

É essencial estabelecer critérios claros para identificar e priorizar ativos organizacionais relevantes para a análise de vulnerabilidades, com base em práticas reconhecidas de governança de TI e segurança da informação. O Guia de Gerenciamento de Vulnerabilidades, publicado pela Secretaria de Governo Digital (Brasil, 2023), apresenta um modelo estruturado com etapas que incluem a definição do escopo, identificação de ativos, priorização e categorização das vulnerabilidades como parte inicial de um processo contínuo.

Adicionalmente, Gaseta (2011) destaca que a clareza na definição de escopo e atribuições, aliada a uma comunicação eficiente entre as áreas técnicas e de gestão, é essencial para minimizar ruídos no processo decisório e assegurar a efetividade das ações voltadas à segurança da informação. Dessa forma, a definição do escopo deve ir além dos aspectos puramente técnicos, contemplando também fatores organizacionais e comunicacionais que impactam diretamente a maturidade e a eficiência do processo de gerenciamento de vulnerabilidades.

Conforme o modelo proposto pelo Governo Federal no Guia de Gerenciamento de Vulnerabilidades (Brasil, 2023), a definição do escopo é a etapa inicial e estratégica do processo, e deve considerar os seguintes passos:

- Identificação dos ativos organizacionais – Consiste em mapear quais sistemas, equipamentos, aplicações, serviços e dados são relevantes para o funcionamento da organização e para o cumprimento de seus objetivos. Essa identificação deve ser orientada por critérios de criticidade, valor da informação e dependência operacional.
- Priorização de ativos – Após o mapeamento, é necessário estabelecer prioridades com base em fatores como impacto em caso de comprometimento, sensibilidade dos dados envolvidos e exposição ao ambiente externo (por exemplo, serviços acessíveis via Internet).
- Delimitação do escopo técnico e organizacional – Define-se quais ativos, redes ou ambientes serão contemplados no ciclo de gerenciamento de vulnerabilidades, levando em conta os recursos disponíveis, a maturidade da equipe e o contexto institucional.

- Atribuição de responsabilidades – O escopo também deve indicar os responsáveis por cada etapa do processo (análise, validação, correção, acompanhamento), a fim de garantir clareza na execução e na comunicação entre os envolvidos.

Esses passos formam a base para a construção de um processo contínuo, que será posteriormente complementado com etapas de identificação, análise, correção e monitoramento das vulnerabilidades. A precisão na definição do escopo é determinante para a eficácia do processo como um todo, pois direciona os esforços para os ativos mais relevantes e minimiza retrabalho.

Souza e Dias (2018) complementam essa perspectiva ao abordarem a importância de alinhar a definição do escopo com as limitações do ambiente corporativo e com os recursos disponíveis. Os autores reforçam a necessidade de estabelecer claramente: quais ativos serão incluídos no processo; quais limitações técnicas ou organizacionais se aplicam (como restringir a análise a ambientes de produção); quem são os responsáveis por cada etapa; e os documentos e diretrizes que fundamentam o processo, como mostrado na Figura 7. Essa abordagem prática reforça a aplicabilidade do modelo em cenários reais, assegurando que o escopo definido esteja adequado a cada organização.

Figura 7 - Fluxograma parcial – escolha de ativos.

Fonte: Elaborado pela autora

3.2 Identificação das vulnerabilidades técnicas

Este objetivo busca compreender as etapas envolvidas na identificação de vulnerabilidades em ativos organizacionais críticos, considerando práticas e metodologias consolidadas em segurança da informação.

A correta identificação de vulnerabilidades é essencial para antecipar riscos e orientar ações de mitigação mais eficazes. O ruído nas fases de identificação das vulnerabilidades pode levar a decisões inconsistentes e falhas na priorização das

ações. A gravidade de uma vulnerabilidade pode ser subestimada ou superestimada, causando atrasos nas correções necessárias ou a alocação incorreta de recursos.

O ruído nos processos decisórios pode ser prejudicial, pois ele gera inconsistências na tomada de decisão, afetando a precisão e a eficácia das respostas a riscos (Kahneman; Sibony; Sunstein, 2021).

A minimização do ruído nas fases de identificação de vulnerabilidades pode ser alcançada por meio de várias estratégias, tais como:

- Padronização dos Processos: estabelecer critérios claros e uniformes para a identificação das vulnerabilidades, com o uso de ferramentas padronizadas e a definição de protocolos para interpretação de resultados pode reduzir a variabilidade nos julgamentos;
- Treinamento e Capacitação: a capacitação contínua dos profissionais envolvidos no processo de identificação, com ênfase na análise crítica e na interpretação precisa dos dados, ajuda a reduzir a subjetividade;
- Melhoria na Comunicação: Uma comunicação clara entre equipes técnicas e de gestão, com a utilização de relatórios padronizados e compreensíveis por todos, ajuda a evitar mal-entendidos e ruídos causados pela falta de alinhamento.

Portanto, ao focar nas fases de identificação das vulnerabilidades, é essencial que o processo seja estruturado de maneira a reduzir ao máximo o ruído, garantindo que as decisões sobre a segurança dos ativos organizacionais sejam baseadas em informações precisas e análises consistentes.

Segundo o Guia de Gerenciamento de Vulnerabilidades (Brasil, 2023), a fase de identificação deve suceder a definição de escopo, e envolve o uso de ferramentas automatizadas, como ferramentas de detecção, além de inspeções manuais e análise de *logs*. Essa combinação possibilita uma visão abrangente das fragilidades técnicas que podem comprometer a confidencialidade, integridade e disponibilidade das informações.

Souza e Dias (2018) destacam que a detecção de vulnerabilidades deve abranger tanto os componentes de rede quanto sistemas e aplicações, sendo fundamental que a varredura seja realizada de forma sistemática e documentada. Os autores ressaltam ainda a importância da padronização nos critérios de análise para evitar subjetividade na interpretação dos resultados.

James Michael Stewart (Stewart, 2020) complementa que, além das abordagens tradicionais de escaneamento e análise de portas, a identificação pode incluir técnicas comportamentais para detectar anomalias operacionais. O autor enfatiza também que as vulnerabilidades devem ser classificadas com base em sua gravidade e no potencial de exploração, o que contribui para uma priorização técnica mais precisa. Além disso, ele ressalta a necessidade de manter as ferramentas e suas bases de dados constantemente atualizadas frente às ameaças emergentes.

Nesse contexto, destaca-se o uso de sistemas de catalogação como o CVE, que permite nomear e documentar vulnerabilidades de forma padronizada e reconhecida globalmente, além de contribuir para a rastreabilidade e comparação com bases de correções e atualizações de segurança.

Dessa forma, o estudo das fases de identificação abrange não apenas a escolha de ferramentas adequadas, mas também a definição de critérios de análise, a documentação técnica dos achados e a categorização das vulnerabilidades conforme seu risco potencial. Isso contribui para a criação de um processo contínuo de gerenciamento, que se apoia em dados concretos, reduz a subjetividade e pode ser integrado com as demais etapas do ciclo de segurança da informação.

A varredura de ativos consiste na execução prática da etapa de identificação das vulnerabilidades técnicas e representa o momento em que os ativos mapeados anteriormente são efetivamente analisados quanto à presença de falhas exploráveis. Essa atividade pode ser realizada com o uso de ferramentas automatizadas, como o OpenVAS e o Nessus, que se destacam pela capacidade de escanear redes, sistemas operacionais e aplicações em busca de vulnerabilidades conhecidas. Conforme Martinelo e Bellezi (2014), essas ferramentas utilizam bases de dados atualizadas com assinaturas de falhas técnicas e exploram portas, protocolos e serviços de rede para identificar comportamentos anômalos ou configurações inseguras.

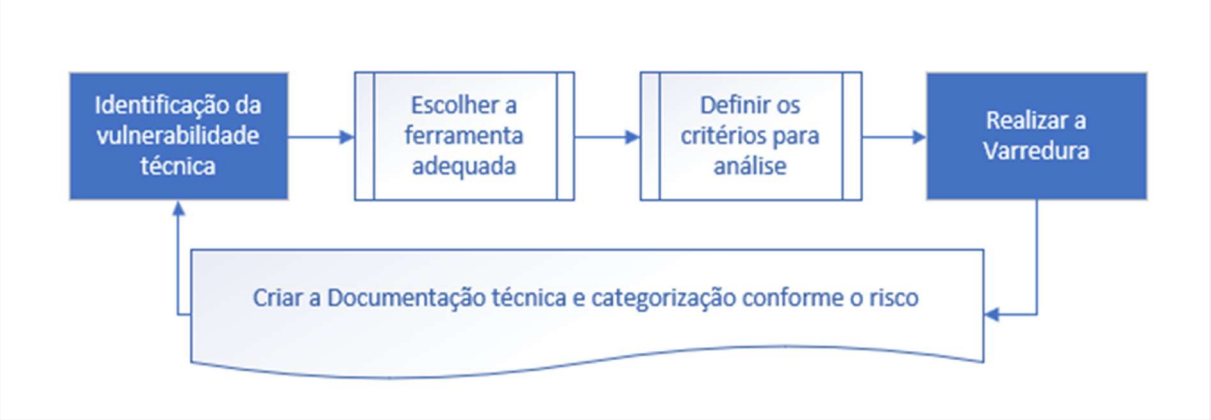
As ferramentas como OpenVAS e Nessus oferecem interfaces intuitivas e painéis configuráveis que facilitam a condução da varredura técnica, mesmo por equipes com diferentes níveis de experiência. A execução pode ser ajustada conforme o escopo definido, permitindo desde análises mais superficiais até varreduras profundas e direcionadas, o que garante flexibilidade conforme a criticidade dos ativos. Segundo Martinel o e Bellezi (2014), esses sistemas possibilitam a seleção de perfis de escaneamento e o acompanhamento da atividade em tempo real, tornando

a etapa de identificação mais acessível e operacionalizável no contexto organizacional.

Outro recurso amplamente utilizado na etapa de varredura de ativos é o *Nmap (Network Mapper)*, uma ferramenta de código aberto conhecida por sua flexibilidade e profundidade técnica. De acordo com Lyon (2022), o Nmap permite a personalização completa da varredura, incluindo a seleção de portas, protocolos e intervalos de IP, além da utilização de diferentes modos de escaneamento.

Essa combinação de recursos técnicos e opções de usabilidade torna o Nmap uma ferramenta acessível e poderosa para a identificação sistemática de fragilidades em ambientes de rede. A Figura 8 apresenta o fluxo de identificação de vulnerabilidades técnicas.

Figura 8 - Fluxograma parcial – identificação das vulnerabilidades técnicas.



Fonte: Elaborado pela autora

3.3 Análise das vulnerabilidades técnicas

Após a identificação e categorização das vulnerabilidades técnicas, a análise das recomendações de ações corretivas se revela uma etapa crítica no processo de gestão de vulnerabilidades, conforme Figura 9.

De acordo com o Guia de Gerenciamento de Vulnerabilidades (Brasil, 2023), o tratamento eficaz das vulnerabilidades requer considerar o contexto organizacional, os recursos disponíveis e a criticidade dos ativos. A priorização orientada por esse conjunto de fatores contribui para intervenções mais assertivas e alinhadas à realidade da organização.

As decisões devem estar alinhadas às prioridades estratégicas da organização e à continuidade dos serviços; como destacam Gaseta (2011) e Souza e Dias (2018), a análise das vulnerabilidades precisa considerar não apenas aspectos técnicos, mas também o contexto organizacional mais amplo, garantindo a alocação eficiente dos recursos disponíveis.

Ferramentas eficazes e padronizadas, bem como critérios de avaliação uniformes, contribuem para a consistência e a qualidade das recomendações de tratamento. Nesse sentido, a eficácia das ferramentas de varredura — como apontam Ferrão e Kreutz (2017) — influencia diretamente na precisão das ações corretivas propostas, sendo importante que as ferramentas de detecção utilizadas sejam atualizadas e adaptadas às necessidades da organização.

A adoção de sistemas de catalogação padronizados, como o CVE (C*ommon Vulnerabilities and Exposures)*, facilita a documentação, a rastreabilidade e a comunicação entre as equipes, tornando o processo mais eficaz e confiável.

O ruído no processo decisório refere-se a variabilidades indesejadas nos julgamentos humanos que ocorrem mesmo quando as decisões são tomadas em contextos semelhantes. Em ambientes organizacionais, esse ruído pode comprometer a consistência das decisões sobre tratamento de vulnerabilidades. Portanto, estruturar os fluxos de informação, padronizar critérios e apoiar-se em dados objetivos são estratégias fundamentais para mitigar esse tipo de interferência (Kahneman; Sibony; Sunstein, 2021).

Com base na análise desenvolvida, é possível sintetizar as principais diretrizes que orientam a etapa de definição das ações corretivas após a identificação das vulnerabilidades. A seguir, são destacados os pontos fundamentais que devem ser considerados para garantir um tratamento eficaz, alinhado às boas práticas de segurança da informação e ao contexto organizacional:

- Utilização do sistema CVE para padronização e rastreabilidade:
  - A adoção do CVE contribui para a padronização, comunicação e rastreabilidade das vulnerabilidades identificadas.
- Ação focada com base nos critérios pré-estabelecidos:
  - A priorização das ações deve considerar a gravidade técnica, a exposição do ativo, a facilidade de exploração e o impacto organizacional, conforme orientações do Guia de Gerenciamento de Vulnerabilidades e autores consultados.

- Importância da comunicação clara e fundamentada:
  - A troca de informações entre equipes técnicas e de gestão deve ser estruturada, clara e baseada em dados, reduzindo o ruído e aumentando a efetividade das decisões.
- Abordagem sistemática e alinhada ao contexto organizacional:
  - A análise deve ser feita de forma sistemática, considerando o contexto da organização, para garantir que as ações corretivas sejam eficazes e alinhadas à gestão de riscos.

Após a análise das vulnerabilidades identificadas, a etapa subsequente consiste na definição e execução das ações corretivas. Conforme orienta o Guia de Gerenciamento de Vulnerabilidades (Brasil, 2023), a mitigação deve ser planejada com base em critérios técnicos e organizacionais, considerando principalmente a gravidade da falha**,** o nível de exposição**,** a facilidade de exploração, o impacto nos ativos críticos e a disponibilidade de correções. O tratamento pode incluir a aplicação de atualizações (*patches*), reconfiguração de sistemas, substituição de componentes inseguros ou, em casos mais urgentes, a remoção temporária do ativo da rede.

Para apoiar a tomada de decisão e reduzir o ruído na priorização, recomenda-se o uso de uma tabela de classificação de vulnerabilidades, que atribui uma pontuação de 1 a 5 com base em cinco critérios principais. A pontuação total indica o nível de prioridade para tratamento. Um exemplo simplificado está apresentado na Tabela 1.

Tabela 1 - Classificação de Vulnerabilidades e Prioridade de Mitigação

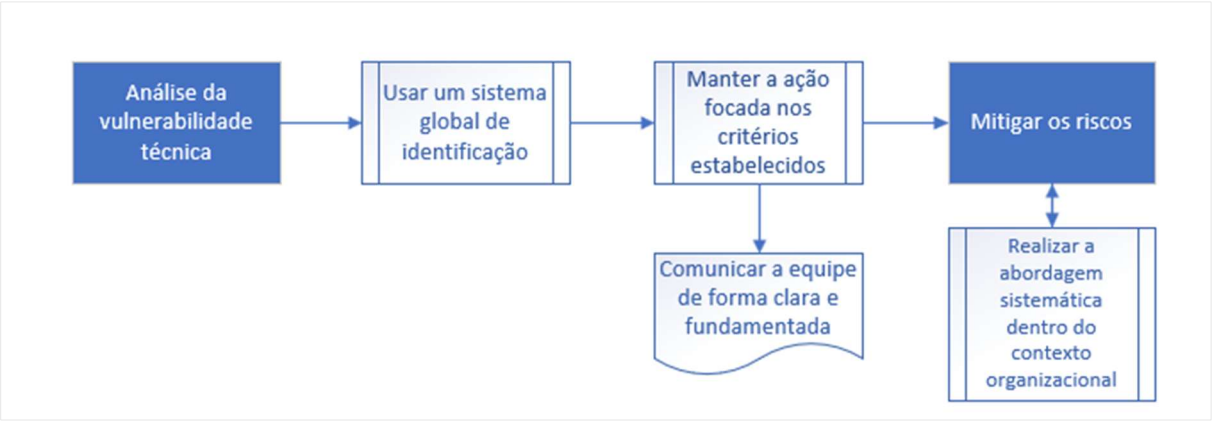
Critério	Pontuação (1 a 5)	Descrição
Gravidade Técnica (CVSS)	1 (baixa) a 5 (crítica)	Baseada em escore CVSS
Exposição do Ativo	1 (interna isolada) a 5 (exposição pública)	Nível de visibilidade e risco externo
Facilidade de Exploração	1 (muito difícil) a 5 (exploração trivial)	Requerimentos técnicos para exploração
Impacto Organizacional	1 (baixo) a 5 (crítico para o negócio)	Efeito na operação, reputação e dados
Disponibilidade de Correção	1 (sem correção disponível) a 5 (correção imediata disponível)	Facilidade de resolver a falha

Fonte: Elaborado pela autora

Pontuação Total (soma de 5 a 25):

- 21 a 25: Prioridade crítica (correção imediata)
- 16 a 20: Prioridade alta (até 3 dias úteis)
- 11 a 15: Prioridade moderada (até 7 dias úteis)
- 6 a 10: Prioridade baixa (acompanhar e reavaliar)
- 5: Prioridade muito baixa (sem ação imediata)

Figura 9 - Fluxograma parcial – análise das vulnerabilidades técnicas.



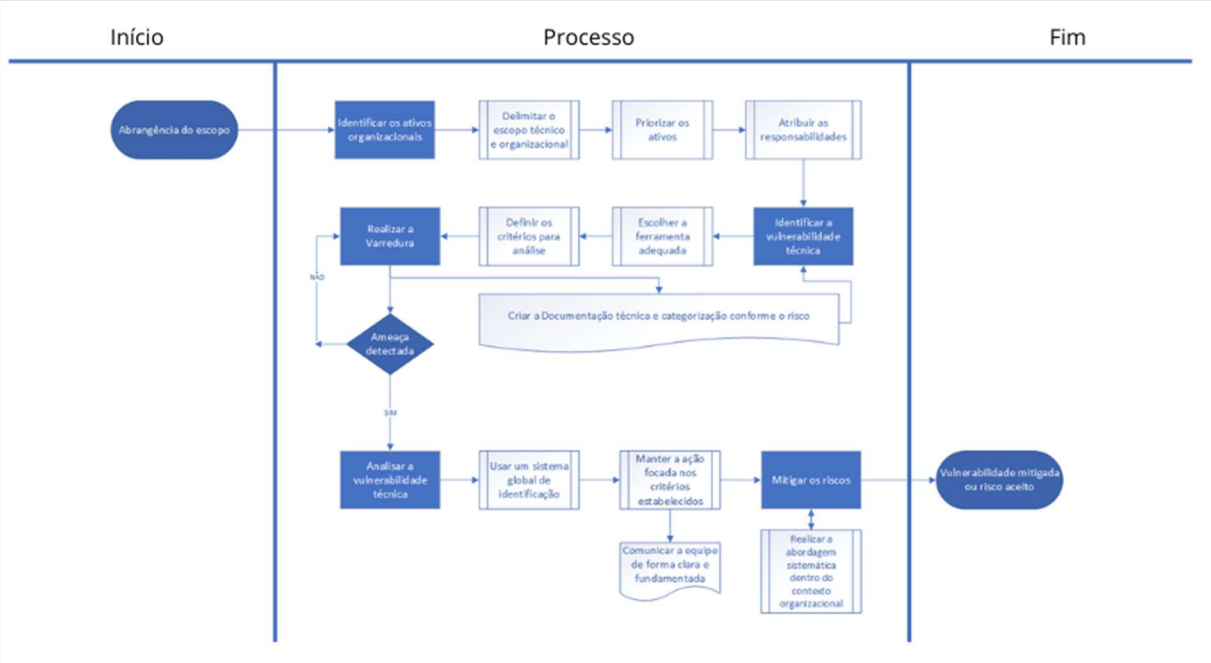
Fonte: Elaborado pela autora

4 Estruturação do processo de gestão de vulnerabilidades técnicas

Este capítulo apresenta a estrutura proposta para um processo contínuo de gestão de vulnerabilidades técnicas em ativos organizacionais críticos. A construção do processo baseia-se nas boas práticas consolidadas na literatura, nos controles normativos (como a ISO/IEC 27002 e os CIS Controls), nas diretrizes do Guia de Gerenciamento de Vulnerabilidades (Brasil, 2023), e na fundamentação teórica desenvolvida nos capítulos anteriores.

O processo sugerido, conforme mostrado na Figura 10, foi organizado em quatro macroetapas principais, subdivididas em atividades que visam reduzir o ruído nas decisões, padronizar a condução do gerenciamento e possibilitar sua aplicação de forma prática e adaptável ao contexto organizacional.

Figura 10 - Proposta de Processo de Gestão de Vulnerabilidades Técnicas



Fonte: Elaborado pela autora

5 CONSIDERAÇÕES FINAIS

Este Trabalho de Conclusão de Curso teve como finalidade propor um modelo de processo para a gestão de vulnerabilidades técnicas em ativos organizacionais críticos, considerando fundamentos da segurança da informação, o uso de ferramentas de varredura, boas práticas normativas e a redução do ruído na tomada de decisão.

A pesquisa, de caráter teórico-prático, fundamentou-se em referências como o Guia de Gerenciamento de Vulnerabilidades (Brasil, 2023), a ISO/IEC 27002:2022, os CIS Controls (CENTER FOR INTERNET SECURITY, 2024) e estudos de Souza e Dias (2018), Stewart (2020) e Ferrão e Kreutz (2017) sobre práticas de identificação e mitigação de vulnerabilidades técnicas. Com isso, buscou-se contribuir para o fortalecimento da segurança da informação nas organizações, com foco na consistência das decisões técnicas.

A hipótese proposta neste trabalho foi a de que seria possível prevenir incidentes de segurança da informação relacionados à exploração de vulnerabilidades, por meio da rápida mitigação de fragilidades nos ativos da organização, utilizando um processo de simples implantação e baixo custo, em alinhamento com a política vigente. Esta hipótese foi confirmada, uma vez que o processo desenvolvido mostrou-se sustentado por práticas reconhecidas. A estrutura do processo permite priorizar ações de mitigação com base em critérios objetivos, utilizando ferramentas acessíveis e protocolos claros de comunicação, o que reforça sua aplicabilidade com custo reduzido e efetividade.

O objetivo geral, de estruturar um processo de gerenciamento de vulnerabilidades técnicas, foi plenamente alcançado por meio da construção de um modelo em quatro macroetapas desenvolvidas com base em literatura especializada e normas como a ISO/IEC 27002, além de guias públicos nacionais e *frameworks* reconhecidos internacionalmente.

Os objetivos específicos também foram atendidos de forma integrada:

- Orientar a abrangência do escopo: foi realizado com a descrição estruturada dos critérios de identificação e priorização de ativos, escopo técnico e atribuições de responsabilidade;

- Estudar as fases de identificação de vulnerabilidades técnicas: contemplado com o mapeamento de ferramentas de varredura, critérios de análise e formas de registro técnico dos achados;
- Analisar as recomendações de ações para os resultados encontrados: cumprido com o detalhamento das ações corretivas proporcionais ao risco, dentro do contexto organizacional;
- Criar um processo para o monitoramento contínuo das vulnerabilidades: consolidado por meio de um modelo cíclico, com reavaliações periódicas, retroalimentação e aprendizado contínuo.

Conclui-se que a gestão eficaz de vulnerabilidades técnicas exige mais do que a detecção de falhas; exige um processo claro, objetivo e integrado à realidade da organização. O diferencial deste trabalho reside na inserção do conceito de ruído no julgamento técnico, abordado de forma transversal em todas as etapas. A redução do ruído — por meio da padronização de critérios, do uso de ferramentas consistentes e da comunicação clara — foi incorporada como elemento essencial para garantir coerência nas decisões, reduzir variabilidade indesejada e fortalecer a postura de segurança da informação. O processo desenvolvido atende aos princípios de simplicidade, aplicabilidade e alinhamento estratégico, tornando-se uma contribuição relevante para organizações que buscam elevar sua maturidade em segurança com foco na vulnerabilidade técnica.

REFERÊNCIAS

ABNT - Associação Brasileira de Normas Técnicas**. NBR ISO/IEC 27001** – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. ABNT, 2006.

BRASIL. Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27002:2022** - Tecnologia da Informação — Segurança da Informação — Código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

BRASIL. Secretaria de Governo Digital. **Guia de gerenciamento de vulnerabilidades.** Versão 2.0. Brasília: Ministério da Gestão e da Inovação em Serviços Públicos, 2023. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf. Acesso em: 30 março de 2025.

CENTER FOR INTERNET SECURITY. **CIS controls.** 2024. Disponível em: https://www.cisecurity.org/controls. Acesso em: 05 abr. 2025.

DO IMPÉRIO, Daniele Almeida; DA SILVA RODRIGUES, Fábio. **Segurança da informação:** enfoque na Cybersecurity. Encontro Internacional de Gestão, Desenvolvimento e Inovação (EIGEDIN), v. 3, n. 1, 2019.

FERNANDES, F. D.; SILVA, J. C. Gestão de vulnerabilidades em segurança da informação: um estudo de caso aplicado a pequenas e médias empresas. **Revista Brasileira de Gestão de Negócios**, v. 23, n. 1, p. 79-96, 2021.

FERRÃO, Isadora; KREUTZ, Diego. Segurança na Web: análise black-box de scanners de vulnerabilidades. In: ESCOLA REGIONAL DE ENGENHARIA DE SOFTWARE (ERES), 1., 2017, Alegre. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2017. p. 137-144.

GARCIA, Alexandre J. P. **Segurança da informação:** uma abordagem gerencial**.** 3. ed. Rio de Janeiro: Ciência Moderna, 2021.

GASETA, Edson Roberto. **Fundamentos de governança de TI.** Rio de Janeiro: Rede Nacional de Ensino e Pesquisa – RNP, 2011.

GREENBONE NETWORKS. **OpenVAS overview.** 2024. Disponível em: https://www.greenbone.net/en/. Acesso em: 10 abr. 2025.

INOVATECHY. **Nessus vulnerability scanner:** Proteção na era digital. 2023. Disponível em: https://inovatechy.com/nessus-vulnerability-scanner-protecao-na-era-digital/. Acesso em: 05 abr. 2025.

KAHNEMAN, Daniel; SIBONY, Olivier; SUNSTEIN, Cass R. **Ruído:** uma falha no julgamento humano. 1. ed. Rio de Janeiro: Objetiva, 2021.

KONZEN, Marcos Paulo; FONTOURA, Lisandra Manzoni; NUNES, Raul Ceretta. **Gestão de riscos de segurança da informação baseada na norma NBR ISO/IEC 27005 usando padrões de segurança**. 2013.

LYON, Gordon. Nmap Network Scanning: **The official Nmap project guide to network discovery and security scanning.** 1. ed. Sunnyvale: Insecure.Com LLC, 2022.

MARTINELO, Clériston Aparecido Gomes; BELLEZI, Marcos Augusto. **Análise de vulnerabilidades com OpenVAS e Nessus**. Revista TIS, v. 3, n. 1, 2014.

MARTINS, Reinaldo de Lima; GUIMARÃES, Ronaldo Cezar de Paula. Ferramentas de verificação de vulnerabilidades de segurança em redes e sistemas computacionais: uma revisão sistemática da literatura. **Revista de Tecnologias na Educação**, v. 13, n. 31, p. 30–45, 2021. Disponível em: https://periodicos.ifrn.edu.br/index.php/RTNE/article/view/14241. Acesso em: 10 abr. 2025.

MENDOZA, Miguel Ángel. **Como usar o OpenVAS para avaliação de vulnerabilidades**. WeLiveSecurity Brasil, 24 jul. 2019. Disponível em: https://www.welivesecurity.com/br/2019/07/24/como-usar-o-openvas-para-avaliacao-de-vulnerabilidades/. Acesso em: 10 abr. 2025.

REZENDE, Denis Alcides; ABREU, Antônio Sérgio Barros de. **Governança de tecnologia da informação e comunicação nas organizações:** guia prático com modelos e exemplos. 4. ed. São Paulo: Atlas, 2019.

SHANNON, Claude Elwood. A mathematical theory of communication. **Bell System Technical Journal**, v. 27, p. 379–423 e 623–656, 1948.

SKOUDIS, Ed; ZELTSER, Lenny. **Malware:** fighting malicious code. 2. ed. Indianapolis: Pearson Education, 2018.

SOUZA, G. P.; DIAS, C. F. Gestão de vulnerabilidades em redes de computadores: detecção e tratamento de vulnerabilidades em ambiente corporativo. In: Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, 2018.

STEWART, James Michael. **CompTIA Security+ guide to network security fundamentals**. 6. ed. Boston: Cengage Learning, 2020.

TENABLE NETWORK SECURITY. **Nessus essentials user guide**. Disponível em: https://www.tenable.com/products/nessus/nessus-essentials. Acesso em: 30 out. 2024.

UNITED STATES. National Institute of Standards and Technology. **National vulnerability database**. Gaithersburg: NIST, [s.d.]. Disponível em: https://nvd.nist.gov/. Acesso em: 06 abr. 2025.

UNITED STATES. National Infrastructure Advisory Council. **Common vulnerability scoring system:** Final Report and Recommendations. Washington, D.C.: CISA, 2004. Disponível em: https://www.cisa.gov/sites/default/files/publications/niac-common-vulnerability-scoring-final-report-10-12-04-508.pdf. Acesso em: 6 abr. 2025.