

POPSCRINIP



Manual de Operação

Gestão de Vulnerabilidades

Autor: Marcelio Soares Lima

Mentor: Max Eduardo Vizcarra Melgar

Última revisão: Julho de 2025

SUMÁRIO

SUMÁRIO.....	2
1. INTRODUÇÃO.....	3
2. VISÃO GERAL DA EMPRESA.....	4
3. PAPÉIS E RESPONSABILIDADES.....	4
4. FERRAMENTAS UTILIZADAS.....	5
• Greenbone Community Edition.....	5
• DefectDojo.....	5
5. INVENTÁRIO DE ATIVOS.....	5
6. PROCESSO DE VARREDURAS.....	7
6.1 Critérios para a realização das varreduras.....	7
6.2 Cronograma Detalhado.....	8
7. CLASSIFICAÇÃO E TRATAMENTO DE VULNERABILIDADES.....	9
7.1 Fluxo de tratamento.....	10
8. CONVENÇÕES DE NOMENCLATURA.....	10
8.1 Varreduras.....	10
8.2 Relatórios.....	11
Relatório Diário (Gerado pelo Greenbone).....	11
Relatório Técnico (Semanal).....	11
Relatório Executivo (Mensal).....	11
9. IMPORTAÇÃO PARA O DEFECTDOJO.....	12
10. BOAS PRÁTICAS.....	13
11. SEGURANÇA DE ACESSO ÀS FERRAMENTAS.....	13
12. MÉTRICAS E RELATÓRIOS.....	14
13. MELHORIA CONTÍNUA.....	15

1. INTRODUÇÃO

A gestão de vulnerabilidades é um processo contínuo e sistemático que envolve a identificação, classificação, priorização e correção de falhas de segurança em ativos de TI, como servidores, dispositivos de rede, sistemas e aplicações. No PoP-SC da Rede Nacional de Ensino e Pesquisa (RNP), essa prática é essencial para garantir a segurança das redes que conectam instituições acadêmicas e científicas em Santa Catarina. Este manual estabelece os procedimentos operacionais e padrões técnicos que orientam essa gestão, incluindo o uso de ferramentas de varredura, controle de inventário de ativos, análise dos relatórios gerados e comunicação dos resultados à gerência. O objetivo é assegurar uma abordagem padronizada, eficiente e alinhada às diretrizes da segurança da informação da RNP.

O conteúdo foi elaborado especialmente para apoiar gestores de vulnerabilidades iniciantes, oferecendo instruções claras e práticas sobre como conduzir cada etapa do processo. Desde a configuração das ferramentas até a interpretação dos relatórios, o manual fornece uma base sólida para quem está começando na área, permitindo que mesmo profissionais com pouca experiência possam aplicar boas práticas com segurança e eficiência.

O objetivo geral é garantir que a gestão de vulnerabilidades seja realizada de forma estruturada, documentada e alinhada às boas práticas organizacionais, contribuindo para a redução de riscos e a melhoria da visibilidade sobre o estado de segurança dos ativos.

Embora tenha sido desenvolvido com foco no ambiente técnico e organizacional do PoP-SC, este manual pode ser adaptado conforme as necessidades específicas de outras unidades da RNP ou instituições parceiras. Os processos descritos são flexíveis e podem ser ajustados para diferentes realidades, mantendo a consistência dos princípios de segurança da informação e gestão de vulnerabilidades.

2. VISÃO GERAL DA EMPRESA

O Ponto de Presença de Santa Catarina (PoP-SC) da Rede Nacional de Ensino e Pesquisa (RNP) é um hub de conectividade instalado na Superintendência de Governança Eletrônica e Tecnologia da Informação e Comunicação (SETIC/UFSC), em Florianópolis. Ele interconecta universidades e centros de pesquisa de todo o estado, fornecendo enlaces de alta capacidade via Backbone RNP e a Rede Metropolitana de Educação e Pesquisa da Região de Florianópolis (REMEP-FLN). O PoP-SC gerencia serviços avançados de internet, assegura alta disponibilidade operacional e oferece suporte técnico e colaboração em tempo real para comunidades acadêmicas, promovendo inovação e excelência em educação e ciência em Santa Catarina.

3. PAPÉIS E RESPONSABILIDADES

O Gestor de Vulnerabilidades deve assumir a responsabilidade formal pelo ciclo completo de identificação, análise, priorização e acompanhamento de correção de vulnerabilidades no PoP.

- Instalar, configurar e atualizar as ferramentas necessárias para a realização das atividades
- Definir e manter políticas e procedimentos de varredura e remediação
- Planejar e executar cronogramas de varredura
- Documentar qualquer processo ou configuração realizada ao decorrer das atividades.
- Analisar relatórios do Greenbone e validar achados
- Realizar ajustes nos relatórios gerados no Greenbone e importar para o DefectDojo
- Acompanhar prazos de correção conforme SLA interno
- Gerar e distribuir relatórios técnicos e executivos
- Registrar lições aprendidas e propor melhorias

4. FERRAMENTAS UTILIZADAS

• Greenbone Community Edition

- Execução e agendamento de Descoberta de Hosts, Varredura de Vulnerabilidade
- Classificação das Vulnerabilidades
- Geração de Relatórios
- Configuração de alertas para notificação e envio de relatórios.



• DefectDojo

- Ingestão de relatórios, acompanhamento e métricas de remediação
- Tratamento das vulnerabilidades
- Automação de importações
- Criação de Relatórios Técnicos e Executivos



5. INVENTÁRIO DE ATIVOS

<

Figura 1 - Exemplo de inventário de ativos.

Todos os ativos conectados ao PoP devem ser revisados, documentados e atualizados no inventário de ativos no mínimo a cada 24 meses e deve conter pelo menos as seguintes informações:

Descrição	Exemplo
Função	Roteador, Switch, Firewall, Servidor web
Endereço IP ou MAC Address	10.0.0.1 / 00:1A:2B:3C:4D:5E
Softwares Instalados	OpenSSH, Nginx, Apache, Grafana
Protocolo de aplicação e/ou porta	22, 25, 80, 443, 8080, 8443
Versão de firmware/SO	IOS XE 17.3.1, Ubuntu 20.04, Windows 11
Acessível pela Internet?	Sim / Não

O acesso ao inventário deve ser restrito exclusivamente à equipe de operações de rede, ao gestor de vulnerabilidades, aos analistas de segurança da informação e, quando necessário, à gerência técnica.

O inventário deve ser mantido em ambiente seguro, preferencialmente em servidor interno com backup regular, criptografia em repouso e em trânsito, e autenticação multifator para acesso.

6. PROCESSO DE VARREDURAS

6.1 Critérios para a realização das varreduras

- Programar para que ocorra diariamente, varreduras de descobertas de hosts.
 - As descobertas devem ser programadas para serem executadas a cada 1 hora.
 - O período de descoberta deve englobar o horário comercial.
 - Deve cobrir todas as redes privadas do PoP.
 - Os dispositivos que permanecem online durante as descobertas de hosts devem ser adicionados em um documento de mapeamento da infraestrutura.
 - Dispositivos que aparecem momentaneamente na descoberta de host, devem ser investigados.
 - Caso o dispositivo pertença a rede, deve ser documentado e apontado como dispositivo intermitente.
 - Se o dispositivo pertencia a rede e não está mais presente, deve ser atualizado e justificado.
- Executar manualmente ou programar varreduras de vulnerabilidades semanalmente.
 - Preferencialmente às sextas-feiras após o expediente..
 - A varredura deve ocorrer após uma sincronização dos feeds realizada em um intervalo de no máximo 7 dias.
 - Deve ser realizada uma varredura “Full and Fast” ajustada para redes privadas.
 - Deve ser realizado varreduras em todas as redes privadas do PoP que estão sendo monitoradas.
 - Deve ser realizada uma varredura “Full and Fast” (Padrão) em todas as redes públicas que estão sob monitoramento.
 - Nesta etapa dispositivos intermitentes devem ser avaliados.
 - Caso não seja possível, configurar uma varredura individual para avaliação quando o dispositivo estiver disponível na rede.
- Deve ser realizado uma varredura de vulnerabilidade em dispositivos críticos da empresa que sofreram atualização ou aplicação de patches.
- Deve ser realizada uma varredura em dispositivos críticos após um incidente de segurança ou campanhas globais de ataques cibernéticos.
- Toda varredura credenciada deve ser limitada a no máximo 20 dispositivos por vez, de preferência configurar uma varredura autenticada para cada dispositivo que será escaneado.

6.2 Cronograma Detalhado

Frequência	Horário	Escopo	Configuração da Varredura	Tipo de Varredura
Diária	00:00 – 23:59	Redes privadas	Automática	Host Discovery
Semanal	Sexta, 18:00 – Segunda, 07:00	Redes privadas	Automática/Manual	Full and Fast ajustada p/ Rede Privada
Semanal	Sexta, 18:00 – Segunda, 07:00	Redes públicas	Automática/Manual	Full and Fast (Padrão)
Após incidente, atualizações e aplicação de patch	18:00 – 07:00	Redes/Dispositivos Críticos	Manual	Full and Fast ou Customizada p/ Dispositivo
Após campanha global de ataques	Imediato	Redes/Dispositivos Críticos	Manual	Full and Fast ou Customizada p/ Dispositivo

7. CLASSIFICAÇÃO E TRATAMENTO DE VULNERABILIDADES

As vulnerabilidades devem ser classificadas e tratadas conforme o prazo máximo abaixo:

Severidade	CVSS	Prazo Máximo para Correção
Crítica	> 8.9	7 dias
Alta	7.0 – 8.9	30 dias
Média	4.0 – 6.9	90 dias
Baixa	0.1 – 3.9	120 dias

Embora a ferramenta Greenbone Community Edition já implemente a classificação baseada na pontuação CVSSv3.x, atualmente não é possível atribuir automaticamente a severidade “Crítica” para vulnerabilidades com escore superior a 8.9, conforme disponibilizado pela calculadora. Para garantir consistência na padronização antes da importação dos relatórios para o DefectDojo, e evitar inconsistências nos cálculos, independentemente da versão do CVSS utilizada, será adotado o critério de atribuição da severidade crítica para todas as vulnerabilidades com pontuação acima de 8.9.

CVSS

CVSS Base

9.8 (High)

CVSS Base Vector

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS Origin

NVD

CVSS Date

Wed, Feb 14, 2024 9:30 PM Coordinated Universal Time

Figura 2 - Vulnerabilidade classificada como “High” com calculadora CVSSv3.1.

7.1 Fluxo de tratamento

1. Triagem inicial e atribuição de severidade Isolamento do ativo, se necessário
2. Comunicação ao responsável técnico
3. Aplicação de correção ou mitigação, que pode incluir:
 - Aplicação de patches
 - Reconfiguração de sistemas
 - Substituição do dispositivo
 - Execução da sugestão técnica do Greenbone
 - Aceitação formal do risco (quando aplicável)
4. Varredura pós-correção para validação
 - Utilizar perfil "Full and Fast" ou varredura customizada conforme o tipo de vulnerabilidade corrigida
5. Atualização do DefectDojo
 - Alterar status da vulnerabilidade para "closed" ou "risk accepted" conforme resultado da validação

8. CONVENÇÕES DE NOMENCLATURA

8.1 Varreduras

- **Nome da Varredura:**
Deve refletir a descrição da rede alvo.
Exemplo: `Varredura_Rede_Visitantes`
- **Comentário na Configuração da Varredura:**
Informar os seguintes detalhes:
 - Quantidade de hosts escaneados em paralelo
 - Tipo de varredura utilizada (ex.: Full and Fast, Varredura Customizada)
 - Quantidade de NVTs executadas simultaneamente (caso diferente da configuração padrão)

`Varredura_Descoberta_Host_Rede_Visitantes`
(Host Discovery, 20 Hosts.)

`Varredura_Vulnerabilidade_Rede_Eventos`
(Full and Fast - Privado, 20 Hosts)

Figura 3 - Exemplos para nomenclatura de varredura, com comentários identificando detalhes.

8.2 Relatórios

Relatório Diário (Gerado pelo Greenbone)

- **Nome:**
Descrição da rede alvo + data da execução
Exemplo: Varredura_Rede_Visitantes_20250711

Varredura de Vulnerabilidade Rede Interna 1-20250625.csv	26/06/2025 01:30	Arquivo CSV
Varredura de Vulnerabilidade Rede Interna 1-20250626.csv	26/06/2025 23:41	Arquivo CSV
Varredura de Vulnerabilidade Rede Interna 1-20250627.csv	28/06/2025 02:20	Arquivo CSV
Varredura de Vulnerabilidade Rede Interna 1-20250628.csv	29/06/2025 17:01	Arquivo CSV
Varredura de Vulnerabilidade Rede Interna 1-20250629.csv	30/06/2025 09:01	Arquivo CSV
Varredura de Vulnerabilidade Rede Interna 1-20250630.csv	02/07/2025 21:18	Arquivo CSV
Varredura de Vulnerabilidade Rede Interna 1-20250701.csv	02/07/2025 21:18	Arquivo CSV
Varredura de Vulnerabilidade Rede Interna 1-20250702.csv	04/07/2025 14:54	Arquivo CSV
Varredura de Vulnerabilidade Rede Interna 1-20250703.csv	04/07/2025 14:58	Arquivo CSV
Varredura de Vulnerabilidade Rede Interna 1-20250704.csv	09/07/2025 02:32	Arquivo CSV
Varredura de Vulnerabilidade Rede Interna 1-20250705.csv	09/07/2025 02:37	Arquivo CSV

Figura 4 - Relatórios autogerados pelo greenbone, com nomenclatura padrão.

Relatório Técnico (Semanal)

- **Nome:**
Tipo do relatório + Data primeiro dia + Data último dia
Exemplo: Relatório_Técnico_20250707_a_20250711

RT Eroam e Visitantes 07072025 a 1107225.pdf	14/07/2025 21:31
RT Servicos 07072025 a 1107225.pdf	14/07/2025 21:33

Figura 5 - Exemplos de nomenclatura para relatórios técnicos.

Relatório Executivo (Mensal)

- **Nome:**
Tipo do relatório + mês e ano de referência
Exemplo: Relatorio_Executivo_Julho_2025

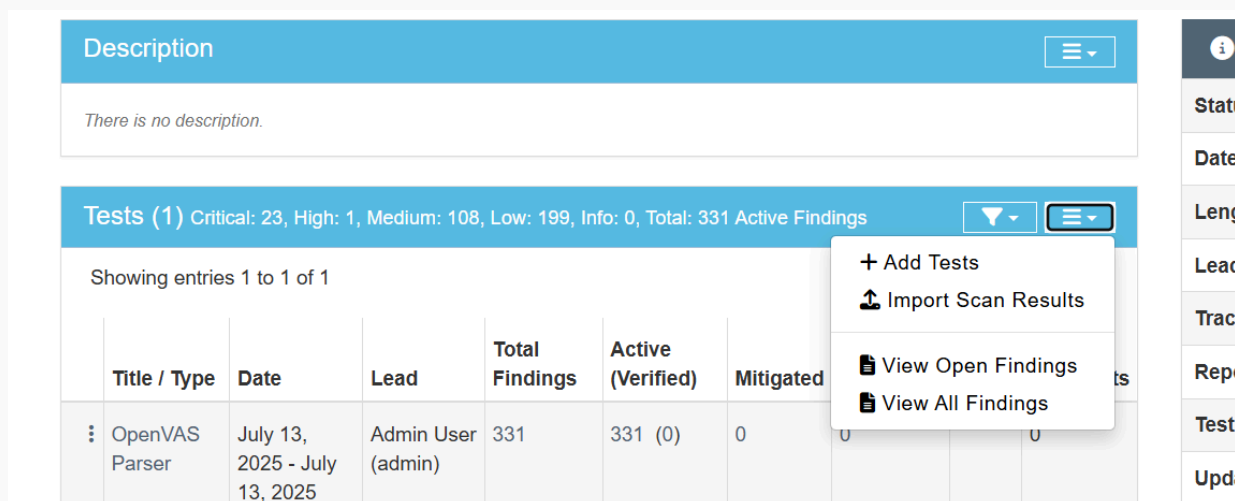
Relatório Executivo PoP-SC mes Junho 2025.pdf	18/07/2025 16:50
---	------------------

Figura 6 - Exemplo de nomenclatura para relatórios executivos.

9. IMPORTAÇÃO PARA O DEFECTDOJO

O relatório deve ser importado ao DefectDojo via interface web ou através da API, no formato de CSV.

- Deve ser decidido antes de realizar a importação, qual padrão será adotado para nomenclatura do “Product Type”, e do “Product”.
- O nome do engagement deve ser algo que identifique as redes ou ativos que estão sendo monitorados pela varredura, é recomendado que tenha o mesmo nome da varredura que foi configurada.
- Processo manual:
 1. Exportar CSV no Greenbone
 2. Importar no DefectDojo, seleccionando o Product
 3. Validar datas, hostnames e severidades
 4. Iniciar workflow de correção



Description

There is no description.

Tests (1) Critical: 23, High: 1, Medium: 108, Low: 199, Info: 0, Total: 331 Active Findings

Showing entries 1 to 1 of 1

Title / Type	Date	Lead	Total Findings	Active (Verified)	Mitigated
OpenVAS Parser	July 13, 2025 - July 13, 2025	Admin User (admin)	331	331 (0)	0

- + Add Tests
- Import Scan Results
- View Open Findings
- View All Findings

Figura 7 - Importação de relatórios do Greenbone para o DefectDojo via interface web.

10. BOAS PRÁTICAS

- **Varreduras autenticadas com mínimo privilégio**
Utilizar credenciais restritas para reduzir riscos e evitar impactos operacionais.
- **Validação de falsos positivos em até 5 dias úteis**
Analisar tecnicamente e documentar justificativas para findings irrelevantes.
- **Registro de evidências**
Salvar logs, capturas de tela e scripts utilizados nas ações de correção ou mitigação.
- **Verificação pós-correção em até 48 horas**
Reexecutar varredura no ativo corrigido para confirmar a eficácia da ação.
- **Comunicação de riscos aos stakeholders**
Informar severidade, impacto e status das vulnerabilidades às equipes responsáveis.
- **Alinhamento estratégico**
Garantir que as metas de remediação estejam conectadas aos objetivos da RNP.

11. SEGURANÇA DE ACESSO ÀS FERRAMENTAS

- **Acesso via HTTPS**
É recomendado utilizar acesso via HTTPS mesmo quando conectado por VPN, garantindo dupla camada de proteção. O certificado utilizado deve ser emitido por uma Autoridade Certificadora (CA) confiável, se disponível. Caso não seja possível, é aceitável utilizar um certificado auto gerado, desde que devidamente instalado e reconhecido pelos navegadores utilizados internamente. Isso evita exposição de credenciais e dados sensíveis durante a comunicação com as ferramentas.
- **Acesso à rede da organização exclusivamente por VPN**
A rede interna deve ser acessada exclusivamente por VPN corporativa, garantindo autenticação, criptografia e controle de acesso. Exceções devem ocorrer apenas em situações emergenciais, e sempre com algum mecanismo de segurança implementado, como acesso remoto via SSH com chave criptográfica ou páginas web protegidas por HTTPS.
- **Atualização das ferramentas e bases de dados**
A base de dados de vulnerabilidades do Greenbone (NVTs) deve ser atualizada com frequência, idealmente de forma automatizada ou ao menos semanalmente. Além disso, recomenda-se realizar uma atualização completa das instalações do Greenbone e do DefectDojo pelo menos a cada 6 meses, garantindo que correções de segurança, melhorias de desempenho e novas funcionalidades estejam aplicadas. Essas atualizações devem ser documentadas e testadas em ambiente controlado antes da aplicação em produção.

12. MÉTRICAS E RELATÓRIOS

A mensuração contínua de indicadores e a elaboração de relatórios são etapas fundamentais para avaliar a eficácia da gestão de vulnerabilidades no PoP-SC. As métricas permitem identificar padrões técnicos, acompanhar o desempenho das ações corretivas e fornecer visibilidade estratégica à equipe técnica e à gerência.

Principais KPIs (Indicadores de Desempenho)

- **Número de vulnerabilidades por severidade**
Classificação com base no CVSS (Crítica, Alta, Média, Baixa), permitindo priorização de correções e avaliação do risco geral.
- **Tempo médio de remediação (MTTR)**
Mede o intervalo entre a detecção e a correção de vulnerabilidades, refletindo a agilidade da equipe e o cumprimento dos prazos definidos.
- **Percentual de falsos positivos**
Indica a proporção de findings que não representam risco real após validação. Métrica útil para ajustar perfis de varredura e reduzir ruído nos relatórios.
- **Cumprimento de SLAs de correção**
Avalia se os prazos máximos de correção por severidade estão sendo respeitados. Casos fora do SLA devem ser destacados e justificados.
- **Distribuição por host, serviço e impacto**
Identifica ativos mais vulneráveis, serviços recorrentes em falhas e áreas críticas da infraestrutura.
- **Correlação com boas práticas e frameworks**
Mapeia vulnerabilidades em relação a controles reconhecidos (OWASP, CIS, NIST, ISO/IEC), facilitando recomendações alinhadas a padrões internacionais.

Tipos de Relatórios

- **Relatórios Técnicos (semanal)**
Apresentam detalhes das varreduras realizadas, vulnerabilidades detectadas, ativos afetados, evidências registradas e sugestão de ações corretivas aplicáveis. Devem incluir gráficos por severidade, distribuição por host e justificativas para falsos positivos.
- **Relatórios Executivos (mensal)**
Consolidam os principais indicadores, tendências de risco, status geral da segurança e recomendações estratégicas. Devem ser objetivos, visuais e alinhados aos objetivos da RNP, facilitando a tomada de decisão pela gestão.

13. MELHORIA CONTÍNUA

- Revisão trimestral do manual e cronogramas
- Ajuste de políticas, prazos e ferramentas conforme evolução de ameaças

Este manual deve ser versionado, revisado e aprovado pela gerência de segurança da informação antes de sua implementação.