

Instituto Federal de Brasília
Campus Brasília
Tecnologia em Sistemas para Internet

Thiago Amâncio Reis Caetano
Vitória Santana Silva

SISTEMA DE GERENCIAMENTO E MONITORAMENTO DE ATIVOS DE TI

Brasília
2025

Thiago Amâncio Reis Caetano
Vitória Santana Silva

SISTEMA DE GERENCIAMENTO E MONITORAMENTO DE ATIVOS DE TI

Trabalho de Conclusão de Curso apresentado ao curso de Tecnologia em Sistemas para Internet do Instituto Federal de Brasília do *Campus* Brasília, como parte da exigência para obtenção do título de Tecnólogo.

Orientador: Prof. MSc. Diógenes Ferreira Fustinoni
Computação/IFB

Brasília
2025

S586 Silva, Vitória Santana.
Sistema de gerenciamento e monitoramento de ativos de TI. / Vitória Santana Silva ; Thiago Amâncio Reis Caetano. – Brasília, 2025.
96 f. : il. color.

Orientador: Diógenes Ferreira Fustinoni.

Trabalho de conclusão de curso (Graduação) – Instituto Federal de Educação, Ciência e Tecnologia de Brasília, Tecnologia em Sistemas para Internet, 2025.

1. Gestão de ativos. 2. Snipe-IT. 3. Institutos educacionais. 4. Automação. I. Caetano, Thiago Amâncio Reis. II. Fustinoni, Diógenes Ferreira. (orient.). III. Título.

CDU 004.41:657.42

Elaborado com os dados fornecidos pelo autor.

Thiago Amâncio Reis Caetano
Vitória Santana Silva

SISTEMA DE GERENCIAMENTO E MONITORAMENTO DE ATIVOS DE TI

Trabalho de Conclusão de Curso apresentado ao curso de Tecnologia em Sistemas para Internet do Instituto Federal de Brasília do *Campus* Brasília, como parte da exigência para obtenção do título de Tecnólogo.

Aprovado em 11 de Dezembro de 2026

BANCA EXAMINADORA

Prof. MSc. Diógenes Ferreira Fustinoni
Computação/IFB
Orientador

Prof. Dr. Marco Rogério Calheira Lima
Computação/IFB
Membro interno

Prof. MSc. James Batista Figueredo
Computação/IFB
Membro interno

Dedicamos este trabalho à Deus, que nos sustentou até aqui, às nossas famílias, pelo apoio incondicional, aos nossos amigos, pelo incentivo constante, e a todos que, de alguma forma, contribuíram para a realização deste trabalho.

AGRADECIMENTOS

A realização deste trabalho foi possível graças à colaboração, paciência e incentivo de muitas pessoas que estiveram presentes ao longo desta jornada.

Agradecemos primeiramente a Deus, por nos conceder força, sabedoria e persistência para enfrentar cada desafio, mesmo diante das dificuldades.

Ao nosso orientador, Prof. MSc. Diógenes Ferreira Fustinoni, pela orientação cuidadosa, pela paciência em cada etapa e pela confiança em nosso potencial. Seu apoio técnico e acadêmico foi essencial para o amadurecimento deste projeto.

Aos nossos familiares, que estiveram ao nosso lado com amor, compreensão e incentivo constante. Foram eles que nos sustentaram nos momentos de maior cansaço e celebraram conosco cada pequena conquista.

Aos colegas e amigos do curso de Tecnologia em Sistemas para Internet, que compartilharam aprendizados, risadas e longas horas de estudo — companheiros fundamentais para tornar esta caminhada mais leve e significativa.

Um agradecimento especial à instituição de ensino Colégio Altaneiro, que inspirou este projeto e possibilitou o desenvolvimento prático da proposta de gestão de ativos de TI. A cada colaborador que contribuiu com respostas, ideias e disponibilidade, nosso sincero reconhecimento.

Por fim, a todos que, de alguma forma, contribuíram direta ou indiretamente para a concretização deste trabalho, deixamos nossa gratidão. Este projeto é fruto não apenas de esforço técnico, mas de uma rede de apoio, aprendizado e colaboração que nos acompanhou do início ao fim.

RECONHECIMENTO DE USO DE TECNOLOGIAS DE INTELIGÊNCIA ARTIFICIAL (IA) GENERATIVA, SOFTWARE E OUTRAS FERRAMENTAS DE APOIO

Foi utilizado IA generativa para apoio à otimização do referencial teórico (*Perplexity AI* e *Consensus*, 2025) e para elaboração de resumos de livros e artigos (*NotebookLM*, 2025). Além disso, foram utilizadas ferramentas de IA para correção gramatical (*Claude* e *Gemini*, 2025).

Reconheço a utilização de ferramenta de IA Generativa (*ChatGPT*, OpenAI, 2025) atuando como tradutor, para tradução de um artigo originalmente de língua inglesa.

Reconheço a utilização do *Microsoft Forms* para levantamento de dados de avaliação por meio de questionários.

Reconheço a utilização do editor de código *Visual Studio Code* (Microsoft) para a escrita do código e texto deste presente trabalho, bem como a utilização de *containers Docker* com imagem LaTeX para a compilação do documento final.

“No cansaço dos dias difíceis, encontro descanso na promessa: ‘Eu vos aliviarei.’”.
— Mateus 11:28

“A sabedoria começa na admiração. É preciso um coração cheio de curiosidade para aprender e viver.”
— Simone de Beauvoir, 1947

RESUMO

CAETANO, Thiago Amâncio Reis; SILVA, Vitória Santana. **Sistema de Registro e Monitoramento de Inventário de TI** 2025. Trabalho de Conclusão de Curso (Graduação) – Tecnólogo em Sistemas para Internet. Instituto Federal de Brasília –Campus Brasília. Brasília/DF, 2025.

Este trabalho apresenta a implementação e customização do sistema *open source* Snipe-IT para a otimização da gestão de ativos de Tecnologia da Informação (TI) em uma instituição de ensino fundamental em Brasília. O estudo fundamenta-se nas deficiências operacionais diagnosticadas no ambiente escolar, caracterizadas pela falta de rastreabilidade dos equipamentos, ausência de padronização nos processos de empréstimo e falhas na comunicação entre o suporte técnico e os usuários. A metodologia adotada classifica-se como pesquisa aplicada, de abordagem mista (qualitativa e quantitativa), utilizando levantamento documental, entrevistas e aplicação de questionários para compor o diagnóstico. Os dados coletados evidenciaram um cenário crítico: 82% dos colaboradores relataram inconsistências nos registros de retirada e devolução de itens e 71% desconheciam a existência de controles sobre perdas ou danos. Como solução, foi desenvolvida uma infraestrutura baseada em contêineres Docker e integrada ao Active Directory (AD) para autenticação centralizada, complementada por *scripts* de automação para *backup* e notificações. A validação da proposta ocorreu por meio de Prova de Conceito (PoC), simulando cenários reais de auditoria e ciclo de vida dos ativos. Os resultados demonstraram que a solução proposta assegura a integridade dos dados, agiliza a auditoria patrimonial via códigos QR e promove a sustentabilidade da gestão de TI na instituição.

Palavras-chave: Gestão de ativos; Snipe-IT; Institutos educacionais; Automação.

ABSTRACT

CAETANO, Thiago Amâncio Reis; SILVA, Vitória Santana. **Sistema de Gerenciamento e Monitoramento de Ativos de TI.** Brasília, 2025. Final Paper (Technologist in Internet Systems) — Instituto Federal de Brasília, Campus Brasília.

This paper presents the implementation and customization of the open-source system Snipe-IT to optimize Information Technology (IT) asset management in an elementary school in Brasília. The study is grounded in operational deficiencies diagnosed within the school environment, characterized by a lack of equipment traceability, the absence of standardized lending processes, and communication failures between technical support and users. The methodology is classified as applied research with a mixed approach (qualitative and quantitative), employing document analysis, interviews, and questionnaires to compose the diagnosis. The collected data revealed a critical scenario: 82% of collaborators reported inconsistencies in item checkout and return records, and 71% were unaware of existing controls regarding losses or damages. As a solution, an infrastructure based on Docker containers was developed and integrated with Active Directory (AD) for centralized authentication, complemented by automation scripts for backup and notifications. The proposal validation occurred through a Proof of Concept (PoC), simulating real-world auditing scenarios and asset lifecycles. Results demonstrated that the proposed solution ensures data integrity, streamlines patrimonial auditing via QR codes, and promotes the sustainability of IT management within the institution.

Keywords: Asset management; Snipe-IT; Educational institutions; Automation.

LISTA DE FIGURAS

Figura 1 – Ciclo de Vida de Ativos de Tecnologia da Informação (TI) 21
Figura 2 – Interface do Snipe-IT 22
Figura 3 – Exemplo de Etiqueta de Ativo 23
Figura 4 – API Reference 24
Figura 5 – Fluxograma das Etapas Metodológicas 35
Figura 6 – Tabela Escopo da Rede 37
Figura 7 – Configuração de *Virtual Local Area Network* (VLAN)s no *switch* 37
Figura 8 – Mapeamento de Ativos de TI CSV 38
Figura 9 – Diagrama de Implementação do Ambiente de Produção 39
Figura 10 – Controle de entrada e saída de materiais 42
Figura 11 – Conferência na retirada/devolução de itens 42
Figura 12 – Registros de perdas, extravios ou danos 43
Figura 13 – Avaliação das condições de armazenamento 43
Figura 14 – Impacto do controle na manutenção técnica 44
Figura 15 – Diagrama de Atividade — Fluxo de Empréstimo (Professor/Setor) 48
Figura 16 – Diagrama de Atividade — Fluxo de Empréstimo (Coordenação/Secretaria) 49
Figura 17 – Diagrama de Atividade — Fluxo de Manutenção (Técnico de TI) 49
Figura 18 – Diagrama de Atividade — Fluxo de Auditoria 50
Figura 19 – Diagrama de Sequência — Comunicação 53
Figura 20 – Arquitetura *Webhook — Snipe-IT* <-> Active Directory *(AD)* 55
Figura 21 – Termo de Responsabilidade 58
Figura 22 – Notificações de Estoque Baixo 59
Figura 23 – Etiquetas Patrimoniais com *Quick Response Code* (QR Code) 59
Figura 24 – Pagina de Detalhes do Ativo 60

LISTA DE QUADROS

Quadro 1 – Regras de Negócio 44
Quadro 2 – Requisitos Funcionais 46
Quadro 3 – Requisitos Não Funcionais 47
Quadro 4 – Requisitos de Implementação e Treinamento 47

LISTA DE SIGLAS E ABREVIATURAS

ABNT Associação Brasileira de Normas Técnicas.
AD *Active Directory*.
API *Application Programming Interface*.
CD/CI *Continuous Delivery/Continuous Integration*.
CGSI Comitê Gestor de Segurança da Informação.
CSV *Comma Separated Values*.
FOSS *Free and Open Source Software*.
HTTPS *Hypertext Transfer Protocol Secure*.
IEC *International Electrotechnical Commission*.
ISO *International Organization for Standardization*.
ITAM *Information Technology Asset Management*.
ITIL *Information Technology Infrastructure Library*.
JSON *JavaScript Object Notation*.
KVM *Kernel-based Virtual Machine*.
LDAP *Lightweitght Directory Access Protocol*.
NBR Norma Brasileira.
PDF *Portable Document Format*.
PoC Prova de Conceito.
QR Code *Quick Response Code*.
RPO *Recovery Point Objective*.
RTO *Recovery Time Objective*.
SGBDR Sistema de Gerenciamento de Banco de Dados Relacional.
SMTP *Simple Mail Transfer Protocol*.
SNMP *Simple Network Management Protocol*.
SO Sistema Operacional.
SQL *Structured Query Language*.
SSH *Secure Shell*.
SSL *Secure Sockets Layer*.
TI Tecnologia da Informação.
TLS *Transport Layer Security*.
UML *Unified Modeling Language*.
VLAN *Virtual Local Area Network*.
VM Máquina Virtual.
VNC *Virtual Network Computing*.
VoIP *Voice over IP*.
VS Code *Visual Studio Code*.

SUMÁRIO

1 INTRODUÇÃO 16
1.1 Tema 17
1.2 Problema 17
1.2.1 Objetivo geral 17
1.2.2 Objetivos específicos 18
1.3 Estrutura do TCC 18
1.4 Classificação da Pesquisa 19

2 FUNDAMENTAÇÃO TEÓRICA 20
2.1 Ativo de TI 20
2.1.1 Ciclo de Vida de Gestão de Ativos de TI 20
2.2 Snipe-IT 21
2.2.1 Etiqueta de Ativo 22
2.2.2 Integrações 23
2.2.3 Empréstimos e devoluções 23
2.2.4 Relatórios e auditoria 24
2.2.5 Pontos fortes e limitações do Snipe-IT 25
2.2.6 Alternativas e justificativa da escolha do Snipe-IT 25
2.3 Infraestrutura 26
2.3.1 Windows Server 26
2.3.1.1 Active Directory 27
2.3.1.2 Microsoft Entra ID 27
2.3.1.3 Linux 27
2.3.1.4 Máquina Virtual 27
2.3.1.5 Docker 27
2.4 Protocolos de Rede 28
2.4.1 SSH 28
2.4.2 SNMP 28
2.4.3 SMTP 28
2.4.4 VNC 28
2.5 Tecnologias 29
2.5.1 Python 29
2.5.2 PowerShell 29
2.5.3 MySQL 29
2.5.4 Microsoft Visual Studio Code 30
2.5.5 Microsoft Forms 30

2.5.6 *Lucidchart* *30*
2.6 Estatística Aplicada à Pesquisa Científica **31**
2.7 Requisitos de *software*: Abordagens e Aplicações **31**
2.7.1 *Requisitos Funcionais* *32*
2.7.2 *Requisitos Não Funcionais* *32*
2.7.3 *Diagrama de Atividade* *33*
2.8 Governança de Ativos de TI **33**

3 METODOLOGIA **35**
3.1 Etapas Metodológicas **35**
3.1.1 *Ferramentas e Tecnologias* *36*
3.1.2 *Delimitação do Estudo* *36*
3.2 Levantamento e Coleta de Dados **36**
3.3 Mapeamento de Ativos **38**
3.4 Planejamento da Arquitetura do Sistema **39**
3.5 Implementação e Treinamento **39**

4 DESENVOLVIMENTO **41**
4.1 Análise Estatística **41**
4.1.1 *Síntese dos Dados* *44*
4.2 Regras de Negócio **44**
4.3 Requisitos **46**
4.3.1 *Requisitos Funcionais* *46*
4.3.2 *Requisitos Não Funcionais* *47*
4.3.3 *Requisitos de Implementação e Treinamento* *47*
4.4 Diagrama de Atividade **48**
4.5 Instalação e Configuração do Sistema **50**
4.5.1 *Ambiente de Implantação* *51*
4.5.2 *Configuração de Acesso e Segurança* *51*
4.5.3 *Integração de Serviços e Comunicação* *52*
4.5.4 *Políticas de Backup e Recuperação de Desastre* *53*
4.5.5 *Integração com Infraestrutura Existente* *54*
4.5.6 *Procedimentos de Implantação* *55*
4.6 Treinamento **56**
4.7 Considerações Finais da Implementação **56**

5 RESULTADOS E DISCUSSÃO **57**
5.1 Prova de Conceito e Simulação de Cenários Operacionais **57**
5.1.1 *Cenário A: Ciclo de Vida do Empréstimo de Ativos Móveis* *57*
5.1.2 *Cenário B: Gestão Proativa de Consumíveis e Alertas* *58*

5.1.3 Cenário C: Auditoria Física e Etiquetagem Inteligente 59

6 CONSIDERAÇÕES FINAIS 61

REFERÊNCIAS 62

APÊNDICE A – TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO 68

APÊNDICE B – INSTRUMENTO DE COLETA DE DADOS 70

APÊNDICE C – DOCUMENTAÇÃO INSTALAÇÃO SNIPE-IT 73

APÊNDICE D – DOCUMENTAÇÃO WEBHOOK 82

1 INTRODUÇÃO

A Tecnologia da Informação (TI) tem se consolidado como um pilar estratégico nas instituições educacionais, impactando diretamente a eficiência dos processos acadêmicos, a gestão administrativa e a proteção do patrimônio tecnológico. Com o avanço da digitalização, os ativos de TI tornaram-se essenciais para o funcionamento das escolas, exigindo uma gestão mais estruturada e inteligente (SND, 2022).

Neste contexto, adotar a visão de capacidade de TI proposta por Bharadwaj (2000) permite compreender como a habilidade organizacional de mobilizar e integrar recursos tecnológicos com outras competências internas pode gerar valor institucional sustentável. Essa perspectiva destaca que não apenas a posse da tecnologia, mas a forma como ela é gerida, determina seu impacto real. Em ambientes escolares, isso se reflete na necessidade de integrar infraestrutura, processos e pessoas em torno da tecnologia disponível.

Entretanto, muitas instituições de ensino ainda enfrentam desafios operacionais significativos na gestão de seus ativos. A movimentação constante de dispositivos entre alunos, professores e setores administrativos dificulta a rastreabilidade, a manutenção preventiva e o controle de garantias e licenças (SND, 2022). Como observa Teixeira (2021, p. 20), sistemas bem implementados reduzem os custos e melhoram o controle financeiro sobre esses recursos.

Além disso, a ausência de automação e a baixa integração entre os sistemas existentes limitam a capacidade de resposta dos departamentos de TI, agravando perdas e ineficiências. De acordo com Gregolinska *et al.* (2022), organizações que investem em tecnologias digitais integradas têm conseguido reduzir o tempo de inatividade de equipamentos em até 50%, aumentar a produtividade em até 30% e obter maior previsibilidade operacional — indicadores também desejáveis no setor educacional.

O crescimento dos investimentos em TI por empresas de diferentes portes evidencia a importância de estratégias eficazes para a gestão de ativos tecnológicos. Segundo levantamento do Gartner (2021), em 2021 os gastos globais com TI ultrapassaram US$ 4 trilhões, com tendência de aumento nos anos seguintes. Esse cenário reforça a necessidade de adotar soluções acessíveis, eficientes e adaptáveis que viabilizem uma administração mais estratégica desses recursos.

A literatura especializada aponta que o retorno efetivo sobre esses investimentos está diretamente ligado à capacidade de gerenciar adequadamente os ativos ao longo de seu ciclo de vida. Para Kamal (2006, *apud* Buch (2023)), esse gerenciamento tornou-se um fator crítico para o sucesso das organizações.

Neste contexto, propõe-se a implementação do *Snipe-IT*, uma solução de código aberto voltada à gestão de ativos de TI, na instituição educacional Altaneiro, um colégio de ensino fundamental localizado em Brasília. Trata-se de uma alternativa prática, de baixo

custo e com ampla possibilidade de customização, capaz de atender às necessidades específicas da instituição analisada. Entre os recursos previstos, destacam-se:

- Comunicação direta entre usuários e equipe técnica;
- Monitoramento contínuo dos dispositivos;
- Automação de tarefas operacionais recorrentes.

Mais do que solucionar problemas locais, a proposta busca construir um modelo replicável, que demonstre como a adoção de tecnologias acessíveis, combinada a boas práticas de gestão, pode gerar ganhos concretos em eficiência, inovação e sustentabilidade na administração dos recursos tecnológicos.

1.1 Tema

Gestão de ativos de TI aplicada ao contexto educacional, com foco na implementação do *Snipe-IT* e no desenvolvimento de soluções complementares para atender às demandas específicas de uma instituição de ensino básica.

1.2 Problema

A ausência de um sistema centralizado e eficiente para a gestão de ativos de tecnologia da informação em uma instituição particular de ensino fundamental tem gerado uma série de desafios operacionais. Entre os principais problemas identificados estão: a dificuldade no rastreamento de *notebooks* emprestados; o controle inadequado de consumíveis como tintas, papéis e peças de reposição; a desorganização e a falta de digitalização de documentos fiscais; e a ausência de monitoramento automatizado de prazos de garantias e licenças, o que tem resultado em perdas financeiras e interrupções de serviço.

Além disso, a comunicação entre os usuários e a equipe de TI ocorre de forma dispersa e ineficiente, prejudicando a priorização e o atendimento de chamados. Somam-se a isso o monitoramento precário do status das câmeras de segurança e a gestão limitada dos recursos de servidor, comprometendo tanto a segurança física quanto a estabilidade da infraestrutura digital da escola. Esses fatores contribuem para o desperdício de recursos, a sobrecarga da equipe técnica e uma experiência insatisfatória para os usuários, evidenciando a necessidade urgente de uma solução integrada e customizável para a gestão de ativos de TI nesse contexto educacional.

1.2.1 Objetivo geral

Implementar o sistema de gestão de ativos de TI *Snipe-IT* na instituição educacional Altaneiro, customizando-o para as necessidades locais por meio de *scripts* e extensões específicas, com o intuito de aprimorar a eficiência operacional, automatizar processos críticos e promover uma gestão mais integrada e estratégica dos recursos tecnológicos.

1.2.2 Objetivos específicos

- Aplicar questionário junto aos principais usuários e membros da equipe técnica para diagnosticar problemas atuais, validar necessidades específicas e embasar a implementação do sistema de gerenciamento de ativos.
- Realizar levantamento detalhado dos requisitos e regras de negócio relacionados à gestão dos ativos tecnológicos da instituição, mapeando as necessidades dos usuários e gestores.
- Identificar, catalogar e documentar detalhadamente os ativos de TI existentes na escola, incluindo computadores, notebooks, câmeras de segurança, consumíveis, servidores e demais equipamentos tecnológicos relevantes.
- Implementar arquitetura *containerizada* do Snipe-IT utilizando *Docker* para garantir portabilidade, escalabilidade e isolamento de serviços em ambiente educacional.
- Desenvolver integração de autenticação centralizada com *Active Directory* (AD/*LDAP*) para unificação de identidades e segurança de acesso.
- Treinar a equipe técnica e os usuários-chave para garantir a correta utilização do sistema, promovendo uma transição suave e eficaz para a nova plataforma de gestão de ativos.

1.3 Estrutura do TCC

O presente trabalho encontra-se dividido em seis capítulos, organizados de forma a conduzir o leitor desde a contextualização do problema até a validação prática da solução proposta. A distribuição do conteúdo obedece à seguinte lógica sequencial:

- O capítulo um estabelece as bases do trabalho, apresentando a contextualização do tema e a definição do problema relacionado à gestão de ativos de TI. Delimita os objetivos gerais e específicos a serem alcançados e apresenta a classificação metodológica do estudo;
- No capítulo dois é apresentado o embasamento conceitual e técnico necessário para o desenvolvimento do projeto. Aborda os princípios da *Information Technology Asset Management* (ITAM) e detalha a arquitetura tecnológica adotada.
- No capítulo três é tratada a metodologia que descreve o percuso investigativo, detalhando as técnicas de levantamento de dados e a análise documental da infraestrutura existente. Apresenta o mapeamento inicial dos ativos e o planejamento da arquitetura do sistema a ser implementado. Um fluxograma é apresentado no início do capítulo para definir a sequência metodológica.
- No capítulo quatro constitui-se o núcleo prático da pesquisa. Inicialmente, apresenta a análise estatística dos dados coletados no diagnóstico, fundamentando a necessidade da intervenção. Em seguida, define as regras de negócio e os requisitos de *software* (funcionais e não funcionais), ilustrados por diagramas de atividade. Por fim, detalha a

execução técnica, abrangendo a instalação do ambiente, a integração de serviços, scripts de automação de backup e a capacitação dos usuários.

- No capítulo cinco é abordado a validação da solução implementada por meio de uma *Prova de Conceito (PoC)*. São apresentados e discutidos cénarios operacionais simulados — incluindo o ciclo de vida de empréstimos, gestão proativa de consumíveis e auditoria física via códigos Quick Response Code *(QR Code)* — demonstrando a conformidade do sistema com os requisitos estabelecidos e a eficácia na resolução dos problemas diagnosticados.

1.4 Classificação da Pesquisa

Este trabalho caracteriza-se como uma pesquisa aplicada, do tipo estudo de caso, com abordagem qualitativa e quantitativa. A investigação é direcionada à realidade institucional de uma escola de ensino fundamental, com foco na resolução de um problema prático: a ausência de um sistema eficiente para o gerenciamento de ativos de TI.

Optou-se pela implementação e customização do *software open source Snipe-IT*, uma solução consolidada e amplamente utilizada na área, o que possibilita a adoção de boas práticas reconhecidas em gestão de ativos, além da redução de custos e da eliminação de licenças proprietárias.

A escolha por adaptar uma ferramenta já existente, em vez de desenvolver uma do zero, também visa ampliar a interoperabilidade com sistemas internos e garantir maior sustentabilidade técnica e financeira à instituição.

2 FUNDAMENTAÇÃO TEÓRICA

A presente revisão bibliográfica tem como objetivo contextualizar e embasar os conceitos fundamentais para a compreensão e desenvolvimento deste trabalho. Para isso, serão abordados temas relacionados à implementação da ferramenta *Snipe-IT*, protocolos de rede de computadores, tecnologias complementares e outros tópicos que sustentam a estruturação e aplicação de soluções para gestão de ativos de Tecnologia da Informação (TI).

Os conteúdos aqui apresentados abrangem tanto os aspectos teóricos quanto práticos das tecnologias e normas que guiam o gerenciamento de ativos, oferecendo uma visão abrangente sobre as possibilidades e os desafios do uso de ferramentas *open source* no contexto corporativo.

2.1 Ativo de TI

Um ativo de TI refere-se a qualquer componente tecnológico, físico ou digital que seja essencial para as operações de uma organização. Esses ativos incluem *hardware*, *software*, redes, dados e serviços. De acordo com a norma International Organization for Standardization *(ISO)*/International Electrotechnical Commission *(IEC)* 19770-1:2017 (ISO, 2017), os ativos de TI são definidos como "itens que têm valor para uma organização e que são utilizados para apoiar objetivos de negócios". Esses itens podem ser:

- ***Hardware*:** Dispositivos físicos como servidores, computadores, dispositivos móveis e equipamentos de rede.
- ***Software*:** Licenças de sistemas operacionais, aplicativos e ferramentas de produtividade.
- **Infraestrutura:** Componentes como roteadores, *switches* e *firewalls*.
- **Dados:** Informações armazenadas em bancos de dados ou sistemas digitais.
- **Serviços:** Recursos de computação em nuvem ou terceirização de tecnologia.

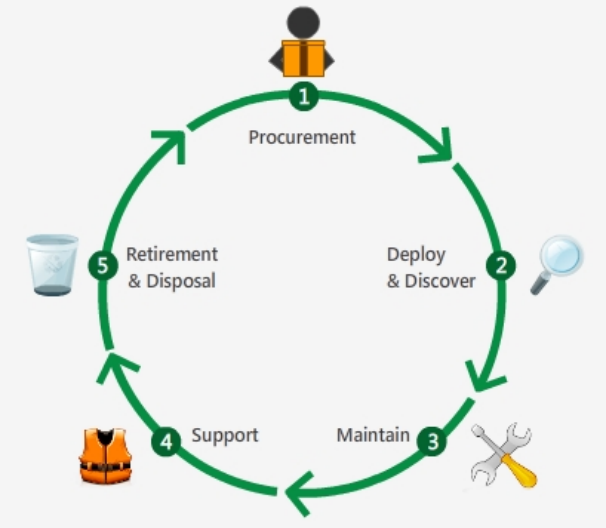
Os ativos de TI são fundamentais para o funcionamento das operações de TI e estão diretamente relacionados à eficiência, segurança e capacidade de inovação da organização (ISO, 2017).

2.1.1 Ciclo de Vida de Gestão de Ativos de TI

O ciclo de vida de gestão de ativos de TI é composto por cinco fases principais interconectadas, representadas de forma circular para ilustrar a natureza contínua e iterativa do processo.

A primeira fase, ***Procurement* (Aquisição)**, representa o início do ciclo onde os ativos são adquiridos pela organização. Esta etapa envolve a identificação de necessidades,

Figura 1 – Ciclo de Vida de Ativos de TI



Fonte: ManageEngine Site (2024).

seleção de fornecedores e formalização de contratos.

Na segunda fase, ***Deploy & Discover*** **(Implantação e Descoberta)**, os ativos são configurados, implementados no ambiente de produção e registrados no inventário organizacional. Esta etapa é fundamental para estabelecer o controle inicial sobre os recursos adquiridos.

A terceira fase, ***Maintain*** **(Manutenção)**, corresponde ao período operacional mais longo do ativo, envolvendo atualizações, correções e otimizações para garantir o funcionamento adequado.

A quarta fase, ***Support*** **(Suporte)**, abrange as atividades de assistência técnica, resolução de incidentes e garantia de disponibilidade dos ativos durante seu período de vida útil.

Finalmente, a quinta fase, ***Retirement & Disposal*** **(Aposentadoria e Descarte)**, trata da retirada controlada dos ativos obsoletos ou que atingiram o fim de sua vida útil, incluindo processos de descarte seguro, migração de dados e conformidade regulatória.

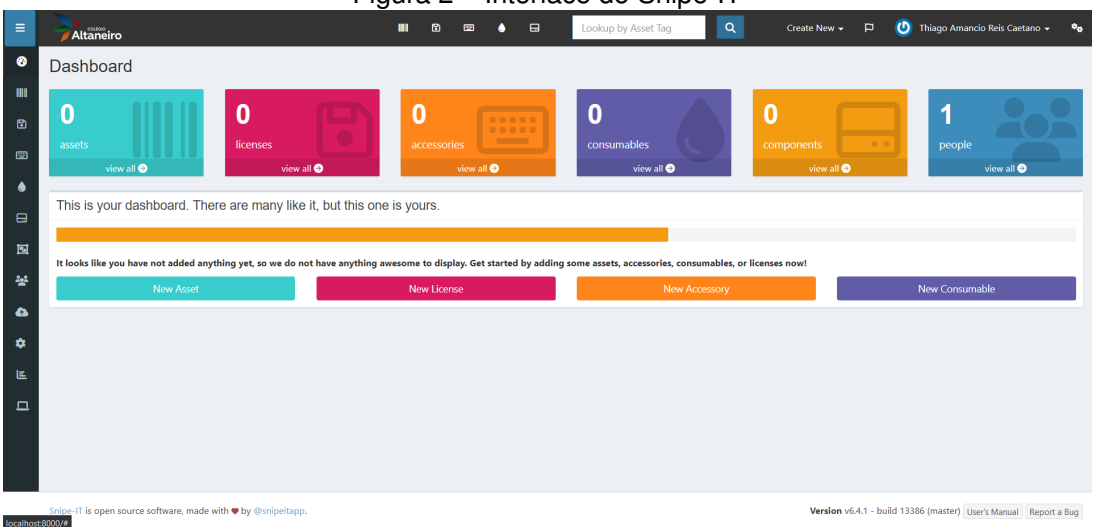
2.2 Snipe-IT

O *Snipe-IT* é uma ferramenta de código aberto *Free and Open Source Software* (FOSS) projetada especificamente para o *Information Technology Asset Management* (ITAM) (SNIPE-IT, 2025c). Ele permite que organizações de diferentes tamanhos rastreiem e administrem seus ativos tecnológicos de forma eficiente, contribuindo para a redução de custos, conformidade regulatória e maior controle operacional (SNIPE-IT, 2025c; TECH.CO, 2025).

Por conta de sua natureza *open source*, o *Snipe-IT* oferece uma série de vantagens em relação a soluções proprietárias, incluindo: custo reduzido, uma vez que é gratuito para uso na modalidade auto-hospedada e não requer licenças de software (SNIPE-IT,

2025c; GOWORKWIZE, 2025); flexibilidade para personalização da interface, campos e fluxos de trabalho (SNIPE-IT, 2025b; GROKABILITY, 2025); e uma comunidade ativa de desenvolvedores e usuários que contribui com correções, novas funcionalidades e suporte colaborativo (GROKABILITY, 2025; CAPTERRA, 2025). Além disso, o código-fonte aberto permite a auditoria de segurança e a verificação de conformidade com requisitos institucionais (TECH.CO, 2025; VIRIMA, 2025), enquanto a documentação oficial e os tutoriais detalham desde a instalação até configurações avançadas, facilitando a adoção em diferentes contextos organizacionais (SNIPE-IT, 2025b).

Figura 2 – Interface do Snipe-IT



Fonte: Criado pelo Autor (2025).

O *Snipe-IT* se destaca também por oferecer uma ampla gama de funcionalidades voltadas ao ciclo de vida dos ativos, como cadastro e categorização de equipamentos, controle de *status* (em uso, disponível, em manutenção, baixado), registro de histórico de empréstimos e devoluções, gerenciamento de licenças de software, contratos e acessórios, bem como geração de relatórios gerenciais e notificações automatizadas por e-mail (SNIPE-IT, 2025c). A aplicação pode ser implantada em servidores próprios ou em serviços de nuvem e conta com recursos de integração via *Application Programming Interface* (API) e suporte a diretórios como *Lightweitght Directory Access Protocol* (LDAP)/*Active Directory*, o que amplia sua interoperabilidade com outros sistemas institucionais e permite automatizar processos de autenticação e atualização de dados (SNIPE-IT, 2025a).

O *Snipe-IT* se destaca, portanto, por oferecer uma ampla gama de funcionalidades que tornam o gerenciamento de ativos eficiente e personalizável, atendendo às diversas necessidades das organizações (SNIPE-IT, 2025c; TECH.CO, 2025). Nas próximas seções, serão abordadas algumas das principais funcionalidades do sistema segundo a documentação oficial do *Snipe-IT*.

2.2.1 Etiqueta de Ativo

No *Snipe-IT*, há a possibilidade de criar etiquetas personalizadas para identificar e rastrear os ativos de TI, utilizando um identificador único (*asset tag*) associado a cada equipamento (SNIPE-IT, 2025c). Essas etiquetas podem conter informações como o nome do ativo, número de série, categoria, localização e responsável, além de um código de barras ou *QR Code* que facilita a leitura por dispositivos móveis ou leitores dedicados (SNIPE-IT, 2025b; TECH.CO, 2025). A etiqueta é impressa e fixada fisicamente no ativo, permitindo que, por meio da leitura do código, o usuário acesse diretamente o registro correspondente no sistema (SNIPE-IT, 2025c).

Figura 3 – Exemplo de Etiqueta de Ativo



Fonte: Snipe-IT (2025).

Com a etiqueta de ativo, os usuários podem acessar rapidamente informações sobre o equipamento, como histórico de manutenção, registros de empréstimo e devolução, *status* de uso e localização atual, o que simplifica a gestão e o controle dos ativos (SNIPE-IT, 2025b; GOWORKWIZE, 2025). Esse mecanismo contribui para reduzir extravios, agilizar inventários físicos e facilitar a atualização de dados no momento em que o ativo é movimentado dentro da instituição (TECH.CO, 2025; VIRIMA, 2025).

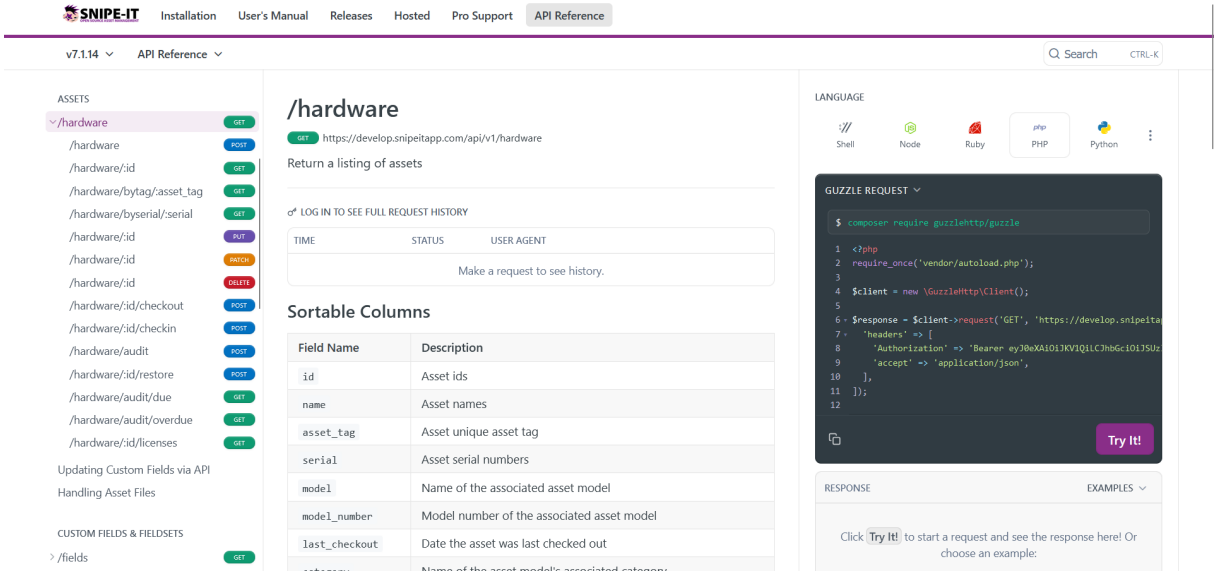
2.2.2 Integrações

Com uma *API*, o *Snipe-IT* permite a integração com outras ferramentas e sistemas, ampliando suas funcionalidades e interoperabilidade (SNIPE-IT, 2025a). Essas integrações podem automatizar processos de cadastro e atualização de ativos, sincronizar dados de usuários com diretórios corporativos (como LDAP e *Active Directory*) e conectar o sistema a soluções externas, como ferramentas de monitoramento, sistemas de *help desk* ou plataformas de emissão de *tickets* (SNIPE-IT, 2025a; GROKABILITY, 2025).

O *Snipe-IT* disponibiliza uma API completa que permite a integração e automação de operações de gestão de ativos de TI. A documentação da API, ilustrada na Figura 4, apresenta endpoints organizados por recursos, incluindo operações para hardware, campos customizados e fieldsets, entre outros.

A API utiliza requisições *Hypertext Transfer Protocol Secure* (HTTPS) padrão (*GET*, *POST*, *PUT*, *PATCH*, *DELETE*) e retorna respostas em formato *JavaScript Object Notation* (JSON). Para autenticação, é necessário um token de acesso (*Bearer token*) que deve ser incluído no cabeçalho das requisições. O *endpoint* `/api/v1/hardware`, por exemplo,

Figura 4 – API Reference



Fonte: Snipe-IT (2025).

permite listar todos os ativos cadastrados no sistema através de uma requisição *GET*, retornando campos sortáveis como `id`, `name`, `asset_tag`, `serial`, `model` e `last_checkout`.

2.2.3 Empréstimos e devoluções

Uma funcionalidade central do *Snipe-IT* é o gerenciamento de empréstimos de ativos a usuários específicos, como professores, técnicos ou alunos, registrando a quem o equipamento foi atribuído e por qual período (SNIPE-IT, 2025c). O sistema permite realizar o *check-out* de um ativo para um usuário ou local, gerar termos de responsabilidade e, posteriormente, registrar o *check-in* na devolução, mantendo um histórico completo dessas movimentações (SNIPE-IT, 2025b; TECH.CO, 2025).

Esse controle formaliza o processo de empréstimo, reduz ambiguidades sobre quem está com determinado equipamento e apoia a responsabilização em casos de danos ou extravio (SNIPE-IT, 2025c; GOWORKWIZE, 2025). Além disso, os registros de empréstimos podem ser utilizados para gerar relatórios de uso, identificando padrões de demanda por certos tipos de ativos e subsidiando decisões de compra ou remanejamento (TECH.CO, 2025).

2.2.4 Relatórios e auditoria

O *Snipe-IT* disponibiliza relatórios configuráveis que permitem acompanhar o inventário por categoria, localização, responsável, *status* e outras variáveis, possibilitando diferentes visões gerenciais sobre os ativos (SNIPE-IT, 2025c). Esses relatórios podem ser exportados em formatos como *Comma Separated Values* (CSV) e *Portable Document Format* (PDF), o que facilita sua utilização em auditorias, prestações de contas e análises internas (SNIPE-IT, 2025b; GOWORKWIZE, 2025).

Em conjunto com as etiquetas e o histórico de movimentação, os relatórios auxiliam na realização de auditorias patrimoniais, conferindo se os ativos registrados no sistema correspondem aos itens encontrados fisicamente na instituição (SNIPE-IT, 2025c; TECH.CO, 2025). Isso contribui para a integridade dos dados e para o atendimento a políticas de governança e conformidade adotadas pela organização (VIRIMA, 2025).

2.2.5 Pontos fortes e limitações do Snipe-IT

Entre os principais pontos fortes do *Snipe-IT*, destaca-se o fato de ser um software livre e de código aberto, sem limitação de número de ativos ou usuários na modalidade auto-hospedada, o que reduz custos e favorece a transparência no tratamento dos dados (SNIPE-IT, 2025c; TECH.CO, 2025). A flexibilidade para personalização de campos, categorias e fluxos, aliada a uma API bem documentada, permite que equipes com conhecimento técnico integrem o sistema a outros serviços e automatizem tarefas recorrentes, como importações em lote e geração de relatórios (SNIPE-IT, 2025a; GOWORKWIZE, 2025).

Outro aspecto positivo está no foco no rastreamento de ativos fixos, com uso de códigos de barras e *QR Codes*, registro de histórico de movimentações e *logs* de auditoria detalhados, que aumentam a responsabilização dos usuários e apoiam processos de conformidade (SNIPE-IT, 2025c; CAPTERRA, 2025). Além disso, a possibilidade de implantação em servidores próprios ou em nuvem, somada a uma comunidade ativa de desenvolvedores, contribui para a evolução contínua da ferramenta (GROKABILITY, 2025; VIRIMA, 2025).

Por outro lado, o *Snipe-IT* apresenta algumas limitações que precisam ser consideradas no planejamento da solução. Entre elas, destacam-se a ausência de recursos nativos de descoberta automática de ativos na rede, o que exige cadastro manual ou importações a partir de outras fontes (TECH.CO, 2025; VIRIMA, 2025), e a inexistência de rastreamento por *GPS*, o que o torna menos adequado a cenários que demandam monitoramento em tempo real de ativos móveis (GOWORKWIZE, 2025).

Também são apontadas como fragilidades o fato de o plano gratuito não incluir suporte oficial (CAPTERRA, 2025), a dependência maior de conhecimento técnico para instalação e customização em ambientes auto-hospedados (TECH.CO, 2025) e a falta de recursos avançados de relatórios e análises quando comparado a soluções comerciais de grande porte (VIRIMA, 2025). Tais limitações, contudo, podem ser mitigadas em contextos institucionais com infraestrutura de TI já estabelecida e equipes capazes de realizar integrações, automatizações e suporte interno ao sistema (GROKABILITY, 2025).

2.2.6 Alternativas e justificativa da escolha do Snipe-IT

No contexto da gestão de ativos de TI, existem diversas soluções que poderiam ser consideradas como alternativas ao *Snipe-IT*, incluindo tanto ferramentas de código aberto quanto plataformas proprietárias (VIRIMA, 2025; NOCOBASE, 2024). Entre os projetos

open source, destacam-se opções como GLPI (GLPI, 2025), openMAINT (OPENMAINT, 2025), Budibase (com *templates* de gestão de ativos) (BUDIBASE, 2025) e NocoBase (NOCOBASE, 2024), enquanto, no campo das soluções comerciais, podem ser mencionados produtos como InvGate Assets (INVGATE, 2025), ManageEngine AssetExplorer (MANAGEENGINE, 2025), SolarWinds (SOLARWINDS, 2025) e ServiceNow (SERVICENOW, 2025).

Ferramentas proprietárias tendem a oferecer módulos integrados de monitoramento, descoberta automática de ativos, *dashboards* analíticos mais sofisticados e suporte técnico formalizado, mas, em contrapartida, normalmente envolvem custos de licenciamento e assinatura que podem ser elevados para instituições educacionais de pequeno e médio porte (TECH.CO, 2025; GROWRK, 2025). Já algumas alternativas *open source* apresentam maior complexidade de configuração ou foco em escopos mais amplos (como gestão de serviços ou *facilities*), o que pode adicionar camadas de funcionalidade não essenciais ao objetivo específico deste trabalho (VIRIMA, 2025; NOCOBASE, 2024).

A escolha do Snipe-IT para este projeto fundamentou-se em três eixos principais: aderência funcional ao problema identificado, viabilidade econômica e alinhamento com a infraestrutura tecnológica existente na instituição (SNIPE-IT, 2025c). Do ponto de vista funcional, o Snipe-IT atende de forma direta às necessidades de rastreabilidade de ativos, controle de empréstimos, registro de histórico e geração de relatórios básicos, sem exigir aquisição de módulos adicionais (SNIPE-IT, 2025c; TECH.CO, 2025). Em termos de custos, a possibilidade de implantação auto-hospedada, sem cobrança de licenças por usuário ou por ativo, mostrou-se compatível com as restrições orçamentárias da escola (GOWORKWIZE, 2025).

Por fim, a disponibilidade de imagens oficiais baseadas em contêineres, documentação acessível e integração nativa com diretórios como *LDAP*/*Active Directory* contribuiu para que o Snipe-IT pudesse ser incorporado à arquitetura já existente, reduzindo o esforço de implantação e manutenção contínua (SNIPE-IT, 2025a). Esses fatores justificam a adoção do Snipe-IT como solução central de gestão de ativos de TI neste trabalho, ao mesmo tempo em que evidenciam sua contribuição prática em relação à literatura e às demais ferramentas analisadas.

2.3 Infraestrutura

A infraestrutura constitui o conjunto de recursos físicos e lógicos que sustentam a comunicação de dados em uma organização, abrangendo *switches*, roteadores, cabeamento estruturado e serviços essenciais como *DHCP* e segmentação por *VLANs* (Tanenbaum *et al.*, 2021). No contexto educacional, essa infraestrutura deve garantir conectividade estável para laboratórios e serviços administrativos (Kurose; Ross, 2021). A segmentação lógica por *VLANs* e *DHCP* são práticas consolidadas para otimizar segurança e eficiência.

2.3.1 Windows Server

O *Windows Server* é um sistema operacional desenvolvido pela *Microsoft* para servidores e ambientes corporativos. Ele oferece uma ampla gama de recursos e serviços para suportar as operações de TI, incluindo gerenciamento de usuários, armazenamento de dados, segurança de rede e virtualização. O *Windows Server* é amplamente utilizado em empresas de todos os portes devido à sua confiabilidade, escalabilidade e integração com outras tecnologias da *Microsoft* (Microsoft, 2025a).

Perante a isso, é importante destacar algumas das principais funcionalidades do *Windows Server* que são relevantes para o gerenciamento de ativos de TI.

2.3.1.1 Active Directory

Para o gerenciamento de usuários, grupos e permissões, o Active Directory *(AD)* é uma ferramenta essencial do *Windows Server*. Ele centraliza a administração de recursos de rede, simplifica a autenticação e autorização de usuários e garante a segurança dos dados. O *AD* é amplamente utilizado em ambientes corporativos para facilitar o gerenciamento de identidades e acessos (Microsoft, 2025c).

2.3.1.2 Microsoft Entra ID

Com a existência das credenciais de forma online e offline, o *Microsoft Entra ID* é uma ferramenta que permite a autenticação de usuários em diferentes dispositivos e serviços da *Microsoft*. Ele oferece uma experiência de login unificada e segura, permitindo que os usuários acessem seus recursos de forma conveniente e protegida. Sendo essencial para a integração de serviços e aplicativos da *Microsoft* (Microsoft, 2025d).

2.3.1.3 Linux

Linux é um sistema operacional de código aberto baseado no *kernel Linux*. Ele é amplamente utilizado em servidores, dispositivos embarcados e sistemas embarcados devido à sua estabilidade, segurança e flexibilidade. O *Linux* oferece uma ampla gama de distribuições e ferramentas que atendem às necessidades de diferentes usuários e organizações (Die.net, 2025).

2.3.1.4 Máquina Virtual

Máquina Virtual (VM) é uma solução utilizada para simular um ambiente computacional completo, permitindo a execução de sistemas operacionais e aplicativos como se estivessem sendo executados em um hardware físico. Os recursos virtuais atribuídos a uma *VM* incluem CPU, memória, armazenamento e interface de rede (Hat, 2024a).

Em ambientes baseados em *Linux*, a Kernel-based Virtual Machine *(KVM)* destaca-se como uma das tecnologias de virtualização mais utilizadas. Trata-se de uma solução de

código aberto incorporada ao *kernel* do *Linux*, que permite ao Sistema Operacional (SO) atuar como um hipervisor nativo, com capacidade de gerenciar diversas *VM*s isoladas (Hat, 2024b)

2.3.1.5 Docker

O *Docker* é uma plataforma voltada para o empacotamento, distribuição e execução de aplicações em ambientes isolados, conhecidos como contêineres. Esses contêineres incluem tudo o que a aplicação precisa para rodar (como bibliotecas e dependências), garantindo que ela funcione de forma consistente em qualquer infraestrutura (Docker, Inc., 2025). Por ser leve e portátil, o *Docker* simplifica o desenvolvimento e a implantação de *software*.

Utiliza, também, uma arquitetura cliente-servidor, isso significa que cliente o *Docker* envia comandos ao *daemon*(*dockerd*), que é responsável por gerenciar imagens, contêineres, redes e volumes. As aplicações são construídas a partir de imagens descritas em um *Dockerfile*, enquanto os contêineres correspondem às instâncias executáveis dessas imagens (Docker, Inc., 2025).

2.4 Protocolos de Rede

Para a implementação de soluções de gerenciamento de ativos de TI, é fundamental compreender os protocolos de rede que permitem a comunicação e o compartilhamento de informações entre dispositivos e sistemas. Esses protocolos estabelecem regras e padrões para a transmissão de dados, garantindo a interoperabilidade e segurança das redes (Jusak; Sukmaaji, 2009).

2.4.1 SSH

O Secure Shell *(SSH)* é um protocolo de rede que permite a comunicação segura entre dispositivos por meio de uma conexão criptografada. Ele é amplamente utilizado para acessar servidores remotos, transferir arquivos e executar comandos de forma segura. O *SSH* utiliza criptografia assimétrica para autenticação e criptografia simétrica para proteger os dados transmitidos. Sendo assim, o uso para gerenciamento e adoção dos ativos de rede é essencial (Roberts, 2019).

2.4.2 SNMP

Utiliza-se o protocolo Simple Network Management Protocol *(SNMP)* para monitoramento e gerenciamento de dispositivos de rede. Ele permite que os administradores coletem informações sobre o desempenho, *status* e configuração dos dispositivos, facilitando a detecção de falhas, otimização de recursos e planejamento de capacidade (Tanenbaum; Wetherall, 2011).

2.4.3 SMTP

O protocolo Simple Mail Transfer Protocol *(SMTP)* é utilizado para envio de e-mails e comunicação entre servidores de e-mail. Ele define as regras para o envio, recebimento e encaminhamento de mensagens eletrônicas, garantindo a entrega segura e confiável dos e-mails. O *SMTP* é essencial para a comunicação interna e externa pela *internet* (Tanenbaum; Wetherall, 2011).

2.4.4 VNC

O Virtual Network Computing *(VNC)* é um protocolo de rede que permite o acesso remoto a computadores e dispositivos por meio de uma conexão segura. Ele é amplamente utilizado para suporte técnico, administração remota e colaboração em equipe. O *VNC* oferece uma interface gráfica para controlar o dispositivo remoto, facilitando a interação e o compartilhamento de informações (Tanenbaum; Wetherall, 2011).

2.5 Tecnologias

As tecnologias de contêineres representam paradigmas modernos na arquitetura de software, permitindo isolamento de aplicações e portabilidade (Romero, 2015). O *Docker* facilita a implantação padronizada de serviços, enquanto protocolos *LDAP*/*Active Directory* centralizam a autenticação (Alencar, 2010). Essas tecnologias foram selecionadas por sua maturidade em gerenciamento de ativos educacionais.

2.5.1 Python

Segundo Silva e Silva (2019), *Python* é uma linguagem de programação descomplicada, criada para favorecer o desenvolvimento ágil de *software*. Por ser de alto nível e próxima da compreensão humana. *Python* é amplamente utilizada em diversas áreas, como ciência de dados, inteligência artificial, automação de tarefas e desenvolvimento *web*. Sua sintaxe clara e concisa facilita a leitura e manutenção do código, tornando-a uma escolha popular entre desenvolvedores e cientistas de dados. (Carvalho, 2023)

2.5.2 PowerShell

O *PowerShell* é uma solução multiplataforma de automação desenvolvida pela *Microsoft*, que incorpora em sua constituição *shell* de linha de comando, linguagem de *script* e estrutura de configuração. Opera com objetos .NET, o que permite a manipulação de objetos e a automação de tarefas administrativas em sistemas operacionais *Windows*. (Microsoft, 2025f)

De acordo com a Microsoft (2025f), "Como uma linguagem de *script*, o *PowerShell* é normalmente usado para automatizar o gerenciamento de sistemas. Ele também é usado

para compilar, testar e implantar soluções, geralmente em ambientes de Continuous Delivery/Continuous Integration *(CD/CI)*". Isso indica que a ferramenta é poderosa para acelerar processos de desenvolvimento e operações, reduzindo erros manuais e aumentando a eficiência.

2.5.3 MySQL

MySQL representa um Sistema de Gerenciamento de Banco de Dados Relacional (SGBDR) elaborado sob licença de código aberto, que é usado para armazenar, estruturar e recuperar dados em diversos contextos. O modelo utilizado é o de cliente/servidor, o que permite que múltiplos usuários acessem e manipulem os dados simultaneamente (Cardoso, 2023).

Essa tecnologia é baseada na linguagem chamada *Structured Query Language* (SQL), por isso ela manipula as informações em um modelo disposto em tabelas organizadas por linhas e colunas. Com isso, a criação de esquemas relacionais e vínculos entre tabelas é facilitada. Alguns de seus destaques incluem controle de acesso, segurança, desempenho estável e facilidade de uso (Erickson, 2024).

Erickson (2024) ainda afirma que sua popularidade se deve aos seus destaques, além de uma comunidade ativa e da confiabilidade do sistema ao ser utilizado por grandes empresas como o *Facebook, AirBnb* e *Booking.com*.

2.5.4 Microsoft Visual Studio Code

O *Visual Studio Code* (VS Code) é um editor de código-fonte produzido pela *Microsoft*, leve, multiplataforma *Windows, Linux* e *macOS* e de código aberto. Possui suporte a diversas linguagens de programação, como *Python, JavaScript, TypeScript*, C++, entre outras. Além disso, conta com uma vasta gama de extensões que permitem personalizar e expandir suas funcionalidades, tornando-o uma ferramenta versátil para desenvolvedores (Jasiulionis, 2025).

Seu foco em produtividade e eficiência, aliado a recursos como depuração integrada, controle de versão e suporte a desenvolvimento colaborativo, fazem do *VS Code* uma escolha popular entre programadores e equipes de desenvolvimento em todo o mundo (Microsoft, 2025g).

2.5.5 Microsoft Forms

O *Microsoft Forms* é uma ferramenta da *Microsoft 365* que cria formulários, questionários, testes e enquetes, possui recursos de coleta de respostas em tempo real e visualização por meio de gráficos. É possível personalizar o *design* dos formulários, adicionar imagens e vídeos, adicionar lógica de ramificação, contém colaboração em equipe, exportação de dados e integração com outros serviços da *Microsoft* (Microsoft, 2025b).

É possível acessar a plataforma por meio de navegadores *web* e dispositivos móveis,e está disponível para contas pessoais e empresariais. Esses formulários podem ser compartilhados tanto internamente quanto externamente, com controle de acesso e suporte multilíngue. Por seguir normas de segurança e privacidade, o *Microsoft Forms* é amplamente utilizado em ambientes educacionais e corporativos para coleta de dados e *feedback* (Microsoft, 2025e).

2.5.6 Lucidchart

O *Lucidchart* é uma plataforma *online* de diagramação inteligente baseada em nuvem, desenvolvida para facilitar a visualização de processos, fluxos de trabalho e estruturas organizacionais de maneira dinâmica e colaborativa. Nela é possível criar fluxogramas, mapas conceituais, organogramas, diagramas Unified Modeling Language *(UML)*, entre outros. Sua principal função é transformar informações complexas em representações visuais interativas, permitindo que equipes visualizem dados, alinhem estratégias e tomem decisões com maior agilidade (Inc., 2025).

2.6 Estatística Aplicada à Pesquisa Científica

A estatística aplicada desempenha um papel indispensável para a análise de dados em pesquisas científicas, fornecendo ferramentas e métodos para interpretar informações qualitativas de forma eficaz. Segundo Morettin (2023), a estatística aplicada é essencial para a coleta, organização, análise e interpretação de dados, permitindo que pesquisadores extraiam conclusões significativas e fundamentadas. Larson (2023) complementa dizendo que qualquer decisão baseada em resultados estatísticos depende da qualidade do planejamento, coleta e análise.

Pensando na análise, conceitos como os de distribuição de frequência e frequência relativa, apresentados e instruídos por Field (2018), são fundamentais para compreender a distribuição dos dados e identificar padrões. Dessa maneira, os dados podem ser organizados de maneira clara e sucinta, facilitando a visualização e interpretação dos resultados.

2.7 Requisitos de *software*: Abordagens e Aplicações

Para construir um sistema que atenda efetivamente às necessidades do usuário e do seu negócio, Vazquez e Simões (2016) destacam que o analista de requisitos deve atuar de forma objetiva, com foco na elaboração estruturada dos processos de requisitos. Essa abordagem converge com a perspectiva de Ledur (2018), que propõe um processo ordenado para a coleta e definição de requisitos .

Para que uma especificação de requisitos seja considerada correta, é necessário que cada requisito atenda, no mínimo, a uma necessidade legítima do negócio. Essa

exigência é reforçada por Vazquez e Simões (2016), que enfatizam a importância do alinhamento entre os requisitos documentados e as demandas reais da organização.

Além disso, conforme aponta Ledur (2018), o estudo de viabilidade representa a etapa inicial do processo de desenvolvimento, sendo responsável por verificar se a construção do produto de *software* é viável sob a ótica organizacional, funcional e técnica. Esse estudo fundamenta o projeto e assegura o alinhamento com os objetivos institucionais.

Nesse contexto, após o estudo de viabilidade, seguem-se as etapas de coleta de requisitos, especificação dos requisitos de *software* e validação desses mesmos requisitos (Ledur, 2018). Vazquez complementa afirmando que a forma final do *software* será reflexo direto do processo de comunicação entre usuário e sistema, até que os objetivos específicos sejam integralmente alcançados (Vazquez; Simões, 2016). Esse processo é essencial para a identificação e o refinamento de todos os tipos de requisitos reconhecidos pelas partes interessadas.

Diante disso, os autores apresentam técnicas apropriadas para a elicitação de requisitos. Embora diversas abordagens possam ser utilizadas, este trabalho concentrar-se-á na entrevista e no questionário. A entrevista é definida como “uma forma de diálogo, formal ou informal, entre duas ou mais pessoas, na qual o entrevistador busca respostas para um conjunto de questões previamente planejadas, e os entrevistados se apresentam como fontes de informação” (Vazquez; Simões, 2016). Já o questionário permite obter, de maneira rápida, informações qualitativas e quantitativas junto ao público-alvo, sendo particularmente útil para a padronização da coleta de dados.

2.7.1 Requisitos Funcionais

Os requisitos funcionais representam o núcleo comportamental do sistema, descrevendo as funcionalidades que o *software* deve executar. Segundo Vazquez e Simões (2016, p. 104), “os requisitos funcionais descrevem o comportamento que o *software* deve ter em termos das tarefas ou serviços do usuário”.

O comportamento esperado pelo *software*, ao ser definido em um requisito funcional, refere-se ao intercâmbio de informações entre o usuário, o sistema em questão e os meios de armazenamento, até que um objetivo específico seja alcançado. Esse objetivo — geralmente relacionado à realização de uma tarefa atribuída ao usuário — permite que seus resultados possam ser utilizados como insumo em outras tarefas, por diferentes usuários ou em outros momentos (Vazquez; Simões, 2016).

De forma complementar, Ledur esclarece que os requisitos funcionais definem o que o sistema deve realizar, sendo usualmente expressos na forma de “o sistema deve <requisito>”, especificando uma ação individual de parte do sistema, como uma função matemática, uma saída, um processo ou um modelo funcional de controle (Ledur, 2018).

2.7.2 Requisitos Não Funcionais

Os requisitos não funcionais atuam como complemento à especificação funcional, pois definem critérios de qualidade e restrições que o sistema deve seguir para além do simples funcionamento. De acordo com Vazquez e Simões (2016, p. 111), eles descrevem limitações gerais aplicáveis aos requisitos funcionais, tornando a especificação do *software* mais completa. Afinal, não basta que o sistema apenas funcione; é essencial que funcione bem.

Ao detalhar o que significa esse "funcionar bem", percebe-se que os requisitos não funcionais estabelecem os níveis de serviço esperados para o *software*. Diferentemente dos requisitos funcionais, que se concentram em tarefas específicas do usuário, os não funcionais abrangem restrições gerais que impactam aspectos como desempenho, segurança, usabilidade e confiabilidade do sistema.

Ledur (2018) reforça que os requisitos não funcionais especificam critérios para avaliar o funcionamento do sistema, e não comportamentos específicos. Eles se diferenciam dos requisitos funcionais justamente por estarem relacionados a propriedades gerais, como desempenho ou confiabilidade, sendo normalmente expressos na forma: "o sistema deve ser <requisito>" .

2.7.3 Diagrama de Atividade

Na obra *UML 2: uma abordagem prática*, Guedes (2018) explica o diagrama de atividade como uma ferramenta visual que demonstra os passos necessários para a conclusão de uma atividade específica. Seu objetivo é representar o fluxo de trabalho dessa atividade.

Esse tipo de modelagem pode ser utilizado para representar processos organizacionais (como etapas de engenharia de processos e *workflows*) ou processos de sistema (como a especificação de processos). Em ambos os casos, tais diagramas auxiliam no detalhamento da lógica por trás de um caso de uso, contribuindo para a compreensão, análise da complexidade e validação de que o caso de uso corresponde à funcionalidade desejada (Guedes, 2018).

O autor ainda afirma que "É mais comum que um diagrama de atividade represente uma única atividade; todavia, é possível que um diagrama contenha mais de uma delas, caso isso seja considerado necessário" (Guedes, 2018, p. 409).

2.8 Governança de Ativos de TI

Algumas vezes os termos governança e gestão de ativos são usados de forma semelhante, mas, no contexto organizacional, possuem significados distintos. A gestão de ativos refere-se ao trabalho operacional: controlar, manter e rastrear os recursos, conforme discutido na seção 2.1.

Já a governança preocupa-se com o nível estratégico: ela define o que se decide, como se decide, quais processos são legítimos e quais normas e padrões devem ser observados, de modo que essas decisões protejam os objetivos institucionais. Por isso, a gestão foca em como fazer, enquanto a governança trata do por que fazer, do para que fazer e de quem é o responsável (Vieira, 2014; Zampolli *et al.*, 2019).

Esse caráter estratégico é fundamental para orientar decisões sobre aquisição, manutenção, atualização e descarte de recursos tecnológicos, garantindo que essas escolhas estejam alinhadas com os objetivos da organização, que os recursos sejam usados de forma eficiente e que o patrimônio institucional seja protegido.

De acordo com Weill e Ross (2004), uma governança eficiente depende da definição clara de responsabilidades em cinco áreas fundamentais: princípios de TI, arquitetura, infraestrutura, necessidades de aplicações e investimentos. Os autores sugerem modelos que podem ser adaptados ao contexto e ao nível de maturidade da organização, sempre reforçando a importância de alinhar a TI às áreas de negócio. Ao definir quem pode decidir e em qual nível, reduzem-se ambiguidades e fortalece-se a transparência.

A governança de ativos de TI deve orientar-se por padrões e normas internacionais que consagram boas práticas. Entre esses documentos está a Associação Brasileira de Normas Técnicas (ABNT) Norma Brasileira (NBR) *ISO* 55001, que oferece uma estrutura para criar políticas, planejar, operar, avaliar e promover a melhoria contínua dos ativos ao longo de seu ciclo de vida (Zampolli *et al.*, 2019). Complementarmente, a *ISO*/*IEC* 27001 define requisitos de segurança da informação para garantir confidencialidade, integridade e disponibilidade Técnicas (2013). A série *ISO*/*IEC* 19770 trata de métodos específicos, como inventário, auditoria de software e gerenciamento de licenças, incentivando transparência e controle dos ativos (ISO, 2017). A integração dessas normas fortalece a instituição ao promover processos rastreaveis, padronizados e alinhados às melhores práticas internacionais.

No plano prático, Vieira (2014) aponta que, no contexto educacional, a governança exige funções bem definidas, processos estruturados e monitoramento constante, sobretudo em ambientes com alta rotatividade de usuários.

No setor público, Marchiori *et al.* (2023a) destaca que uma gestão de ativos adequada é essencial para a inovação e adaptação institucional; em ambientes mais burocráticos e com estruturas rígidas, a reconfiguração da TI e a coordenação entre setores dependem diretamente de práticas sólidas de governança. Pereira (2016), ao estudar uma empresa de telecomunicações, corrobora a ideia de que o controle de ativos vinculado a processos bem estabelecidos reduz custos, melhora o desempenho operacional e promove maior sustentabilidade dos recursos — conclusões aplicáveis tanto ao setor público quanto a instituições de ensino.

A reunião desses conceitos teóricos, normativos e práticos embasa a metodologia adotada neste estudo. Assim, é possível construir um sistema de gestão de ativos alinhado às práticas de governança, sustentável e ajustado às melhores práticas internacionais.

3 METODOLOGIA

Diante dos conceitos e ferramentas abordados na fundamentação teórica, torna-se possível estabelecer uma estrutura prática para aplicar a proposta na realidade institucional analisada. A seguir, será apresentada a metodologia adotada, que detalha as etapas do estudo, as técnicas de coleta de dados utilizadas e os instrumentos desenvolvidos para subsidiar a implementação do sistema.

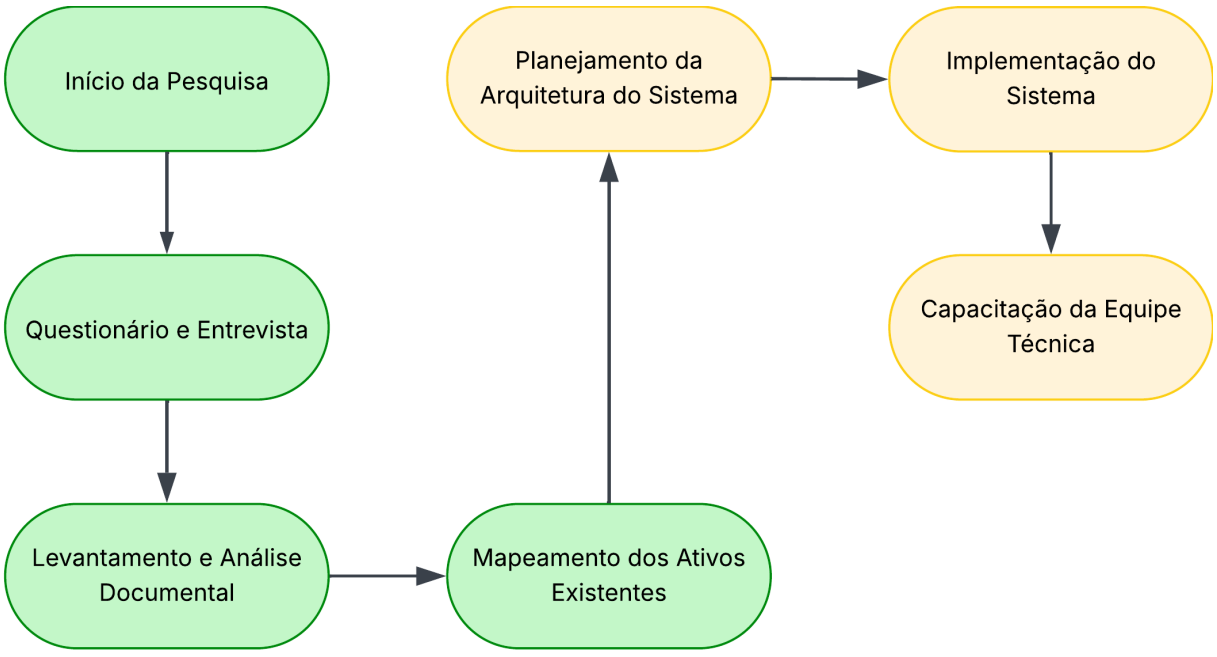
A presente pesquisa seguiu uma abordagem prática voltada à identificação e solução de falhas no gerenciamento de ativos de Tecnologia da Informação (TI) em uma instituição educacional. As atividades metodológicas foram organizadas em etapas sequenciais, envolvendo desde o levantamento da situação atual até a implementação e avaliação de um sistema informatizado de controle de inventário, com base no *software* livre *Snipe-IT* e *scripts* personalizados.

3.1 Etapas Metodológicas

A condução da pesquisa compreende as seguintes etapas:

1. Aplicação de questionário e entrevistas com os principais usuários e equipe técnica;
2. Levantamento e análise documental da infraestrutura de TI da instituição;
3. Mapeamento, catalogação e documentação dos ativos de TI existentes;
4. Planejamento da arquitetura do sistema a ser implantado;
5. Capacitação dos usuários finais e treinamento para utilização do sistema;

Figura 5 – Fluxograma das Etapas Metodológicas



Fonte: Elaborado pelo autor (2025).

3.1.1 Ferramentas e Tecnologias

- Software de código aberto **Snipe-IT**;
- **Máquina Virtual (VM)**;
- ***Docker*** e ***Docker Compose***;
- Banco de dados ***MySQL***;
- *Scripts* personalizados em ***Python*** e ***PowerShell***;
- Integração com ***Active Directory*** e **Application Programming Interface *(API)***;
- Ferramentas de coleta de dados (formulários e entrevistas);
- Planilhas CSV para inventário inicial e importação automatizada de dados.

3.1.2 Delimitação do Estudo

A pesquisa está limitada ao escopo da rede interna da instituição analisada, abrangendo apenas ativos eletrônicos fixos (computadores, impressoras, servidores, switches e roteadores). Equipamentos móveis e itens de uso pessoal que não constam nos registros oficiais da instituição foram excluídos do estudo.

3.2 Levantamento e Coleta de Dados

O diagnóstico inicial da infraestrutura de rede da instituição foi realizado por meio da análise da documentação técnica previamente existente. É importante ressaltar que **toda a topologia de rede, incluindo a segmentação por *Virtual Local Area Network* (VLAN) e a organização dos dispositivos, já havia sido implementada e estava em pleno funcionamento antes do início deste projeto**. A documentação analisada apresenta um panorama básico dessa infraestrutura preexistente, que organiza dispositivos como computadores, impressoras, servidores, câmeras de vigilância e telefones com tecnologia *Voice over IP* (VoIP) por meio de redes locais virtuais. A segmentação por *VLAN* é uma prática comum para aumentar a segurança e a eficiência da rede (Tanenbaum; Wetherall, 2011).

Entretanto, uma análise minuciosa dessa documentação revelou inconsistências e lacunas que comprometem a confiabilidade das informações catalogadas, dificultando a identificação precisa e o controle eficaz dos ativos. Esse cenário infringe diretrizes fundamentais da gestão de serviços de TI segundo o Information Technology Infrastructure Library *(ITIL)*, afetando a rastreabilidade e o alinhamento entre infraestrutura e serviços (AXELOS, 2019).

A Figura 6 apresenta um exemplo da documentação preexistente que mapeia a estrutura de rede já implementada na instituição, enquanto a Figura 7 ilustra uma amostra da configuração de VLAN em um *switch*, também previamente configurado. **Ambas as figuras representam o estado atual da infraestrutura encontrada no início deste trabalho, não tendo sido implementadas ou configuradas durante este projeto**. Apesar de represen-

tarem uma base mínima de controle, tais registros carecem de padronização, atualização e detalhamento técnico suficiente, reforçando a necessidade de um levantamento mais abrangente e sistemático que justifica a implementação de um sistema de gestão de ativos.

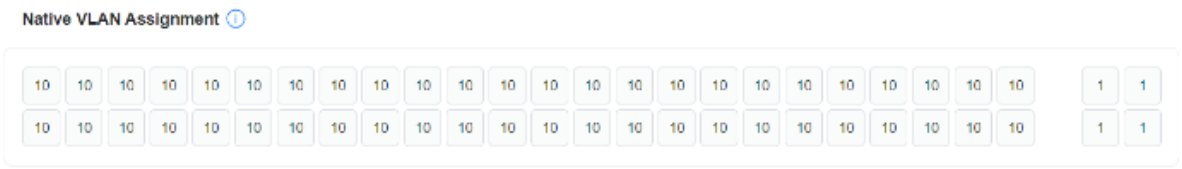
Figura 6 – Tabela Escopo da Rede

Nome	Rede	Vlan
Rede Lan	192.168.0.0/24	1
Rede Câmeras	192.168.1.0/24	10
Rede Diretoria	192.168.2.0/24	20
Rede Professores	192.168.3.0/24	30
Rede Funcionários	192.168.4.0/24	40
Rede Visitantes	192.168.5.0/24	50
Rede Telefonia	192.168.6.0/24	60
Rede Catraca	192.168.7.0/24	70

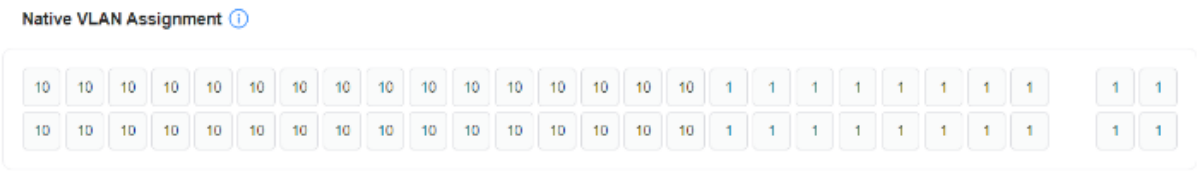
Fonte: Documentação existente na instituição (2025).

Figura 7 – Configuração de VLANs no *switch*

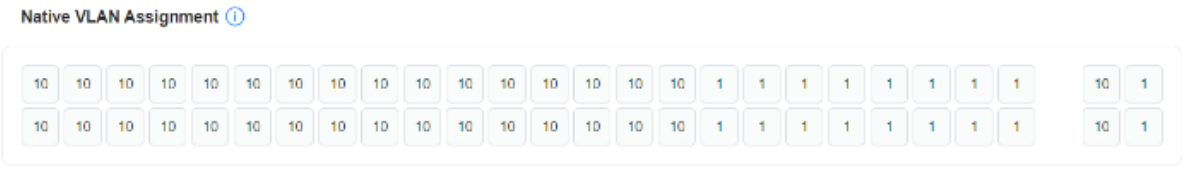
SW01



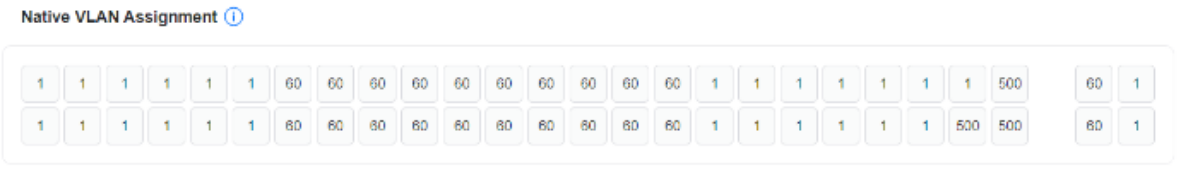
SW02



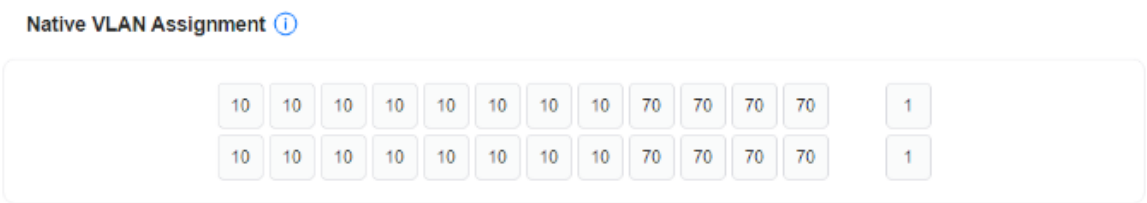
SW03



SW04



SW05



Fonte: Documentação existente na instituição (2025).

A infraestrutura de rede da instituição já possuía uma segmentação lógica imple-

mentada através de VLANs, conforme apresentado na Tabela 6. Esta configuração organiza os diferentes segmentos da rede escolar em sete VLANs distintas, cada uma com seu endereçamento e identificador específico.

Para complementar o levantamento documental, foram adotadas duas estratégias metodológicas principais: aplicação de questionário estruturado e realização de entrevistas semiestruturadas. O questionário foi desenvolvido com base na norma International Organization for Standardization *(ISO)* 55002:2018, nas diretrizes metodológicas de Cervo, Bervian e Silva (Cervo *et al.*, 2006), e na obra *Gestão de Estoques* de Bráulio Wilker Silva (2019).

Optou-se pela aplicação autoadministrada, sem a presença do pesquisador, conforme a orientação metodológica de que “o questionário, sem a presença do investigador, é preenchido pela pessoa que fornece as informações” (Cervo *et al.*, 2006, p. 168). Essa abordagem permite maior padronização na coleta e reduz possíveis vieses, favorecendo a obtenção de dados mais objetivos e representativos. Segundo os autores, “o questionário é a forma mais usada para coletar dados, pois possibilita medir com mais exatidão o que se deseja” (Cervo *et al.*, 2006, p. 168).

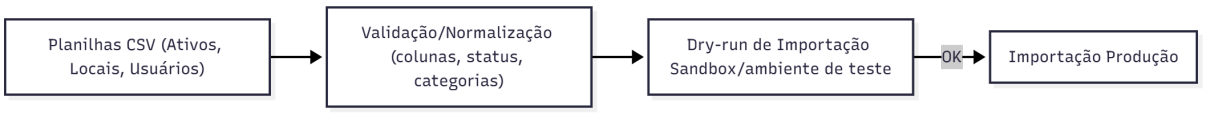
Além disso, entrevistas semiestruturadas foram conduzidas com membros da equipe técnica da instituição para levantar os requisitos funcionais e não funcionais do sistema de gestão de ativos. Essa etapa seguiu as boas práticas descritas por Vazquez e Simões (Vazquez; Simões, 2016), que enfatizam a importância da elicitação orientada ao negócio, considerando as premissas, restrições e alinhamento com os objetivos organizacionais.

A identificação precoce das regras de negócio e das necessidades operacionais visa garantir que o sistema proposto — a ser implementado no *Snipe-IT* — esteja adequadamente ajustado à realidade institucional. Os dados coletados foram organizados e validados junto aos *stakeholders*, em conformidade com as práticas do *ITIL*, que reforça a importância da gestão eficaz de ativos para a continuidade e a confiabilidade dos serviços de TI (AXELOS, 2019).

3.3 Mapeamento de Ativos

O mapeamento de ativos será realizado com base na documentação existente e em entrevistas com a equipe técnica. Será elaborado um inventário, consolidado em uma planilha no formato Comma Separated Values *(CSV)*, que servirá como base para a importação automatizada de dados no *Snipe-IT*. A planilha incluirá informações como marca, quantidade, data de aquisição e valor contábil dos ativos.

Figura 8 – Mapeamento de Ativos de TI CSV



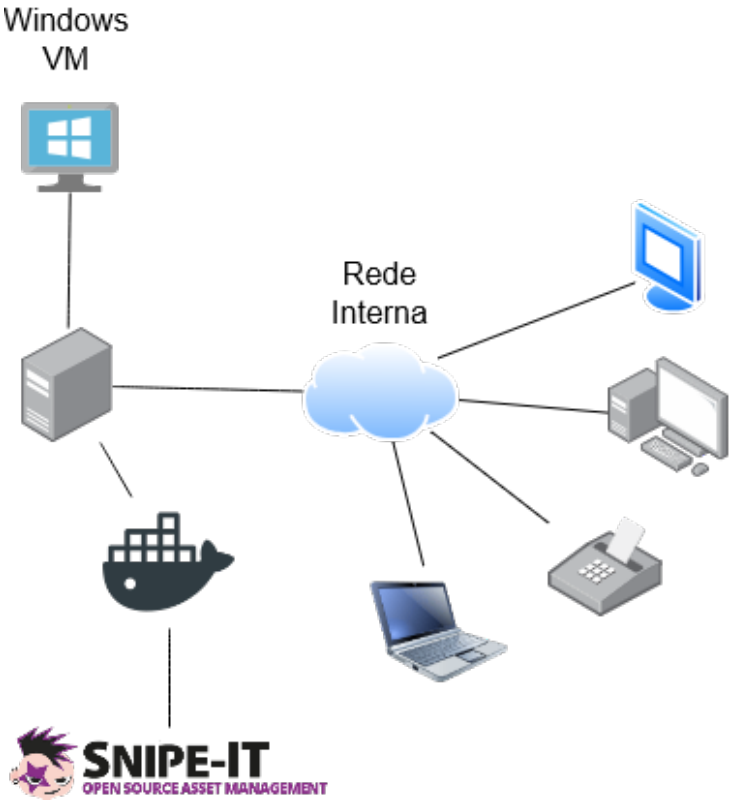
Fonte: Elaborado pelo autor (2025).

3.4 Planejamento da Arquitetura do Sistema

Nesta fase de configuração, o sistema será implantado em um servidor local com especificações técnicas compatíveis, considerando aspectos fundamentais como *backup*, segurança e escalabilidade. Para simplificar o processo de instalação e configuração do *Snipe-IT*, será utilizada a *VM*.

Considerando os recursos de integração e personalização oferecidos pelo *Snipe-IT*, incluindo a integração com o Active Directory *(AD)*, o sistema será configurado de forma a atender às demandas específicas da instituição.

Figura 9 – Diagrama de Implementação do Ambiente de Produção



Fonte: Elaborado pelo autor (2025).

A Figura 9 ilustra a arquitetura de implantação do sistema *Snipe-IT* na infraestrutura de rede da instituição. O ambiente foi implementado utilizando uma máquina virtual Windows como servidor central, conectada à rede interna da organização.

Após a finalização da configuração do sistema, será realizada a importação dos ativos de TI, bem como dos usuários e locais. Também serão ajustados os campos personalizados, categorias e os respectivos status dos ativos.

3.5 Implementação e Treinamento

A implementação do *Snipe-IT* na instituição seguirá um cronograma estruturado, priorizando a personalização do sistema através de *scripts* e extensões específicas desenvolvidas para atender às demandas identificadas no levantamento inicial. Durante esta fase, serão configurados os elementos fundamentais do sistema, incluindo categorias de ativos, centros de custo, cadastro de usuários e definição de permissões de acesso, além da integração com as ferramentas já consolidadas no ambiente técnico da instituição. Essa personalização possibilitará o alinhamento do sistema com as características operacionais específicas da organização, proporcionando maior eficiência e controle na administração patrimonial.

Simultaneamente, será implementado um programa de capacitação direcionado à equipe técnica e aos usuários estratégicos, enfatizando o domínio das funcionalidades do sistema e a maximização de seu potencial. A capacitação contemplará um treinamento, desenvolvimento de materiais instrucionais e acompanhamento sistemático durante a fase de transição. A meta central consiste em assegurar uma migração harmoniosa e produtiva para a nova plataforma, reduzindo resistências organizacionais e falhas operacionais, enquanto se promove a autonomia dos usuários na gestão eficiente do patrimônio institucional.

4 DESENVOLVIMENTO

Com a metodologia definida e o planejamento das ações estruturado, o trabalho avança para a etapa de desenvolvimento. Neste capítulo, são apresentados os dados coletados, as análises realizadas com base nas respostas obtidas e a organização das informações que servirão de base para as futuras etapas de implantação e personalização do sistema.

4.1 Análise Estatística

A pesquisa contou com a participação de 17 colaboradores da instituição, divididos em setores administrativos, técnicos e corpo docente — sendo este último a maioria entre os respondentes. Essa diversidade fortalece a análise, pois permite uma leitura coletiva das percepções institucionais.

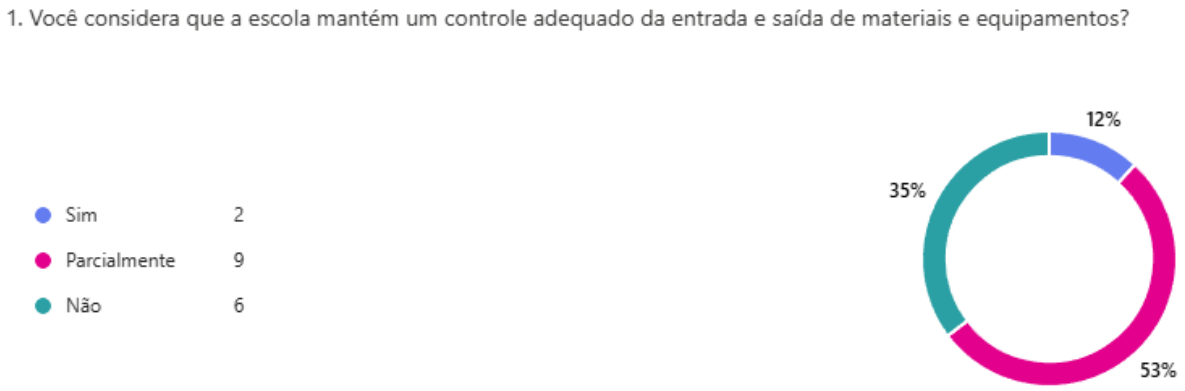
De acordo com artigo publicado na *Revista Internacional de Debates da Administração & Públicas*, os autores Silva e Pereira (2022) afirmam que decisões construídas de forma compartilhada tendem a gerar maior senso de equipe e clareza nos objetivos comuns, o que contribui para o avanço dos processos institucionais de maneira integrada e eficaz.

Pensando nisso, e em como um questionário poderia ser respondido por pessoas com diferentes níveis de conhecimento técnico, foi elaborado um *forms* com 21 perguntas. Essas perguntas estão divididas em um segmento geral e outro específico para as áreas de atuação dos respondentes.

A seguir, apresenta-se uma análise dos dados coletados, destacando as principais informações obtidas:

Os dados revelam deficiências críticas no controle de materiais e equipamentos. Conforme a Figura 10, apenas 12% dos respondentes consideram que a escola mantém controle adequado, enquanto 53% indicam controle parcial e 35% afirmam não existir controle adequado.

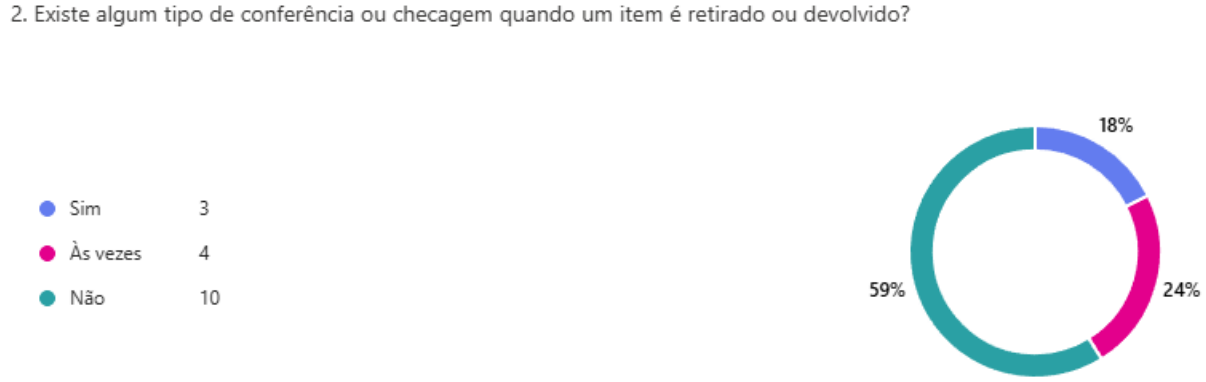
Figura 10 – Controle de entrada e saída de materiais



Fonte: Dados da pesquisa (2025).

A análise revela fragilidades críticas nos processos de conferência. Conforme demonstrado na Figura 11, 82% dos respondentes indicam que não existe ou existe apenas às vezes algum tipo de conferência quando itens são retirados ou devolvidos.

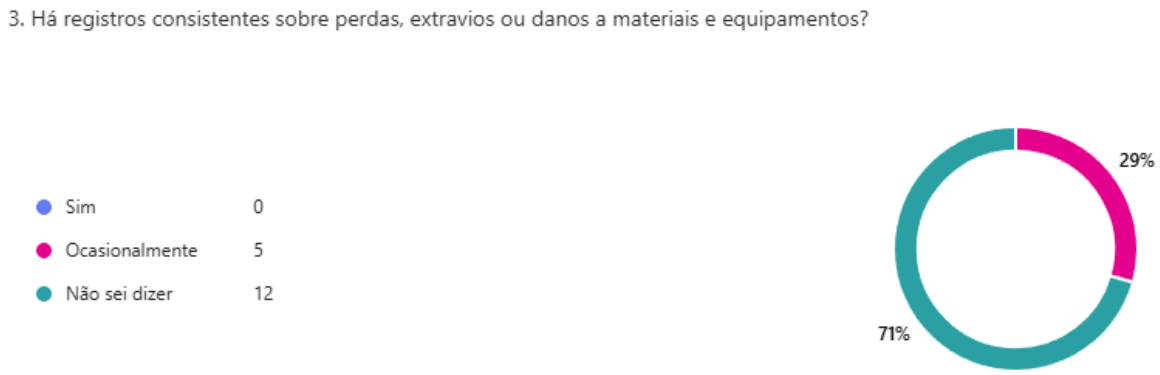
Figura 11 – Conferência na retirada/devolução de itens



Fonte: Dados da pesquisa (2025).

Os registros sobre perdas, extravios ou danos apresentam ausência quase total de controle. A Figura 12 demonstra que 71% dos respondentes não sabem informar sobre a existência desses registros, evidenciando falta completa de transparência no processo.

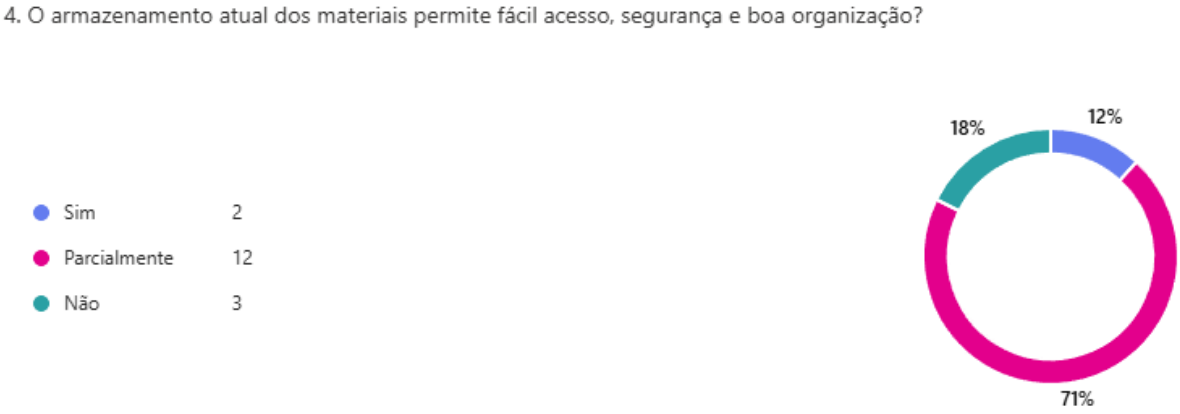
Figura 12 – Registros de perdas, extravios ou danos



Fonte: Dados da pesquisa (2025).

Os dados sobre armazenamento revelam deficiências significativas. Apenas 12% dos respondentes consideram que o armazenamento atual permite fácil acesso, segurança e boa organização (ver Figura 13).

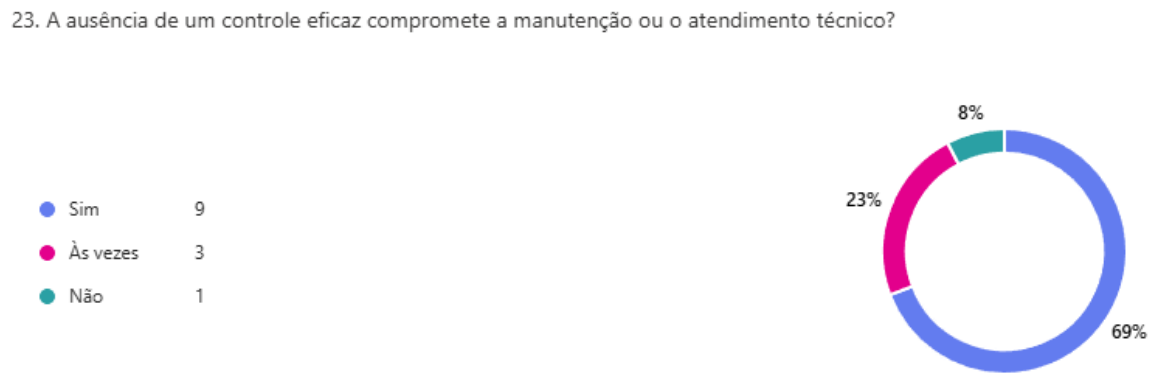
Figura 13 – Avaliação das condições de armazenamento



Fonte: Dados da pesquisa (2025).

Os dados revelam consenso sobre o impacto da ausência de controle na manutenção técnica. É importante ressaltar que o questionário utilizou uma estrutura de ramificação por setores, sendo que 13 dos 17 respondentes pertencem a áreas que utilizam diretamente atendimento técnico. Dentro desse grupo, conforme demonstra a Figura 14, 69% dos respondentes confirmam que a ausência de controle eficaz compromete a manutenção ou atendimento técnico.

Figura 14 – Impacto do controle na manutenção técnica



Fonte: Dados da pesquisa (2025).

4.1.1 Síntese dos Dados

A análise dos dados revela um cenário que corrobora solidamente a necessidade de implementação de um sistema de gerenciamento de ativos na instituição escolar pesquisada:

Deficiências Críticas Identificadas:

- 82% relatam ausência ou inadequação de processos de conferência.
- 71% não têm conhecimento sobre registros de perdas e danos.

Impactos Operacionais:

- 69% confirmam que a ausência de controle compromete a manutenção técnica.
- Deficiências na comunicação sobre disponibilidade de recursos.

Os resultados obtidos proporcionam fundamentação sólida para a implementação de um sistema de gerenciamento de ativos, considerando que existe reconhecimento institucional das deficiências críticas de controle e há impactos mensuráveis na operação e manutenção (Barbetta, 2019).

4.2 Regras de Negócio

As regras de negócio estabelecem as políticas organizacionais que orientam o funcionamento do sistema:

Quadro 1 – Regras de Negócio

Código	Descrição
RN01	**Controle Patrimonial Obrigatório** — Todo equipamento de Tecnologia da Informação (TI) deve ser cadastrado no sistema antes de ser colocado em uso operacional.
RN02	**Rastreabilidade de Empréstimos** — Equipamentos móveis só podem ser emprestados mediante registro formal no sistema.

Continua na próxima página

Quadro 1 – Continuação da página anterior

Código	Descrição
RN03	**Controle de Garantias** — Todo ativo deve ter sua garantia controlada, com alertas automáticos 30 dias antes do vencimento.
RN04	**Gestão de Consumíveis por Estoque Mínimo** — Consumíveis devem ser controlados por níveis mínimos, gerando alertas automáticos para reposição.
RN05	**Documentação Fiscal Vinculada** — Toda nota fiscal deve ser digitalizada e vinculada ao respectivo ativo.
RN06	**Licenciamento de *Software*** — Licenças devem ser controladas quantitativamente, impedindo instalações que excedam licenças adquiridas.
RN07	**Responsabilidade por Ativo** — Todo ativo deve ter um responsável formal designado.
RN08	**Auditoria de Localização** — A localização física deve ser verificada periodicamente através de inventários com códigos Quick Response Code *(QR Code)*.
RN09	***Backup* de Dados Críticos** — Dados devem ser protegidos através de *backups* automáticos diários.
RN10	**Integração com Infraestrutura Corporativa** — O sistema deve utilizar autenticação corporativa existente.
RN11	**Monitoramento de Segurança Física** — Câmeras devem ter status operacional monitorado continuamente.
RN12	**Identificação Padronizada** — Todos os ativos devem possuir etiquetas com códigos *QR Code* únicos.
RN13	**Capacitação Obrigatória** — Usuários devem ser treinados antes de obter acesso ao sistema.
RN14	**Validação antes da Implantação** — O sistema deve ser testado antes da implantação definitiva.
RN15	**Documentação de Processos** — Procedimentos e lições aprendidas devem ser documentados.
RN16	**Solicitação de Ativos** — Usuários podem solicitar empréstimo de equipamentos disponíveis através do sistema, informando finalidade, período necessário e justificativa.
RN17	**Aprovação de Solicitações** — Solicitações de empréstimo devem ser aprovadas por técnico ou administrador antes da liberação do equipamento.
RN18	**Reserva de Equipamentos** — Equipamentos podem ser reservados para uso futuro, com prazo máximo de 7 dias para retirada.

Continua na próxima página

Quadro 1 – Continuação da página anterior

Código	Descrição
RN19	**Fila de Solicitações** — Quando o equipamento não estiver disponível, o sistema deve permitir entrada em fila de espera com notificação automática quando liberado.
RN20	**Histórico de Solicitações** — O sistema deve manter histórico completo de todas as solicitações do usuário (aprovadas, rejeitadas, pendentes).

Fonte: Elaborado pelo autor (2025).

4.3 Requisitos

Em concordância com as regras de negócio e as necessidades identificadas, os requisitos do sistema são divididos em funcionais, não funcionais e de implementação e treinamento. Estes requisitos visam garantir que o sistema atenda às expectativas dos usuários e às necessidades operacionais da instituição.

4.3.1 Requisitos Funcionais

Os requisitos funcionais descrevem as funcionalidades que o sistema deve oferecer para atender às necessidades do negócio.

Quadro 2 – Requisitos Funcionais

Código	Descrição
RF01	**Cadastro de Ativos de TI** — O sistema deve permitir o cadastro completo de equipamentos de TI, incluindo computadores, câmeras e consumíveis. Cada ativo deve ter numeração patrimonial única.
RF02	**Controle de Empréstimos** — O sistema deve gerenciar empréstimos de equipamentos móveis, registrando responsável, data e prazo de devolução.
RF03	**Gestão de Consumíveis** — O sistema deve controlar o estoque de consumíveis, registrando entradas, saídas e gerando alertas automáticos para reposição.
RF04	**Gerenciamento de Documentos Fiscais** — Permitir digitalização e vinculação de notas fiscais a ativos específicos.
RF05	**Sistema de Notificações** — Enviar alertas automáticos sobre garantias, licenças e prazos de empréstimo.
RF06	**Controle de Licenças de *Software*** — Controlar licenças de *software* quantitativamente, impedindo uso além do limite.
RF07	**Monitoramento de Câmeras** — Monitorar status das câmeras, alertando falhas e equipamentos *offline*.

Continua na próxima página

Quadro 2 – Continuação da página anterior

Código	Descrição
RF08	**Solicitação de Empréstimo** — Permitir solicitações com justificativa e finalidade.
RF09	**Aprovação de Solicitações** — Permitir aprovação ou rejeição com observações.
RF10	**Reserva de Equipamentos** — Permitir reserva com prazo máximo de 7 dias.
RF11	**Notificações de Solicitações** — Enviar notificações automáticas de *status* e prazos.

Fonte: Elaborado pelo autor (2025).

4.3.2 Requisitos Não Funcionais

Os requisitos não funcionais estabelecem características de qualidade e restrições que o sistema deve atender.

Quadro 3 – Requisitos Não Funcionais

Código	Descrição
RNF01	**Usabilidade** — O sistema deve apresentar interface intuitiva e responsiva, compatível com dispositivos móveis.
RNF02	**Performance** — Responder às consultas em até 5 segundos, suportando múltiplos usuários.
RNF03	**Confiabilidade** — Garantir alta disponibilidade e *backups* automáticos.
RNF04	**Segurança** — Implementar autenticação via *Active Directory* e criptografia.
RNF05	**Escalabilidade** — Suportar aumento de ativos, usuários e dados sem reestruturação.
RNF06	**Portabilidade** — Ser containerizado (*Docker*) para fácil implantação e manutenção.

Fonte: Elaborado pelo autor (2025).

4.3.3 Requisitos de Implementação e Treinamento

Quadro 4 – Requisitos de Implementação e Treinamento

Código	Descrição
RI01	**Infraestrutura Tecnológica** — O sistema deve ser implementado utilizando *containers Docker*, compatível com *Linux* e banco de dados *MySQL*.
RI02	**Integração com *Active Directory*** — Autenticação corporativa unificada.

Continua na próxima página

Quadro 4 – Continuação da página anterior

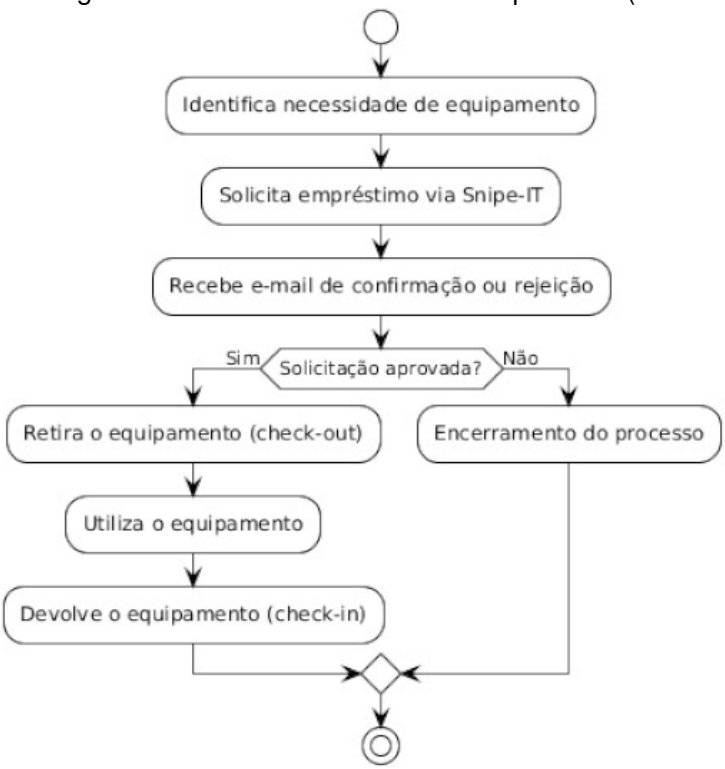
Código	Descrição
RI03	**Application Programming Interface *(API)* REST** — Interface para integração com sistemas corporativos.
RI04	**Sistema de Etiquetas Padronizadas** — Geração de etiquetas *QR Code* únicas para identificação de ativos.
RI05	**Capacitação de Usuários** — Treinamento obrigatório antes do uso.
RI06	**Testes de Usabilidade** — Validação com usuários reais antes da implantação.
RI07	**Documentação de Processos** — Registro completo das implementações e desafios.

Fonte: Elaborado pelo autor (2025).

4.4 Diagrama de Atividade

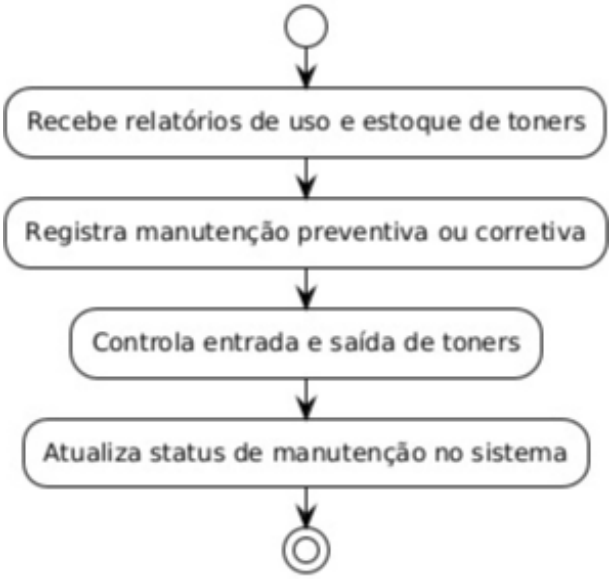
Seguindo as diretrizes apresentadas por (Guedes, 2018), os diagramas de atividade a seguir (Figuras 15, 16, 17 e 18) ilustram o fluxo de operações do sistema proposto, destacando as interações entre os usuários e as funcionalidades principais do sistema de gerenciamento de ativos de TI.

Figura 15 – Diagrama de Atividade — Fluxo de Empréstimo (Professor/Setor)



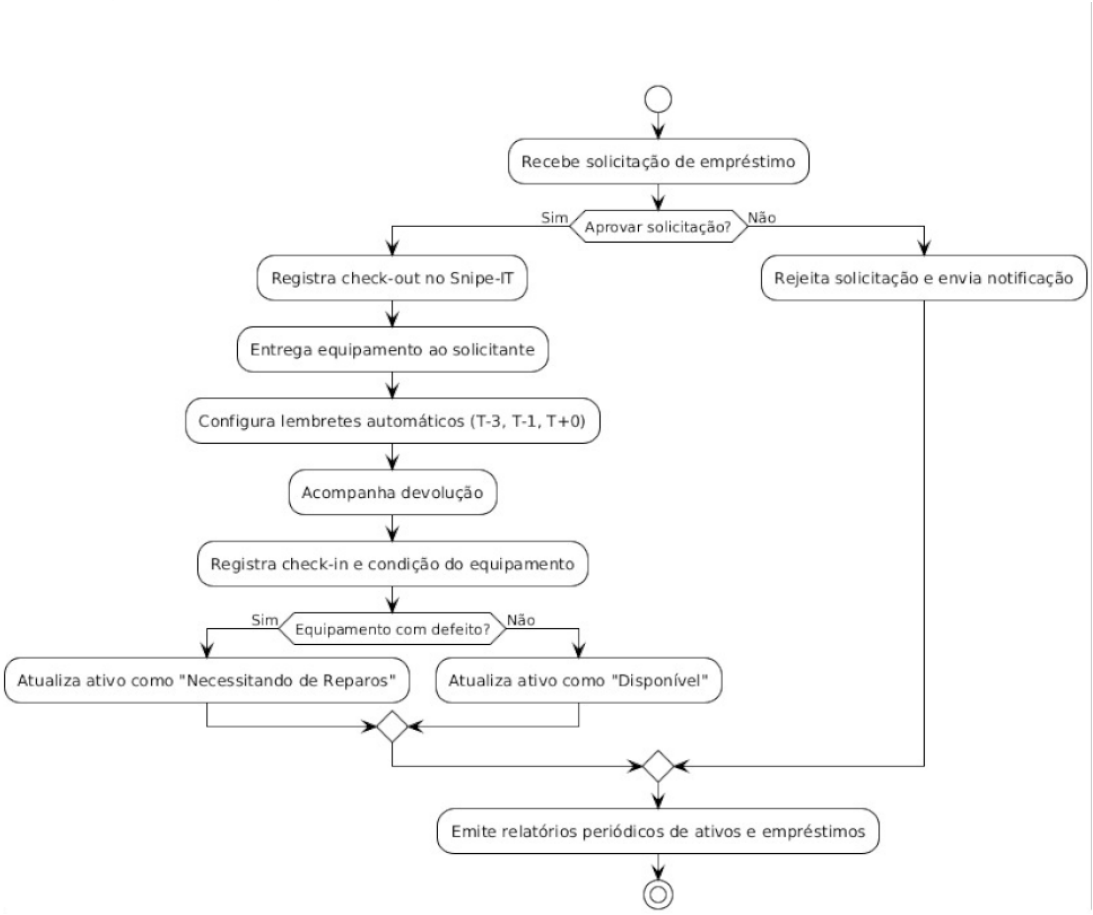
Fonte: Elaborado pelo autor (2025).

Figura 16 – Diagrama de Atividade — Fluxo de Empréstimo (Coordenação/Secretaria)



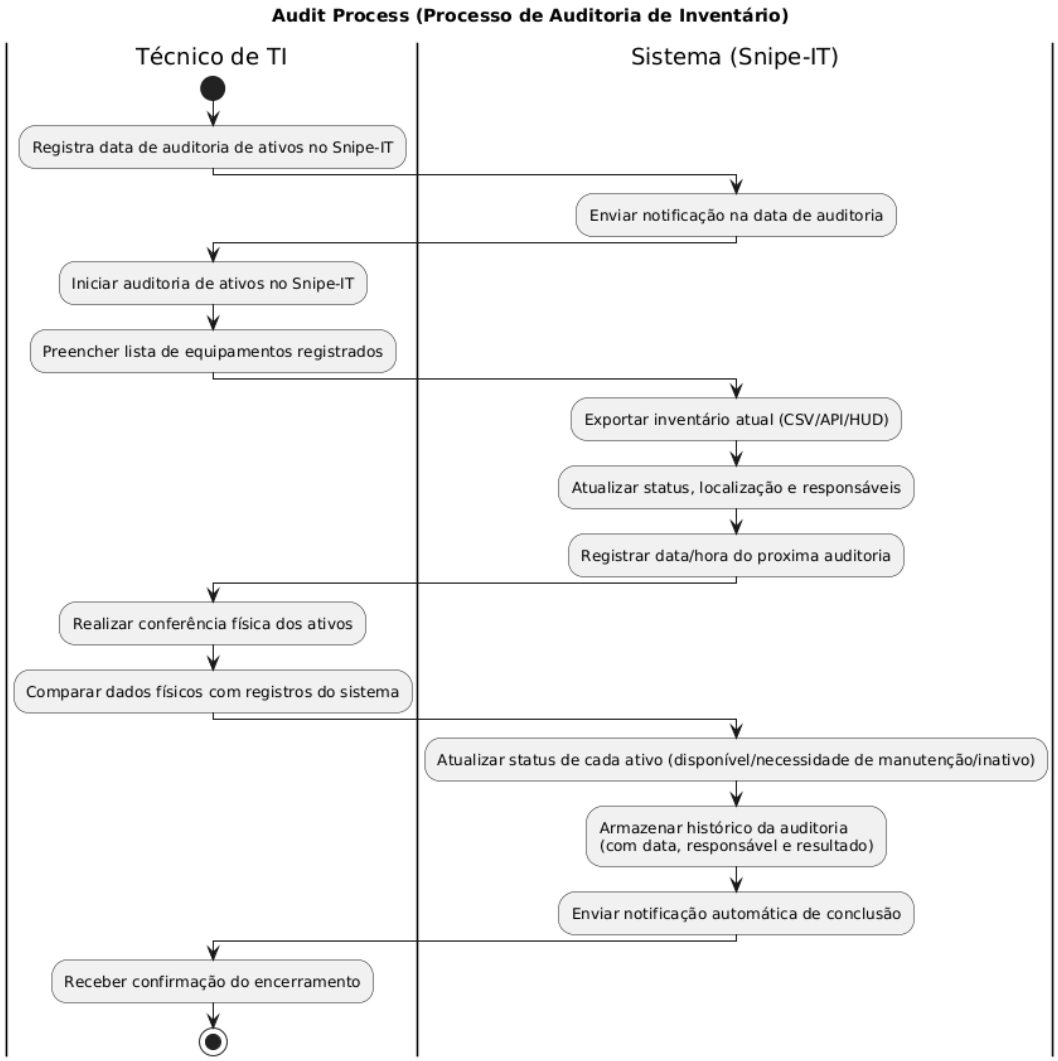
Fonte: Elaborado pelo autor (2025).

Figura 17 – Diagrama de Atividade — Fluxo de Manutenção (Técnico de TI)



Fonte: Elaborado pelo autor (2025).

Figura 18 – Diagrama de Atividade — Fluxo de Auditoria



Fonte: Elaborado pelo autor (2025).

4.5 Instalação e Configuração do Sistema

Para a instalação, foram adotadas práticas que seguem em conformidade com normas nacionais e internacionais, seguindo princípios de segurança da informação e boas práticas de gestão de TI para garantir a integridade, a rastreabilidade e a disponibilidade das informações sobre os ativos.

Utilizando a Resolução nº 03/2021 do Comitê Gestor de Segurança da Informação (CGSI) da Universidade Federal do Rio Grande do Norte (UFRN) (2021) como referência, a implementação viabiliza o registro e a rastreabilidade dos equipamentos, incluindo o acompanhamento do ciclo de vida e a conexão com as políticas da instituição. Além disso, as configurações respeitam a *International Organization for Standardization* (ISO) 55001, padronizando os registro, a autenticação e o controle dos ativos (Zampolli *et al.*, 2019).

4.5.1 Ambiente de Implantação

Para o ambiente de implementação, o sistema foi idealizado para atender aos requisitos de portabilidade (RNF06) e escalabilidade (RNF05) por meio de *Máquina Virtual (VM)* e conteinerização via *Docker*, assim explícito na seção 2.3. Utilizar um sistema virtual atesta o isolamento dos serviços, a administração eficiente de recursos e recuperação rápida em caso de falhas, dessa forma é possível se alinhar aos princípios de gestão recomendados pela ISO (2017) e manter a infraestrutura flexível e escalável com capacidade de reconfiguração caso necessário (Marchiori *et al.*, 2023b).

Ter essa automatização na gestão dos *containers* auxilia separar e integrar cada parte do sistema de forma independente, como a aplicação central, o banco de dados e o servidor de redes (Docker, Inc., 2025), conforme apresentado na Figura 9. Essa abordagem descomplica testes, atualizações e manutenções, além de garantir portabilidade entre diferentes ambientes.

A configuração do ambiente ampara a regra de negócio RN09 (*Backup* de Dados Críticos) e o requisito não funcional RNF03 (Confiabilidade), assegurando a proteção dos dados através de *backups* automáticos e alta disponibilidade do sistema. Viabilizando a disponibilidade e garantia contra perda de dados essenciais necessários ao controle de patrimonio (RN01), dando continuidade aos processos institucionais (Zampolli *et al.*, 2019; GESIN, 2021). Automatizar esses processos e usar ferramentas de código aberto ajuda a melhorar a organização e diminuir os custos operacionais (Buch, 2023). Isso contribui para uma infraestrutura tecnológica mais alinhada às boas práticas de governança e gestão de TI (McLachlan, 2018; AXELOS, 2019).

4.5.2 Configuração de Acesso e Segurança

A configuração de acesso e segurança assegura a integridade e o gerenciamento dos ativos, desempenhando um papel crucial na mitigação de riscos jurídicos e de segurança (Buch, 2023; Sodré; Berenguel, 2018), em consonância com as normas *ISO*/International Electrotechnical Commission *(IEC)* 27001 e *ISO* 55001, que focam na proteção e gestão de riscos (Zampolli *et al.*, 2019; Técnicas, 2013).

Por isso, a autenticação acontece por meio da integração com o *Microsoft Entra ID* em integração com o Active Directory *(AD)*, dessa maneira o controle é centralizado e o login padronizado com a instituição, conforme o requisito de implementação RI02. Essa estrutura é fundamental para a Information Technology Asset Management *(ITAM)*, pois minimiza riscos e atende aos requisitos de Controle de Acesso ao manter registro preciso e atualizado dos perfis de usuários para implementar controles técnicos que fornecem acesso autorizado (Técnicas, 2013).

A implementação de *IDs* únicos permite identificar adequadamente quem acessou dados sensíveis e quais alterações foram realizadas, ampliando a transparência das ações

administrativas e reduzindo a possibilidade de acessos não autorizados (Técnicas, 2013). A administração de ativos, tanto físicos quanto lógicos, é considerada um pilar central na defesa cibernética; estima-se que organizações que aplicaram de maneira integrada os seis controles primários conseguiram prevenir cerca de 80% dos incidentes de segurança (CIS CONTROLS, 2021 *apud* Buch (2023)).

Se tratando da comunicação, ela é protegida através do protocolo Hypertext Transfer Protocol Secure *(HTTPS)*, o que garante a aplicação de medidas criptográficas em conformidade com as políticas de controle. A norma Associação Brasileira de Normas Técnicas (ABNT) Norma Brasileira (NBR) *ISO*/*IEC* Técnicas (2013) estabelece que a organização deve proteger os dados pessoais transmitidos por redes públicas ou compartilhadas. Ademais, a utilização de um servidor *proxy* reverso permite o balanceamento de carga e o redirecionamento automático das requisições, reforçando a política de segurança, uma vez que a proteção de suas configurações constitui um controle essencial para neutralizar riscos (Buch, 2023) e assegurar a continuidade dos serviços.

Sodré e Berenguel (2018) destacam que a adoção dessas ações previnem a organização em relação a sua responsabilidade legal e limitar o impacto de eventuais incidentes, garantindo o alinhamento às políticas internas e os padrões globais. Sobre a autenticação, o programa é integrado ao *Microsoft Entra ID* em junção ao *AD*, o que garante um controle centralizado dos usuários, pois o *login* é unificado com a instituição. Além disso, essa junção reduz possibilidades de acesso externo e aumenta a visibilidade das ações administrativas.

Neste contexto ainda foi aplicada a camada de comunicação segura através do protocolo *HTTPS*, utilizando um certificado digital válido. A configuração com um servidor *proxy* reverso permite compensar as conexões e redirecionar automaticamente as requisições, o que fortalece a política de segurança.

4.5.3 Integração de Serviços e Comunicação

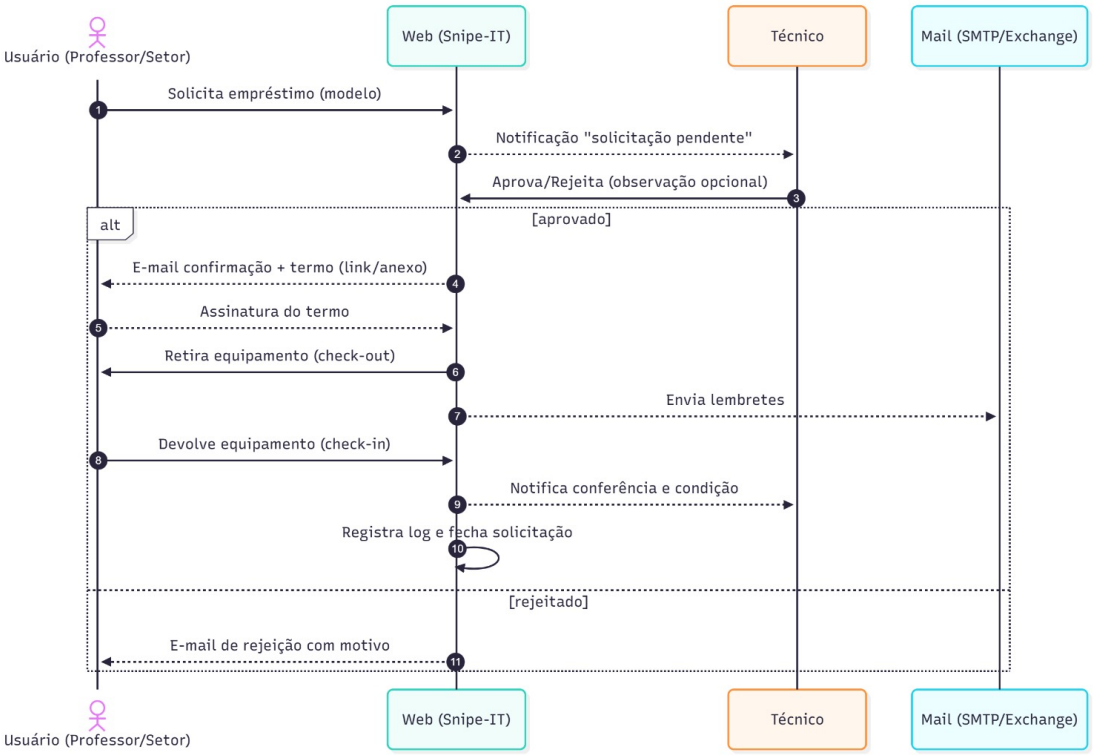
A gestão de ativos de TI *ITAM* demanda um inventário detalhado para auxiliar na tomada de decisão referente a aquisição, alocação e reaproveitamento de recursos tecnológicos (Buch, 2023). Diante dessa perspectiva, o servidor de email corporativo foi integrado ao sistema para envio de notificações, alertas e redefinição de senhas, assegurando a conformidade com as políticas institucionais e mantendo um registro centralizado das comunicações.

A criação de uma conta de serviço dedicada no *Microsoft Exchange 365*, seguida da configuração de uma senha de aplicativo (*app password*) para autenticação moderna, conforme exigido pelas políticas de segurança da Microsoft. Posteriormente, os parâmetros do servidor *Simple Mail Transfer Protocol* (SMTP) (`smtp.office365.com`, porta 587 com *Transport Layer Security* (TLS)) e as credenciais da conta foram configurados no painel administrativo do *Snipe-IT* pelos autores deste trabalho.

Essa abordagem está em sintonia com o acompanhamento contínuo dos ativos de TI e com a gestão de seu ciclo de vida, conforme levantado pela AXELOS (2019), além de fortalecer a governança da informação e a rastreabilidade das ações do sistema, em conformidade com as diretrizes das normas *ISO*/*IEC* 55001 e *ISO*/*IEC* 19770-1 (Zampolli *et al.*, 2019; ISO, 2017).

As variáveis de ambiente foram centralizadas em um arquivo dedicado contendo parâmetros de rede, conexão com o banco de dados e configurações de autenticação. Essa padronização facilita a reimplantação do ambiente, simplifica os procedimentos de *backup* e acelera as atualizações. A preservação de configurações exatas, completas e consistentes é imprescindível para o sistema de gestão de ativos (GESIN, 2021), cujo propósito é administrar os recursos durante todo o seu ciclo de vida.

Figura 19 – Diagrama de Sequência — Comunicação



Fonte: Elaborado pelo autor (2025).

4.5.4 Políticas de Backup e Recuperação de Desastre

Este capítulo baseia-se no *script* de *backup* desenvolvido especificamente para este projeto, cujo objetivo é automatizar o processo diário de salvaguardar as informações críticas do sistema. O procedimento executa a cópia de segurança do banco de dados *MariaDB* por meio do comando *mysqldump*, assegurando a exportação consistente das informações, de forma a garantir os documentos e arquivos vinculados aos ativos, além das variáveis de ambiente e arquivos de configuração do *Docker Compose*, indispensáveis para reconstrução precisa do ambiente de implantação em caso de falha total.

Os *backups* são organizados em diretórios datados e compactados para otimizar o espaço de armazenamento físico, facilitando a gestão e o controle de versões. Um mecanismo de expurgo automático exclui *backups* com mais de sete dias, assegurando a rotatividade dos dados e prevenindo a sobrecarga de espaço, em estrita observância às boas práticas de governança de dados. O *script* também atribui as permissões adequadas aos arquivos gerados, reforçando a segurança e reduzindo a possibilidade de falhas humanas, o que contribui para a confiabilidade do processo.

Esta solução baseia-se nas melhores práticas descritas em *frameworks* internacionais, como o Information Technology Infrastructure Library *(ITIL)* 4, que definem metas claras para o Recovery Time Objective *(RTO)* e o de Recovery Point Objective *(RPO)*, garantindo a sustentabilidade operacional e a integridade da informação (AXELOS, 2019). De igual modo, segue as diretrizes da *ISO* 5500, garantindo que a política de *backup* alinha-se aos preceitos de governança de ativos e minimize os riscos (Zampolli *et al.*, 2019). Essa abordagem integrada entre inovação técnica própria e bases normativas consolida a robustez do plano de *backup* e recuperação de desastre, conferindo confiabilidade e resiliência ao sistema implantado.

4.5.5 Integração com Infraestrutura Existente

O segundo *script* foi desenvolvido para que pudesse ocorrer uma sincronização automatizada entre o *Snipe-IT* e o *AD*, através de um serviço intermediário em *Python*, baseado no *framework FastAPI*. Com isso, é possível realizar a integração bidirecional entre os dois sistemas, não necessitando mais de intervenções manuais para manter os cadastros atualizados. Em resultado, o serviço estabelece comunicação segura com o controlador de domínio via *Lightweitght Directory Access Protocol* (LDAP) e com o *Snipe-IT* por meio de sua *API*.

Para maximizar o valor da solução proposta e garantir a consistência de dados entre sistemas, **foi desenvolvida neste projeto uma integração customizada entre o *Snipe-IT*, o *Active Directory* local e o Microsoft Entra ID (antigo Azure AD)** da instituição. Essa integração envolveu o desenvolvimento de componentes de software e a configuração de protocolos seguros de comunicação.

A autenticação de usuários no *Snipe-IT* foi integrada ao serviço de diretório corporativo através do protocolo LDAP, utilizando comunicação criptografada na porta 636. Essa implementação permite que colaboradores utilizem suas credenciais institucionais existentes para acessar o sistema de gestão de ativos, eliminando a necessidade de criação e manutenção de contas duplicadas.

A configuração técnica envolveu:

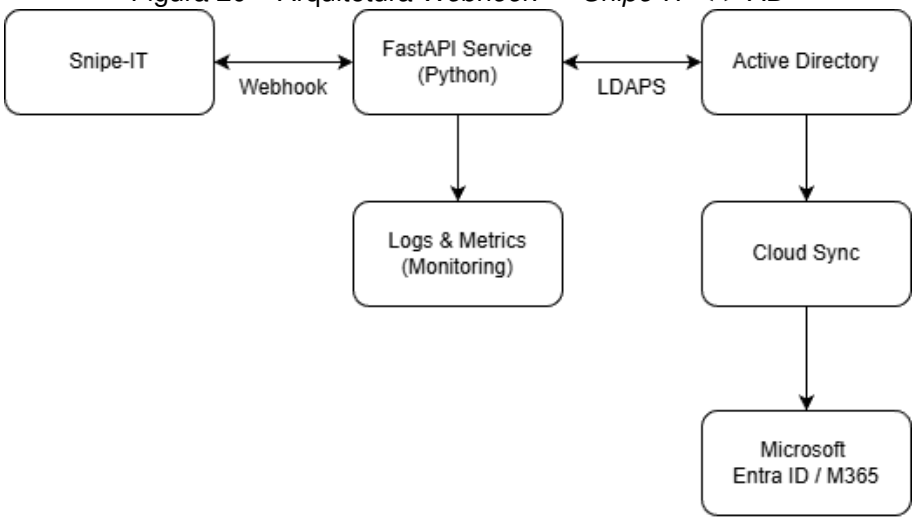
- **Bind DN**: Configuração de conta de serviço com permissões restritas de leitura no AD para consultas LDAP
- **Base DN**: Definição da Unidade Organizacional (OU) raiz onde os usuários são

localizados (`DC=colegio,DC=altaneiro,DC=local`)

- **Filtros de pesquisa**: Implementação de filtros LDAP para identificar usuários ativos e grupos específicos
- **Mapeamento de atributos**: Sincronização de campos como nome completo, email, departamento e telefone entre AD e *Snipe-IT*
- **Certificado *Secure Sockets Layer* (SSL)/TLS**: Configuração de certificado autoassinado do Controlador de Domínio para estabelecimento de conexão segura

Arquitetada dessa forma, o serviço tem sincronizações periódicas e acionamentos manuais via *webhooks*, além de registrar logs detalhados e disponibilizar *endpoints* de *health check*, mantendo o monitoramento constante e a alta confiabilidade do sistema. Sendo uma solução desenvolvida sob medida para este projeto, o *script* integra-se à infraestrutura virtualizada descrita no Capítulo 2, explorando a flexibilidade dos *containers Docker* para oferecer escalabilidade e interoperabilidade. Essa integração assegura a unicidade dos registros, simplifica-se a administração de perfis de usuário e reforça-se a blindagem da segurança institucional.

Figura 20 – Arquitetura *Webhook — Snipe-IT <-> AD*



Fonte: Elaborado pelo autor (2025).

4.5.6 Procedimentos de Implantação

O processo de instalação compete as seguintes etapas:

1. Atualização do ambiente operacional e instalação dos pacotes necessários;
2. Criação da estrutura de diretórios e configuração dos volumes de armazenamento persistente;
3. Configuração dos contêineres da aplicação e do sistema gerenciador de banco de dados;
4. Definição das credenciais de acesso e variáveis de configuração do ambiente;
5. Inicialização dos serviços conteinerizados e validação da comunicação entre componentes;

6. Implementação do servidor de proxy reverso e instalação do certificado *SSL*/*TLS*;
7. Execução de testes funcionais de acesso e validação do mecanismo de autenticação.

A documentação detalhada referente a esses procedimentos encontra-se nos Apêndices C e D. As documentações desenvolvidas e material de instrução utilizado no treinamento estão disponíveis no repositório *GitHub* do projeto: <https://github.com/MoonAmon/docs-TCC>, facilitando a replicação do ambiente, futuras manutenções e atualizações.

4.6 Treinamento

Já para o treinamento, foi adotado uma abordagem híbrida, combinando sessões presenciais com material de apoio desenvolvido para facilitar a aprendizagem dos usuários. Foi elaborado um material de treinamento abrangente, contendo um passo-a-passo ilustrado sobre as ações a serem tomadas pelos professores e coordenação. A metodologia seguiu as recomendações propostas por Acclario (2025), que destacam a importância da interação direta, suporte imediato e adaptação ao perfil dos usuários para garantir a eficiência da capacitação. Essa estratégia visa assegurar que todos os usuários estejam aptos a utilizar o sistema de forma eficaz, além de fortalecer a conscientização sobre políticas de segurança e governança de TI, alinhadas às normas internacionais como a *ISO* 55001 e às melhores práticas de gestão que fundamentam uma cultura de segurança organizacional (Zampolli *et al.*, 2019; McLachlan, 2018).

4.7 Considerações Finais da Implementação

A implementação do *Snipe-IT*, complementada pela integração com o *Active Directory*, a geração de etiquetas *QR Code*, os *scripts* de sincronização e a automatização do *backup*, criou uma estrutura única e confiável para a gestão de ativos de TI e usuários na instituição. Dessa forma, isso ajuda a diminuir erros e reforça o controle sobre os recursos tecnológicos, alinhando-se as orientações da instituição. Mesmo sendo identificados algumas necessidades de ajustes finos, como limpeza de dados antigos e importância de treinamento contínuo em caso de novos colaboradores, a solução concretizada atende aos requisitos estabelecidos, proporcionado uma sólida e confiável base para a gestão dos ativos. Logo, o próximo capítulo abordará a Prova de Conceito e os teste realizados para validar o funcionamento da aplicação. Assim, é possível evidenciar na prática os benefícios e melhorias alcançadas, nas áreas de rastreabilidade, controle e auditoria de patrimônio.

5 RESULTADOS E DISCUSSÃO

Ao adotar uma abordagem baseada em *Prova de Conceito (PoC)* e análise comparativa, este documento demonstra como a solução técnica implementada responde diretamente às dores operacionais diagnosticadas. A estrutura de resultados foi desenhada para evidenciar a conformidade com (ISO, 2017) e *ITIL*, demonstrando que a solução Snipe-IT, quando devidamente customizada e integrada ao *AD*, oferece uma robustez comparável ou superior a soluções proprietárias de mercado, com a vantagem adicional da sustentabilidade financeira proporcionada pelo licenciamento de código aberto.

5.1 Prova de Conceito e Simulação de Cenários Operacionais

Para validar a eficácia do *Snipe-IT* frente às regras de negócio e requisitos funcionais do Colégio Altaneiro, foi realizada uma PoC abrangente. Esta etapa consistiu na simulação controlada de fluxos de trabalho críticos, mimetizando a operação real da escola para demonstrar como o sistema resolve os problemas de rastreabilidade, manutenção e auditoria.

5.1.1 Cenário A: Ciclo de Vida do Empréstimo de Ativos Móveis

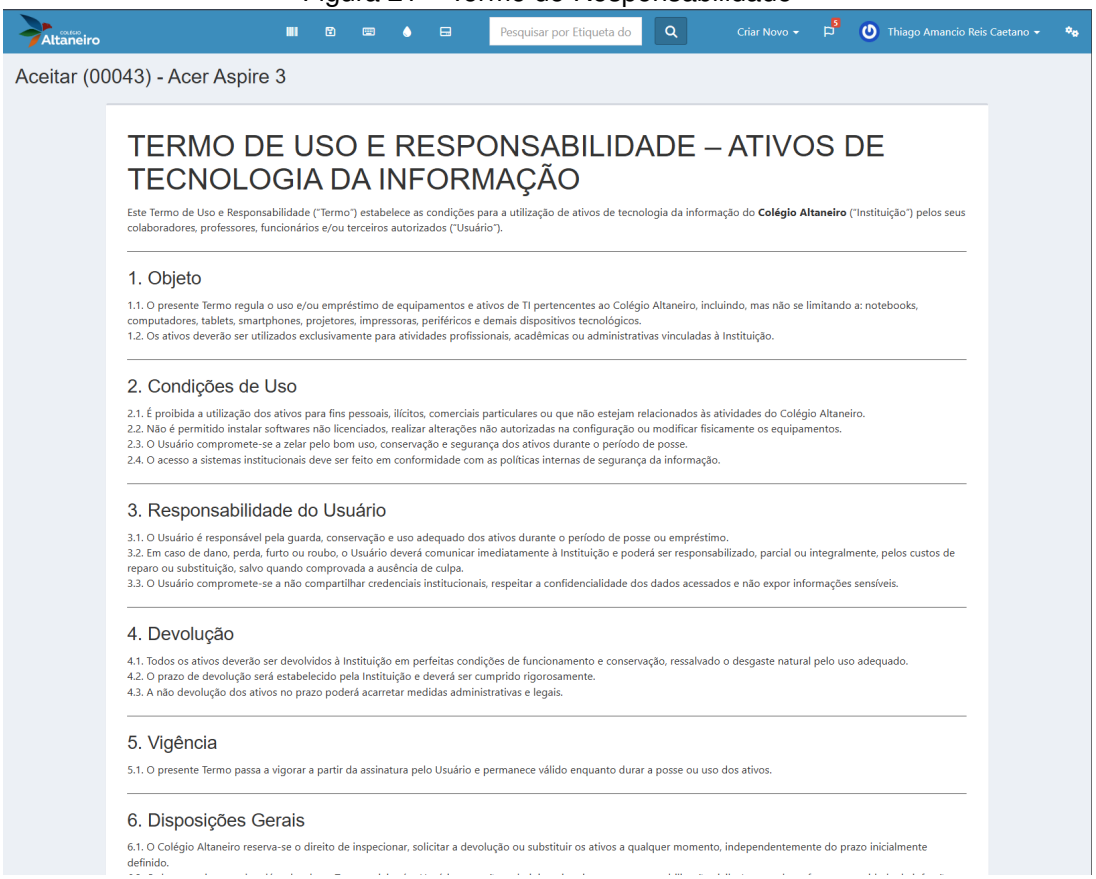
Este cenário foi desenhado para validar o atendimento à regra de negócio RN02 (Rastreabilidade de Empréstimos) - (Quadro 1) e ao requisito RF02 (Controle de Emprestimos) - (Quadro 2), atacando diretamente o problema da falta de conferência identificado no diagnóstico.

Execução da Simulação: O fluxo iniciou-se com a solicitação de um *notebook* por um perfil de um usuário através da interface *web* do *Snipe-IT* de acordo com fluxo (Figura **??**). O perfil associado ao grupo de tecnicos recebeu uma notificação via e-mail, fez inserção de justificativa nas notas e data prevista de devolução, conforme definido no RF08 (Solicitação de Empréstimo) - (Quadro 2). Ao aprovar a solicitação, o sistema realizou a baixa lógica do ativo no estoque disponível e gerou o registro de *check-out*. O usuário assinou digitalmente o Termo de Responsabilidade gerado automaticamente pelo sistema, vinculando formalmente o ativo ao usuário.

Resultado Obtido: O sistema gerou automaticamente um Termo de Responsabilidade digital vinculado ao usuário e ao ativo específico (identificado pelo número de série e etiqueta patrimonial) - (Figura 23). A validação deste fluxo comprovou a eliminação da informalidade. O sistema impediu a liberação do ativo sem a atribuição de um responsável formal conforme defenido RN07 (Responsabilidade por Ativo) - (Quadro 1), criando um rastro de auditoria indelével. Na etapa de devolução (*check-in*), o técnico registrou o estado

de conservação do equipamento. A interface permitiu a anotação de observações sobre arranhões ou defeitos, alimentando o histórico de vida do ativo.

Figura 21 – Termo de Responsabilidade



Fonte: Elaborado pelo autor (2025).

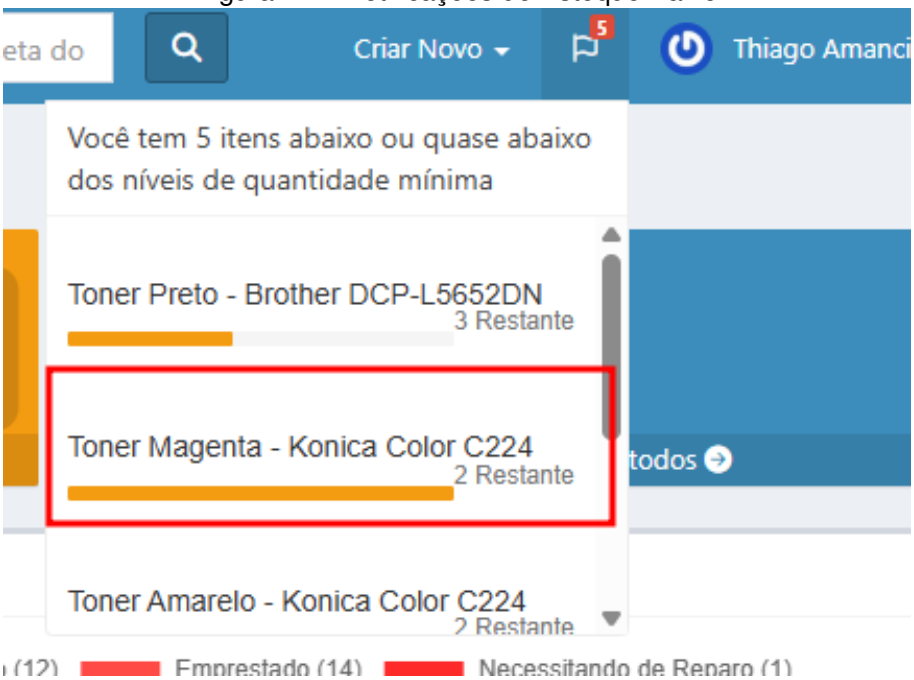
5.1.2 Cenário B: Gestão Proativa de Consumíveis e Alertas

Visando mitigar o problema da gestão reativa de materiais, simulou-se o controle de estoque de toners de impressão, validando os requisitos RF03 (Gestão de Consumíveis) - (Quadro 2) e RF11 (Notificações) - (Quadro 2).

Execução da Simulação: Foi cadastrado o item *"Toner Magenta - Konica Color C224"* com um estoque físico de 4 unidades e configurado um *"Nível Mínimo de Estoque"* de 2 unidades. Executaram-se baixas sucessivas simulando o consumo diário da escola.

Resultado Obtido: Assim que o estoque atingiu o limiar de 2 unidades, o *Snipe-IT* disparou automaticamente um alerta para a equipe de gestão. Este resultado valida a transformação do processo de compras: o sistema passou a atuar como um gatilho proativo para a reposição, eliminando o risco de ruptura de estoque que paralisaria as impressões da escola.

Figura 22 – Notificações de Estoque Baixo



Fonte: Elaborado pelo autor (2025).

5.1.3 Cenário C: Auditoria Física e Etiquetagem Inteligente

Para atender à regra de negócio RN08 (Auditoria de Localização) - (Quadro 1) e RI01 (Cadastro Completo) - (Quadro 4), validou-se a eficácia do sistema de etiquetagem.

Execução da Simulação: O sistema gerou etiquetas patrimoniais contendo *QR Code* únicos para cada ativo cadastrado. Utilizando um dispositivo móvel conectado à rede da escola, realizou-se a leitura do *QR Code* fixado em um *notebook*.

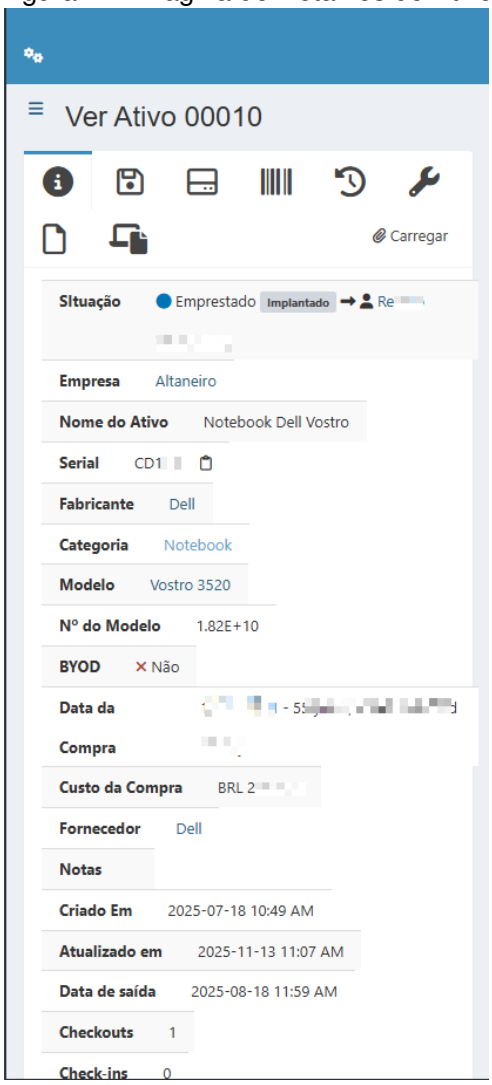
Figura 23 – Etiquetas Patrimoniais com QR Code



Fonte: Elaborado pelo autor (2025).

Resultado Obtido: A leitura do código redirecionou instantaneamente o navegador do dispositivo móvel para a página de detalhes do ativo no *Snipe-IT* após autenticação do usuário. O técnico pôde visualizar, em tempo real e em campo, informações cruciais: data de compra, fim da garantia, usuário responsável e histórico de manutenção. Esta funcionalidade validou o requisito de mobilidade e agilidade na auditoria. A capacidade de realizar verificações pontuais com apenas um scan de *QR Code* reduz drasticamente o tempo necessário para auditorias patrimoniais, transformando uma tarefa que levava dias em um processo contínuo e fluido.

Figura 24 – Pagina de Detalhes do Ativo



Fonte: Elaborado pelo autor (2025).

Os resultados demonstram que a adoção de *Snipe-IT*, quando devidamente customizada e integrada à infraestrutura de rede existente, é capaz de profissionalizar a gestão de ativos de TI. A solução entregue não apenas resolve o problema imediato do descontrole de inventário, mas estabelece uma base de dados confiável para futuras tomadas de decisão orçamentária e estratégica na instituição.

6 CONSIDERAÇÕES FINAIS

A implementação do *Snipe-IT* mostrou-se uma resposta eficaz às fragilidades identificadas no gerenciamento de ativos de TI no Colégio Altaneiro. O trabalho recuperou o problema central — marcado pela falta de rastreabilidade, inconsistência nos registros e ausência de padronização — e demonstrou que o objetivo geral foi plenamente atingido, assim como os objetivos específicos definidos na introdução.

O diagnóstico realizado por meio de questionários, entrevistas e análise documental revelou lacunas significativas nos processos de controle, que foram confirmadas pelos dados estatísticos apresentados no capítulo de desenvolvimento. A partir disso, a implantação do sistema, acompanhada de integrações, *scripts* de automação e padronização dos fluxos, permitiu construir uma solução sólida, escalável e alinhada às boas práticas de governança de TI. Os testes e simulações mostraram que a rastreabilidade, a auditoria e o controle de consumíveis foram substancialmente aprimorados, refletindo diretamente na eficiência operacional.

A principal contribuição deste trabalho está na demonstração prática de como ferramentas *open source*, quando planejadas de forma metodológica, podem atender demandas reais de instituições educacionais, reduzindo custos, fortalecendo a transparência e organizando processos internos. Também contribui ao campo acadêmico ao integrar conceitos de engenharia de requisitos, governança de ativos e metodologias aplicadas.

Como limitações, destaca-se que a pesquisa foi conduzida em apenas uma instituição e em um período restrito de testes, o que limita a análise de impactos de longo prazo. Para estudos futuros, recomenda-se investigar a adoção do *Snipe-IT* em múltiplas instituições, comparar seu desempenho com outras soluções de *ITAM* e avaliar a maturidade do sistema após ciclos completos de uso.

Em síntese, a pesquisa evidencia que a gestão de ativos de TI pode ser significativamente aprimorada por soluções acessíveis e bem estruturadas, e que a adoção do *Snipe-IT* representa um passo consistente em direção a processos mais seguros, eficientes e alinhados às necessidades institucionais.

REFERÊNCIAS

ACCLARIO. **The role of user training in successful system implementations**. 2025. Acesso em: 15 nov. 2025. Disponível em: <https://acclario.com.au/the-role-of-user-training-in-successful-system-implementations/>.

ALENCAR, M. A. S. **Fundamentos de redes de computadores**. Manaus: UFAM/CETAM, 2010. Disponível em: <https://ifpr.edu.br/pronatec/wp-content/uploads/sites/46/2012/07/Instalador_e_Reparador_de_Redes_de_Computadores.pdf>. Acesso em: 19 dez. 2025. Disponível em: <https://ifpr.edu.br/pronatec/wp-content/uploads/sites/46/2012/07/Instalador_e_Reparador_de_Redes_de_Computadores.pdf>.

AXELOS. **ITIL Foundation: ITIL 4 Edition**. Londres: TSO (The Stationery Office), 2019.

BARBETTA, P. A. **Estatística aplicada às ciências sociais**. 9. ed. [S.l.]: Editora da UFSC, 2019.

BHARADWAJ, A. S. A resource-based perspective on information technology capability and firm performance: an empirical investigation. **MIS Quarterly**, v. 24, n. 1, p. 169–196, 2000. Disponível em: <https://www.researchgate.net/publication/220260264_A_Resource-Based_Perspective_on_Information_Technology_Capability_and_Firm_Performance_An_Empirical_Investigation>. Acesso em: 28 abr. 2025.

BUCH, G. H. **Proposta e implementação de um sistema automatizado para o gerenciamento de ativos de TI integrando ferramentas open source**. 2023. Disponível em: <https://repositorio.ufsc.br/handle/123456789/248493>. Acesso em: 08 mai. 2025.

BUDIBASE. **Budibase: open source low-code platform**. 2025. Acesso em: 22 dez. 2025. Disponível em: <https://budibase.com>.

CAPTERRA. **Snipe-IT: pricing, reviews, pros & cons**. 2025. Acesso em: 20 dez. 2025. Disponível em: <https://www.capterra.com/p/150016/Snipe-IT/>.

CARDOSO, R. **MySQL: guia completo de como utilizar o sistema**. 2023. Disponível em: <https://www.locaweb.com.br/blog/temas/codigo-aberto/mysql-guia-completo-de-como-utilizar-o-sistema/>. Acesso em: 18 jun. 2025.

CARVALHO, C. **O que é Python?** 2023. Disponível em: <https://www.alura.com.br/artigos/python>. Acesso em: 16 jun. 2025.

CERVO, A. L.; BERVIAN, P. A.; SILVA, R. d. **Metodologia científica**. 6. ed. São Paulo, SP: Pearson, 2006. E-book. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 10 mai. 2025.

DIE.NET. **Introduction to Linux - Chapter 1**. 2025. Disponível em: <https://linux.die.net/Intro-Linux/chap_01.html>.

Docker, Inc. **Docker Documentation**. 2025. <https://docs.docker.com/>. Acesso em: 16 nov. 2025.

ERICKSON, J. **MySQL: entendendo o que é e como é usado**. 2024. Disponível em: <https://www.oracle.com/br/mysql/what-is-mysql/>. Acesso em: 18 jun. 2025.

FIELD, A. P. **Discovering statistics using IBM SPSS statistics**. 5th. ed. [S.l.]: SAGE, 2018.

GARTNER. **Gartner Forecasts Worldwide IT Spending to Reach $4 Trillion in 2021**. 2021. Disponível em: <https://www.gartner.com/en/newsroom/press-releases/2021-04-07-gartner-forecasts-worldwide-it-spending-to-reach-4-trillion-in-2021>.

GESIN. **Plano de Gestão de Ativos de Informação**. Santa Catarina: [s.n.], 2021. Documento institucional. Acesso em: 08 nov. 2025.

GLPI. **GLPI: gestionnaire libre de parc informatique**. 2025. Acesso em: 22 dez. 2025. Disponível em: <https://glpi-project.org>.

GOWORKWIZE. **Snipe-IT reviews 2026: features, pricing, support and more**. 2025. Acesso em: 19 dez. 2025. Disponível em: <https://www.goworkwize.com/blog/snipe-it-review>.

GREGOLINSKA, E. *et al.* **Capturing the true value of Industry 4.0**. 2022. Disponível em: <https://www.mckinsey.com/capabilities/operations/our-insights/capturing-the-true-value-of-industry-four-point-zero>. Acesso em: 10 mai. 2025.

GROKABILITY. **Snipe-IT: a free open source IT asset/license management system**. 2025. GitHub. Acesso em: 18 dez. 2025. Disponível em: <https://github.com/snipe/snipe-it>.

GROWRK. **Top Snipe-IT alternatives for IT asset management in 2025**. 2025. Acesso em: 22 dez. 2025. Disponível em: <https://growrk.com/blog/snipe-it-alternatives>.

GUEDES, G. T. A. **UML 2: uma abordagem prática**. 3. ed. São Paulo: Novatec Editora, 2018.

HAT, R. **O que é KVM**. 2024. Disponível em: <https://www.redhat.com/pt-br/topics/virtualization/what-is-KVM>. Acesso em: 15 jun. 2025.

HAT, R. **O que é uma máquina virtual (VM)**. 2024. Disponível em: <https://www.redhat.com/pt-br/topics/virtualization/what-is-a-virtual-machine>. Acesso em: 15 jun. 2025.

INC., L. S. **O que é diagramação inteligente?** 2025. Acesso em: 12 jun. 2025. Disponível em: <https://www.lucidchart.com/blog/pt/diagramas-inteligentes>.

INVGATE. **InvGate Assets: IT asset management software**. 2025. Acesso em: 27 dez. 2025. Disponível em: <https://www.invgate.com/it-asset-management-software>.

ISO. **ISO/IEC 19770-1:2017**. 2017. Disponível em: <https://www.iso.org/standard/65666.html>.

JASIULIONIS, D. **What is VS Code: an overview of the popular code editor and its features**. 2025. Acesso em: 12 jun. 2025. Disponível em: <https://www.hostinger.com/tutorials/what-is-vs-code>.

JUSAK, J.; SUKMAAJI, A. Network inventory collection system for managing and monitoring information technology asset. **International Conference Proceedings**, 2009.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet: uma abordagem top-down**. 8. ed. Porto Alegre: Bookman, 2021.

LARSON, R. E. **Estatística aplicada: retratando o mundo**. 8. ed. [S.l.]: Bookman, 2023. E-book. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 02 jul. 2025.

LEDUR, C. L. **Análise e projeto de sistemas**. SAGAH, 2018. E-book. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788595021792/>.

MANAGEENGINE. **ManageEngine AssetExplorer**. 2025. Acesso em: 27 dez. 2025. Disponível em: <https://www.manageengine.com/products/asset-explorer>.

MARCHIORI, D. M. *et al.* O papel das capacidades de ti, capacidade de reconfiguração de ti e inovatividade no desempenho organizacional: evidências do setor público brasileiro. **Revista de Administração Pública**, v. 57, n. 2, p. e2022–0221, 2023. Acesso em: 18 set. 2025. Disponível em: <https://www.researchgate.net/publication/370970049_O_papel_das_capacidades_de_TI_capacidade_de_reconfiguracao_de_TI_e_inovatividade_no_desempenho_organizacional_evidencias_do_setor_publico_brasileiro>.

MARCHIORI, D. M. *et al.* O papel das capacidades de ti, capacidade de reconfiguração de ti e inovatividade no desempenho organizacional: evidências do setor público brasileiro. **Revista de Administração Pública**, Rio de Janeiro, v. 57, n. 2, 2023.

MCLACHLAN, P. E. **Pocket CIO – The Guide to Successful IT Asset Management**. Birmingham: Packt Publishing Ltd., 2018. Acesso em: 08 nov. 2025.

MICROSOFT. **Active Directory**. 2025. Disponível em: <https://learn.microsoft.com/pt-br/windows-server/identity/active-directory-domain-services/get-started>.

MICROSOFT. **Descrição do serviço do Microsoft Forms**. 2025. Acesso em: 12 jun. 2025. Disponível em: <https://learn.microsoft.com/pt-br/office365/servicedescriptions/microsoft-forms-service-description>.

MICROSOFT. **Get Started with Windows Server**. 2025. Disponível em: <https://learn.microsoft.com/pt-br/windows-server/get-started/get-started-with-windows-server>.

MICROSOFT. **Microsoft Entra ID**. 2025. Disponível em: <https://www.microsoft.com/pt-br/security/business/identity-access/microsoft-entra-id#overview>.

MICROSOFT. **O que é o Microsoft Forms?** 2025. Acesso em: 12 jun. 2025. Disponível em: <https://support.microsoft.com/pt-br/topic/o-que-o-microsoft-forms-6b391205-523c-45d2-b53a-fc10b22017c8>.

MICROSOFT. **O que é o PowerShell?** 2025. Disponível em: <https://learn.microsoft.com/pt-br/powershell/scripting/overview?view=powershell-7.4>. Acesso em: 18 jun. 2025.

MICROSOFT. **Por que criamos o Visual Studio Code**. 2025. Acesso em: 12 jun. 2025. Disponível em: <https://code.visualstudio.com/docs/editor/whyvscode>.

MORETTIN, P. A. **Estatística básica**. 10. ed. [S.l.]: Saraiva Uni, 2023. E-book. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788571441484/>. Acesso em: 02 jul. 2025.

NOCOBASE. **Top 8 open source IT asset management software for 2025**. 2024. Acesso em: 21 dez. 2025. Disponível em: <https://www.nocobase.com/en/blog/it-asset-management-software>.

OPENMAINT. **openMAINT: open source maintenance management**. 2025. Acesso em: 23 dez. 2025. Disponível em: <https://www.openmaint.org>.

PEREIRA, L. M. P. **Gestão de Ativos: Estudo de Caso em Empresa de Telecomunicações**. Dissertação (Mestrado) — Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2016. Acesso em: 19 set. 2025. Disponível em: <https://www.maxwell.vrac.puc-rio.br/colecao.php?strSecao=resultado&nrSeq=28116&idi=1&rc=1>.

ROBERTS, R. M. Networking fundamentals. **Constructing an Ethical Hacking Knowledge Base for Threat Awareness and Prevention**, 2019.

ROMERO, D. **Containers com Docker: do desenvolvimento à produção**. São Paulo: Casa do Código, 2015.

SERVICENOW. **ServiceNow IT asset management**. 2025. Acesso em: 23 dez. 2025. Disponível em: <https://www.servicenow.com/products/it-asset-management.html>.

SILVA, B. W. **Gestão de Estoques: Planejamento, Execução e Controle**. 2. ed. [S.l.]: BWS Consultoria, 2019.

SILVA, J.; PEREIRA, A. GestÃo participativa na escola pÚblica. **Revista Internacional de Debates da Administração & Públicas - RIDAP**, v. 7, n. 1, 2022. Disponível em: <https://periodicos.unifesp.br/index.php/RIDAP/article/view/13660>. Acesso em: 4 jul. 2025.

SILVA, R. O. d.; SILVA, I. R. S. Linguagem de programação python. **Tecnologias em Projeção**, v. 10, n. 1, p. 55–71, 2019.

SND. **A importância da gestão de ativos de TI no setor de educação**. 2022. Blog SND. Disponível em: <https://blog.snd.com.br/educacional/a-importancia-da-gestao-de-ativos-de-ti-no-setor-de-educacao/>. Acesso em: 10 mai. 2025.

SNIPE-IT. **Documentation – API Reference (API Overview)**. 2025. Acesso em: 18 dez. 2025. Disponível em: <https://snipe-it.readme.io/reference/api-overview>.

SNIPE-IT. **Documentation – Introduction**. 2025. Acesso em: 18 dez. 2025. Disponível em: <https://snipe-it.readme.io/docs/introduction>.

SNIPE-IT. **Product Features – Snipe-IT: free open source IT asset management**. 2025. Acesso em: 18 dez. 2025. Disponível em: <https://snipeitapp.com/product>.

SNIPE-IT. **Snipe-IT Documentation**. 2025. Disponível em: <https://snipe-it.readme.io/docs>.

SODRé, R. Farragoni Rodrigues da S.; BERENGUEL, O. L. Visão holística da gestão de ativos na tecnologia da informação. **South American Development Society Journal**, v. 4, n. 12, p. 230, 2018. Acesso em: 13 nov. 2025. Disponível em: <https://www.sadsj.org/index.php/revista/article/view/197>.

SOLARWINDS. **SolarWinds IT asset management**. 2025. Acesso em: 23 dez. 2025. Disponível em: <https://www.solarwinds.com/solutions/it-asset-management>.

TANENBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. J. **Computer Networks**. 6. ed. Boston: Pearson, 2021.

TANENBAUM, A. S.; WETHERALL, D. J. **Redes de Computadores**. 5. ed. [S.l.]: Pearson, 2011.

TECH.CO. **Snipe-IT core features, pricing, pros & cons**. 2025. Acesso em: 19 dez. 2025. Disponível em: <https://tech.co/asset-tracking/snipe-it-review>.

TEIXEIRA, P. J. S. **Evolutive Software Asset Management**. 2021. Trabalho de Mestrado. Disponível em: <https://recipp.ipp.pt/bitstream/10400.22/19862/1/DM_PauloTeixeira_MEI_2021.pdf>. Acesso em: 13 mai. 2025.

TéCNICAS, A. B. de N. **ABNT NBR ISO/IEC 27001:2013 — Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos**. Rio de Janeiro: ABNT, 2013. Acesso em: 05 nov. 2025. Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=325112>.

Universidade Federal do Rio Grande do Norte (UFRN). **Resolução Normativa nº 03/2021–CGRC, de 08 de junho de 2021: Aprova normas gerais referentes à Política de Gestão de Ativos de Tecnologia da Informação**. S. l.: UFRN, 2021. Acesso em: 01 nov. 2025. Disponível em: <https://sipac.ufrn.br/sipac/VerInformativo?id=174330>.

VAZQUEZ, C. E.; SIMÕES, G. S. **Engenharia de requisitos: software orientado ao negócio**. 1. ed. Rio de Janeiro: Brasport, 2016. E-book. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 10 mai. 2025.

VIEIRA, A. C. V. **Organização e gestão da manutenção em estabelecimentos de ensino**. Coimbra: [s.n.], 2014. Tese de doutoramento. Disponível em: http://hdl.handle.net/10316/24890. Acesso em: 10 set. 2025.

VIRIMA. **Snipe asset management: features, limitations, and alternative**. 2025. Acesso em: 19 dez. 2025. Disponível em: <https://virima.com/blog/snipe-asset-management-features-limitations-and-alternative>.

WEILL, P.; ROSS, J. W. **IT Governance: How Top Performers Manage IT Decision Rights for Superior Results**. Boston: Harvard Business School Press, 2004. Acesso em: 20 set. 2025. Disponível em: <https://www.researchgate.net/publication/236973378>.

ZAMPOLLI, M.; JR., G. J. d. S. G.; HONDA, R. **Gestão de Ativos: guia para a aplicação da Norma ABNT NBR ISO 55001 considerando as diretrizes da ISO 55002:2018**. São Paulo: Procobre / International Copper Association, 2019.

APÊNDICE A – Termo de Consentimento Livre e Esclarecido

Título do Estudo: Implementação de um Sistema de Gerenciamento e Monitoramento de Ativos de TI no Colégio Altaneiro

Responsáveis: Thiago Amâncio Reis Caetano & Vitória Santana Silva

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

O (A) Senhor (a) está sendo convidado (a) a participar do trabalho descrito neste documento. Por favor, leia este documento com bastante atenção antes de assiná-lo. Caso haja alguma palavra ou frase que o (a) senhor (a) não consiga entender, converse com os autores responsáveis pelo estudo ou com um membro da equipe para esclarecê-los.

A proposta deste termo de consentimento livre e esclarecido (TCLE) é explicar tudo sobre o estudo e solicitar a sua permissão para participar do mesmo.

O objetivo deste trabalho é implementar e avaliar um sistema de gerenciamento de ativos de Tecnologia da Informação (Snipe-IT), com integração a serviços complementares, para melhorar o controle, a rastreabilidade e a organização dos equipamentos tecnológicos utilizados pela escola e tem como justificativa à necessidade de aprimorar a gestão dos equipamentos, reduzir perdas, facilitar o suporte técnico e criar uma base estruturada para decisões administrativas.

Se o(a) Sr.(a) aceitar participar do trabalho, os procedimentos envolvidos em sua participação são os seguintes: levantamento dos ativos de TI; entrevistas e questionários com a equipe técnica; instalação, configuração e testes do sistema Snipe-IT; validação com os setores envolvidos; e documentação dos resultados para fins acadêmicos. Não serão coletados dados sensíveis de alunos.

Todo trabalho que envolve pessoas ou informações institucionais pode apresentar riscos mínimos, como desconforto em entrevistas ou exposição não intencional de dados internos. Para reduzir esses riscos, todas as informações serão tratadas com sigilo e armazenadas de forma segura.

Contudo, este trabalho também pode trazer benefícios. Os possíveis benefícios resultantes da implementação do sistema como: organização do inventário de TI, maior rastreabilidade, redução de extravios, melhorias no suporte técnico e otimização dos processos administrativos. Tais benefícios são diretos para a instituição, pois o sistema permanecerá disponível após sua implementação.

Sua participação no trabalho é totalmente voluntária, ou seja, não é obrigatória. Caso o(a) Sr.(a) decida não participar, ou ainda, desistir de participar e retirar seu consentimento durante o trabalho, não haverá nenhum prejuízo ao atendimento que você recebe ou possa vir a receber na instituição.

Não está previsto nenhum tipo de pagamento pela sua participação no trabalho e o(a) Sr.(a) não terá nenhum custo com respeito aos procedimentos envolvidos.

Caso ocorra algum problema ou dano com o(a) Sr.(a), resultante de sua participação no trabalho, o(a) Sr.(a) receberá todo o atendimento necessário, sem nenhum custo pessoal e garantimos indenização diante de eventuais fatos comprovados, com nexo causal com o trabalho.

Solicitamos também sua autorização para apresentar os resultados deste estudo em eventos da área de saúde e publicar em revista científica nacional e/ou internacional. Por ocasião da publicação dos resultados, seu nome será mantido em sigilo absoluto, bem como em todas as fases do trabalho.

É assegurada a assistência durante todo o trabalho, bem como é garantido ao Sr.(a), o livre acesso a todas as informações e esclarecimentos adicionais sobre o sistema e suas consequências, enfim, tudo o que o(a) Sr.(a) queira saber antes, durante e depois da sua participação o(a) Sr.(a) terá acesso a informações e esclarecimentos adicionais sobre o trabalho, suas etapas e consequências.

Rubrica do Membro

Rubrica do participante/responsável

Esse Termo é assinado em duas vias, sendo uma do(a) Sr.(a) e a outra para os membros.

Declaração de Consentimento

Concordo em participar do trabalho intitulado: "SISTEMA DE GERENCIAMENTO E MONITORAMENTO DE ATIVOS DE TI".

Nome do participante ou responsável Documento assinado digitalmente gov.br YASMIN GOMES CARNEIRO Data: 21/11/2025 10:04:45-0300 Verifique em https://validar.iti.gov.br Assinatura do participante ou responsável	Data: _____/_____/_____

Eu, Thiago Amâncio Reis Caetano, declaro cumprir as exigências contidas nos itens IV.3 e IV.4, da Resolução nº 466/2012 MS.

Documento assinado digitalmente gov.br THIAGO AMANCIO REIS CAETANO Data: 21/11/2025 10:45:12-0300 Verifique em https://validar.iti.gov.br	Data: ____/____/____

Eu, Vitória Santana Silva, declaro cumprir as exigências contidas nos itens IV.3 e IV.4, da Resolução nº 466/2012 MS.

Documento assinado digitalmente gov.br VITORIA SANTANA SILVA Data: 16/11/2025 17:11:41-0300 Verifique em https://validar.iti.gov.br	Data: 16 / 11 / 25

APÊNDICE B – Instrumento de Coleta de Dados

O formulário a seguir foi utilizado como instrumento de coleta de dados no desenvolvimento deste Trabalho de Conclusão de Curso. Ele foi elaborado e aplicado por meio da plataforma *Microsoft Forms*, entre os dias 06 e 09 de maio de 2025, com o objetivo de diagnosticar a percepção dos colaboradores da escola sobre a gestão de materiais, equipamentos e ativos de tecnologia.

O questionário foi estruturado com base em perguntas objetivas e de resposta única, organizadas por meio de lógica condicional (ramificações), que direcionaram os respondentes a diferentes blocos de perguntas conforme a função informada (setor administrativo, educacional, financeiro ou tecnologia da informação).

Todas as respostas foram coletadas de forma anônima e confidencial, com tempo médio de resposta estimado entre 5 e 10 minutos.

Plataforma: Microsoft Forms

Link: forms.office.com/r/q2vvyxB25A

Tipo de formulário: Online, com ramificações por setor

Formato das respostas: Múltipla escolha e campo aberto (última pergunta)

Abaixo estão listadas as perguntas apresentadas no formulário, com a respectiva estrutura de resposta.

Bloco Geral — Perguntas comuns a todos os setores

1. **Você considera que a escola mantém um controle adequado da entrada e saída de materiais e equipamentos?** ( ) Sim ( ) Parcialmente ( ) Não
2. **Existe algum tipo de conferência ou checagem quando um item é retirado ou devolvido?** ( ) Sim ( ) Às vezes ( ) Não
3. **Há registros consistentes sobre perdas, extravios ou danos a materiais e equipamentos?** ( ) Sim ( ) Ocasionalmente ( ) Não sei dizer
4. **O armazenamento atual dos materiais permite fácil acesso, segurança e boa organização?** ( ) Sim ( ) Parcialmente ( ) Não
5. **Com que frequência você precisa de um item que não está disponível (em falta, danificado)?** ( ) Com frequência ( ) Raramente ( ) Nunca
6. **Você acredita que um sistema de inventário poderia ajudar a reduzir desperdícios e melhorar a eficiência?** ( ) Sim ( ) Talvez ( ) Não
7. **Você sente que a reposição de materiais ocorre de forma planejada ou reativa?** ( ) Planejada ( ) Reativa ( ) Não sei dizer

8. **O atual fluxo de materiais (solicitação, entrega, devolução) é simples e bem definido?** ( ) Sim ( ) Mais ou menos ( ) Não
9. **Qual função você exerce na escola?** ***(define o bloco de perguntas específico)*** ( ) Administração ( ) Financeiro ( ) Educacional ( ) T.I

Bloco Administrativo

10. **Você considera que há clareza sobre quais setores são responsáveis pelos bens e equipamentos da escola?** ( ) Sim ( ) Parcialmente ( ) Não
11. **A direção fornece orientações claras sobre o uso e a conservação de materiais e equipamentos?** ( ) Sim ( ) Às vezes ( ) Não
12. **Existe algum procedimento padronizado para registrar a entrada e saída de bens (equipamentos, móveis etc.)?** ( ) Sim ( ) Às vezes ( ) Não
13. **Há dificuldades em localizar, reservar ou rastrear ativos utilizados por diversos setores?** ( ) Sim ( ) Ocasionalmente ( ) Não
14. **Você acredita que a escola poderia se beneficiar de um sistema formal de controle e gestão de ativos?** ( ) Sim ( ) Talvez ( ) Não

Bloco Educacional

15. **Já precisou adiar ou adaptar uma atividade por não encontrar materiais ou equipamentos disponíveis?** ( ) Sim ( ) Raramente ( ) Nunca
16. **Seria útil poder agendar com antecedência o uso de recursos como notebooks, sala multimídia, etc?** ( ) Sim ( ) Talvez ( ) Não
17. **Os professores recebem informações suficientes sobre a disponibilidade e o estado dos materiais?** ( ) Sim ( ) Não
18. **Você considera que o uso dos recursos pedagógicos é bem distribuído entre as turmas e docentes?** ( ) Sim ( ) Mais ou menos ( ) Não

Bloco Financeiro

19. **O controle de ativos atual influencia de alguma forma na elaboração ou revisão do orçamento escolar?** ( ) Sim ( ) Parcialmente ( ) Não
20. **Você acredita que relatórios sobre perdas, aquisições e movimentações de ativos ajudariam na transparência financeira?** ( ) Sim ( ) Talvez ( ) Não
21. **Há registros padronizados de aquisição e substituição de bens duráveis?** ( ) Sim ( ) Parcialmente ( ) Não sei

Bloco Tecnologia da Informação (T.I.)

22. **Existe atualmente um inventário formal de equipamentos de TI (computadores, roteadores, tablets etc.)?** ( ) Sim ( ) Parcialmente ( ) Não

23. **A ausência de um controle eficaz compromete a manutenção ou o atendimento técnico?** ( ) Sim ( ) Às vezes ( ) Não
24. **Você vê valor em registrar o histórico de manutenção, troca e uso de equipamentos tecnológicos?** ( ) Sim ( ) Talvez ( ) Não

Bloco Final — Comentário Aberto (Todos os setores)

25. **Deseja comentar algo sobre a gestão de ativos na escola ou sugerir alguma melhoria?** *(Campo de resposta aberta)*

APÊNDICE C – Documentação Instalação Snipe-IT

DOCUMENTAÇÃO DA INSTALAÇÃO DO SISTEMA SNIPE-IT

1. Introdução

Este documento tem como objetivo descrever detalhadamente o processo de **instalação, configuração e integração do sistema Snipe-IT**, utilizado para o gerenciamento de ativos de Tecnologia da Informação (TI) na instituição.
A documentação foi elaborada para garantir **rastreabilidade, reprodutibilidade e manutenção futura** do ambiente implantado, além de servir como **evidência técnica** da implementação prática do TCC.

---

2. Ambiente de Instalação

Componente	Especificação
Sistema Operacional	Ubuntu Server 22.04 LTS
Virtualização	Máquina Virtual (VM) local
Gerenciador de containers	Docker e Docker Compose
Banco de Dados	MariaDB
Acesso remoto	SSH
Autenticação	Microsoft 365 (Entra ID)
Serviço de e-mail (SMTP)	Outlook 365
Certificado SSL	Let's Encrypt / Autoassinatura
Backup	Diário automático (volumes Docker)

---

3. Etapas da Instalação

3.1 Instalação via Docker

1. **Atualização do sistema e instalação de dependências**

```
sudo apt update && sudo apt install docker.io docker-compose -y
Criação do diretório do projeto```
```

2. Criação do diretório do projeto

```
mkdir /opt/snipeit && cd /opt/snipeit
```

3. Download do `docker-compose.yml`
   - Obtenção do arquivo oficial do Snipe-IT via GitHub.
   - Configuração dos volumes persistentes e rede Docker.
4. Configuração do `docker-compose.yml`

```
volumes:
  db_data:
  storage:

services:
  app:
    image: snipe/snipe-it:${APP_VERSION:-v7.0.11}
    restart: unless-stopped
    volumes:
      - storage:/var/lib/snipeit
    ports:
      - "${APP_PORT:-8000}:80"
    depends_on:
      db:
        condition: service_healthy
        restart: true
    env_file:
      - .env

  db:
    image: mariadb:11.5.2
    restart: unless-stopped
    volumes:
      - db_data:/var/lib/mysql
    environment:
      MYSQL_DATABASE: snipeitdb
      MYSQL_USER: admin
      MYSQL_PASSWORD: Adm1n!
      MYSQL_ROOT_PASSWORD: Adm1n!
    healthcheck:
      # https://mariadb.com/kb/en/using-healthcheck-sh/#compose-file-example
      test: ["CMD", "healthcheck.sh", "--connect", "--innodb_initialized"]
      interval: 5s
      timeout: 1s
      retries: 5
```

5. Inicialização dos containers

```
sudo docker-compose up -d
```

3.2 Configuração do Arquivo `.env`

O arquivo .env define as variáveis de ambiente e parâmetros do sistema.

Principais parâmetros configurados:

```
# ------------------------------------------
# REQUIRED: DOCKER SPECIFIC SETTINGS
# ------------------------------------------
APP_VERSION=v6.4.1
APP_PORT=8000

# ------------------------------------------
# REQUIRED: BASIC APP SETTINGS
# ------------------------------------------
APP_ENV=production
APP_DEBUG=false
# Please regenerate the APP_KEY value by calling `docker compose run --rm
snipeit php artisan key:generate --show`. Copy paste the value here
APP_KEY=dkckh3%6kd8!@ahg9
APP_URL=https://ativos.escola.local
# https://en.wikipedia.org/wiki/List_of_tz_database_time_zones - TZ
identifier
APP_TIMEZONE='America/Sao_Paulo'
APP_LOCALE=pt-BR
MAX_RESULTS=500

# ------------------------------------------
# REQUIRED: UPLOADED FILE STORAGE SETTINGS
# ------------------------------------------
PRIVATE_FILESYSTEM_DISK=local
PUBLIC_FILESYSTEM_DISK=local_public

# ------------------------------------------
# REQUIRED: DATABASE SETTINGS
# ------------------------------------------
DB_CONNECTION=mysql
DB_HOST=db
DB_PORT='3306'
DB_DATABASE=snipeitdb
DB_USERNAME=admin!
DB_PASSWORD=Adm1n!pass3o7d!
MYSQL_ROOT_PASSWORD=Adm1n!pass3o7d!
DB_PREFIX=null
DB_DUMP_PATH='/usr/bin'
DB_CHARSET=utf8mb4
DB_COLLATION=utf8mb4_unicode_ci

# ------------------------------------------
```

```
# OPTIONAL: SSL DATABASE SETTINGS
# ------------------------------------------
DB_SSL=false
DB_SSL_IS_PAAS=false
DB_SSL_KEY_PATH=null
DB_SSL_CERT_PATH=null
DB_SSL_CA_PATH=null
DB_SSL_CIPHER=null
DB_SSL_VERIFY_SERVER=null

# ------------------------------------------
# REQUIRED: OUTGOING MAIL SERVER SETTINGS
# ------------------------------------------
MAIL_MAILER=smtp
MAIL_HOST=smtp.server.com
MAIL_PORT=587
MAIL_USERNAME=ativos@escola.com.br
MAIL_PASSWORD=smtp#password!
MAIL_ENCRYPTION=tls
MAIL_TLS_VERIFY_PEER=false
MAIL_FROM_ADDR=ativos@escola.com.br
MAIL_FROM_NAME='Ativos Escola'
MAIL_REPLYTO_ADDR=ativos@escola.com.br
MAIL_REPLYTO_NAME='Escola Altaneiro'
MAIL_AUTO_EMBED_METHOD='attachment'

# ------------------------------------------
# REQUIRED: DATA PROTECTION
# ------------------------------------------
ALLOW_BACKUP_DELETE=false
ALLOW_DATA_PURGE=false

# ------------------------------------------
# REQUIRED: IMAGE LIBRARY
# This should be gd or imagick
# ------------------------------------------
IMAGE_LIB=gd

# ------------------------------------------
# OPTIONAL: BACKUP SETTINGS
# ------------------------------------------
MAIL_BACKUP_NOTIFICATION_DRIVER=null
MAIL_BACKUP_NOTIFICATION_ADDRESS=null
BACKUP_ENV=true

# ------------------------------------------
# OPTIONAL: SESSION SETTINGS
# ------------------------------------------
SESSION_LIFETIME=12000
EXPIRE_ON_CLOSE=false
```

```
ENCRYPT=false
COOKIE_NAME=snipeit_session
COOKIE_DOMAIN=null
SECURE_COOKIES=false
API_TOKEN_EXPIRATION_YEARS=40

# -----------------------------------------
# OPTIONAL: SECURITY HEADER SETTINGS
# -----------------------------------------
APP_TRUSTED_PROXIES=192.168.1.1,10.0.0.1,172.16.0.0/12
ALLOW_IFRAMING=false
REFERRER_POLICY=same-origin
ENABLE_CSP=false
CORS_ALLOWED_ORIGINS=null
ENABLE_HSTS=false

# -----------------------------------------
# OPTIONAL: CACHE SETTINGS
# -----------------------------------------
CACHE_DRIVER=file
SESSION_DRIVER=file
QUEUE_DRIVER=sync
CACHE_PREFIX=snipeit

# -----------------------------------------
# OPTIONAL: REDIS SETTINGS
# -----------------------------------------
REDIS_HOST=null
REDIS_PASSWORD=null
REDIS_PORT=6379

# -----------------------------------------
# OPTIONAL: MEMCACHED SETTINGS
# -----------------------------------------
MEMCACHED_HOST=null
MEMCACHED_PORT=null

# -----------------------------------------
# OPTIONAL: PUBLIC S3 Settings
# -----------------------------------------
PUBLIC_AWS_SECRET_ACCESS_KEY=null
PUBLIC_AWS_ACCESS_KEY_ID=null
PUBLIC_AWS_DEFAULT_REGION=null
PUBLIC_AWS_BUCKET=null
PUBLIC_AWS_URL=null
PUBLIC_AWS_BUCKET_ROOT=null

# -----------------------------------------
# OPTIONAL: PRIVATE S3 Settings
# -----------------------------------------
```

```
PRIVATE_AWS_ACCESS_KEY_ID=null
PRIVATE_AWS_SECRET_ACCESS_KEY=null
PRIVATE_AWS_DEFAULT_REGION=null
PRIVATE_AWS_BUCKET=null
PRIVATE_AWS_URL=null
PRIVATE_AWS_BUCKET_ROOT=null

# --------------------------------------------
# OPTIONAL: AWS Settings
# --------------------------------------------
AWS_ACCESS_KEY_ID=null
AWS_SECRET_ACCESS_KEY=null
AWS_DEFAULT_REGION=null

# --------------------------------------------
# OPTIONAL: LOGIN THROTTLING
# --------------------------------------------
LOGIN_MAX_ATTEMPTS=5
LOGIN_LOCKOUT_DURATION=60
RESET_PASSWORD_LINK_EXPIRES=900

# --------------------------------------------
# OPTIONAL: MISC
# --------------------------------------------
LOG_CHANNEL=stderr
LOG_MAX_DAYS=10
APP_LOCKED=false
APP_CIPHER=AES-256-CBC
APP_FORCE_TLS=false
GOOGLE_MAPS_API=
LDAP_MEM_LIM=500M
LDAP_TIME_LIM=600
```

3.3 Configuração do HTTPS

- Instalação do Nginx como proxy reverso.
- Criação de arquivo de configuração:

```
sudo vim /etc/nginx/sites-available/snipeit
```

- Configuração do `nginx`:

```
server {
    listen 80;
    server_name ativos.escola.local;
    return 301 https://$host$request_uri;
```

```
}
server {
    listen 443 ssl;
    server_name ativos.escola.local;

    ssl_certificate /etc/ssl/certs/snipeit.crt;
    ssl_certificate_key /etc/ssl/private/snipeit.key;

    location / {
        proxy_pass http://127.0.0.1:8000; # Porta do Snipe-IT no Docker
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
}
```

- Geração de certificado SSL:

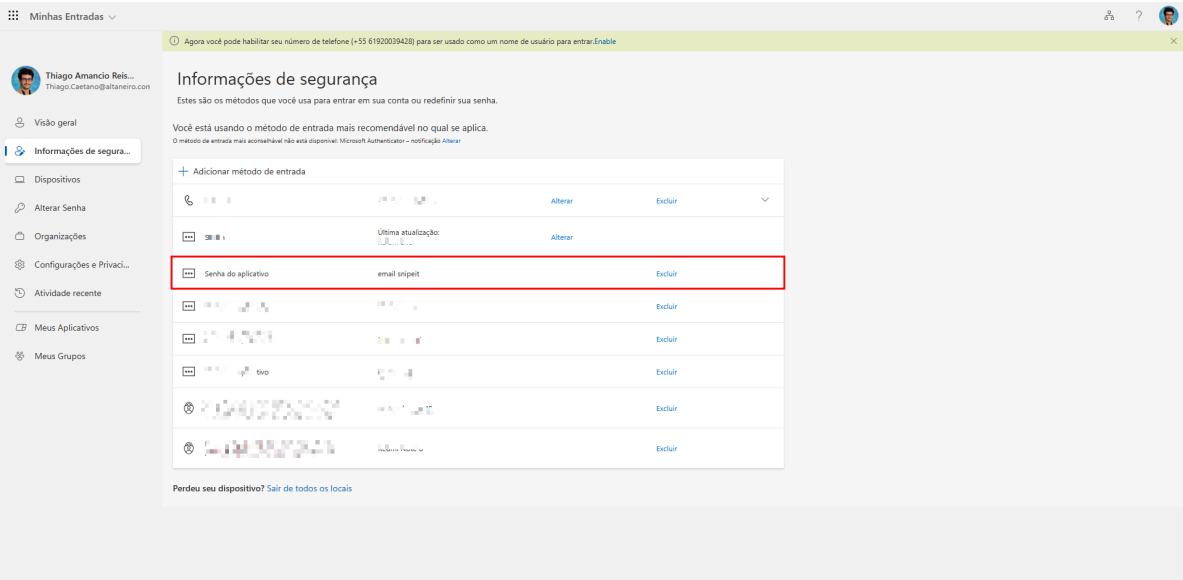
```
sudo certbot --nginx -d ativos.escola.local
```

- Redirecionamento HTTP → HTTPS.

3.4 Configuração do SMTP

Configuração com Microsoft Exchange para envio de notificações e recuperação de senha.

- Geração de senha de aplicativo para configuração no `.env`:

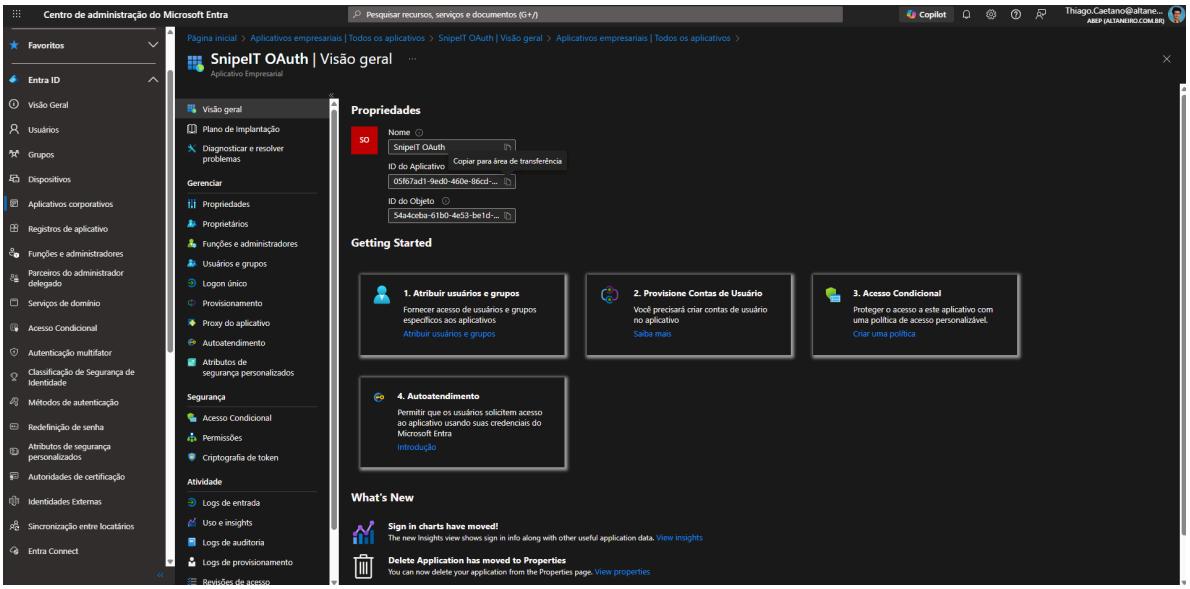


- Configuração do server SMTP no `.env`:

```
# ------------------------------------------
# REQUIRED: OUTGOING MAIL SERVER SETTINGS
# ------------------------------------------
MAIL_MAILER=smtp
MAIL_HOST=smtp.server.com
MAIL_PORT=587
MAIL_USERNAME=ativos@escola.com.br
MAIL_PASSWORD=smtp#password!
MAIL_ENCRYPTION=tls
MAIL_TLS_VERIFY_PEER=false
MAIL_FROM_ADDR=ativos@escola.com.br
MAIL_FROM_NAME='Ativos Escola'
MAIL_REPLYTO_ADDR=ativos@escola.com.br
MAIL_REPLYTO_NAME='Ativos Escola'
MAIL_AUTO_EMBED_METHOD='attachment'
```

3.5 Integração com Microsoft 365 (Entra ID)

- Registro da aplicação no Azure Portal.



- Configuração dos parâmetros no Snipe-IT.

Teste de autenticação federada com contas institucionais.

3.6 Exportação de Dados

3.6.1 Ativos

- Exportação inicial de dados em formato CSV/Excel

3.6.2 Usuários

- Exportação via Microsoft Admin Center (CSV).

3.7 Importação no Snipe-IT

- Acesso ao módulo Importação > CSV Upload.
- Mapeamento das colunas CSV com os campos internos do Snipe-IT.
- Verificação de duplicidades e inconsistência dos dados.

APÊNDICE D – Documentação Webhook

Projeto: Integração Snipe-IT ⇄ Active Directory (LDAPS)

Visão Geral

Este projeto implementa uma **integração bidirecional automatizada** entre o **Snipe-IT** e o **Active Directory**, permitindo sincronização de usuários em ambas as direções através de um **serviço Python (FastAPI)**.

O serviço comunica-se via **LDAPS (porta 636)** com o **Controlador de Domínio**, possibilitando:

- Criação, atualização e desativação de usuários
- Sincronização periódica automática
- Sincronização manual via webhooks
- Rate limiting para proteger as APIs

Todo o fluxo ocorre **dentro da rede local (LAN)**, com opção de integração com **Microsoft Entra ID** (Microsoft 365) através do **Cloud Sync**.

Funcionalidades

Sincronização Bidirecional

- **LDAP → Snipe-IT**: Replica usuários do Active Directory para o Snipe-IT
- **Snipe-IT → LDAP**: Replica usuários do Snipe-IT para o Active Directory

Operações Suportadas

- **Criação de usuários**: Cria usuários automaticamente em ambos os sistemas
- **Atualização de dados**: Sincroniza alterações de nome, email, telefone, departamento, cargo
- **Desativação**: Desativa usuários que não existem mais no sistema de origem
- **Habilitação**: Reativa usuários desativados quando necessário

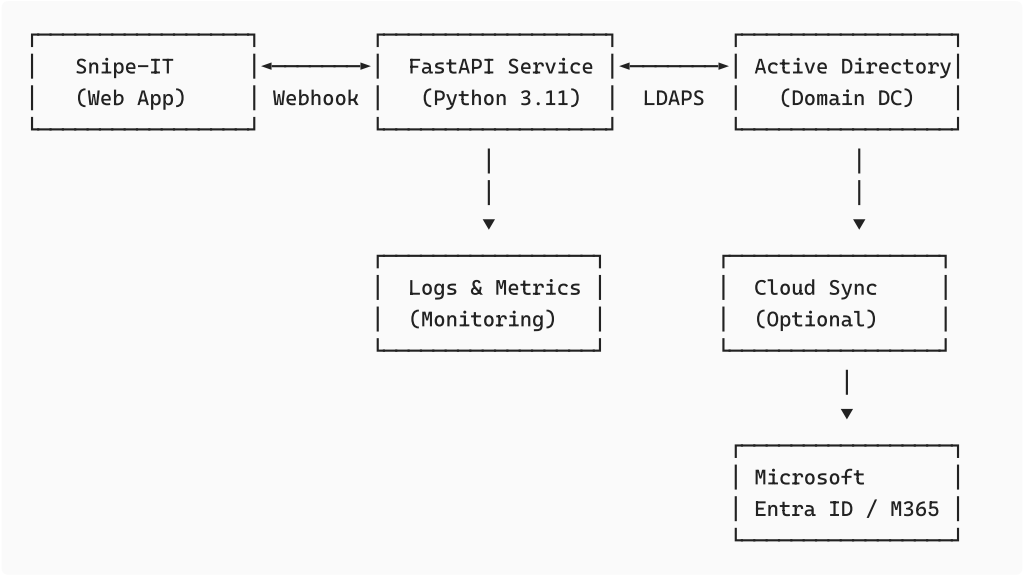
Sincronização Automática

- Sincronização periódica configurável (padrão: 15 minutos)
- Execução na inicialização da aplicação
- Logs detalhados de cada operação

Segurança

- Autenticação via webhook secret
- Suporte a SSL/TLS para LDAPS
- Rate limiting para proteção das APIs
- Validação de dados com Pydantic

Arquitetura



Fluxo de Sincronização

LDAP → Snipe-IT

1. LDAPService busca todos os usuários do AD
2. SnipeITService busca todos os usuários do Snipe-IT
3. SyncService compara os dados e identifica:
   - Usuários novos (existem no LDAP, não no Snipe-IT)
   - Usuários para atualizar (dados diferentes)
   - Usuários para desativar (não existem mais no LDAP)
4. Executa as operações necessárias

Snipe-IT → LDAP

1. SnipeITService busca todos os usuários do Snipe-IT
2. LDAPService busca todos os usuários do AD
3. SyncService compara os dados e identifica:
   - Usuários novos (existem no Snipe-IT, não no LDAP)
   - Usuários para atualizar (dados diferentes)
   - Usuários para desativar (não existem mais no Snipe-IT)
4. Executa as operações necessárias no AD

Estrutura do Projeto

```
WebhookSnipeIT_AD/
├── app/
│   ├── __init__.py
│   ├── main.py                # Aplicação FastAPI principal
│   ├── config.py              # Configurações e variáveis de ambiente
│   │
│   ├── models/
│   │   ├── __init__.py
│   │   └── user.py            # Modelos Pydantic (LDAPUser, SnipeITUser,
SyncResult)
│   │
```

```
│   ├── routes/
│   │   ├── __init__.py
│   │   └── routes.py           # Endpoints da API (webhooks e health check)
│   │
│   ├── services/
│   │   ├── __init__.py
│   │   ├── ldap_service.py     # Serviço de integração com LDAP/AD
│   │   ├── snipeit_service.py  # Serviço de integração com Snipe-IT
│   │   └── sync_service.py     # Lógica de sincronização bidirecional
│   │
│   └── utils/
│       ├── __init__.py
│       └── rate_limiter.py     # Rate limiter para proteção de APIs
│
├── logs/                       # Diretório de logs (gerado automaticamente)
├── docker-compose.yml          # Configuração Docker Compose
├── Dockerfile                  # Imagem Docker da aplicação
├── requirements.txt            # Dependências Python
├── .env                        # Variáveis de ambiente (não versionado)
├── README.md                   # Documentação principal
└── DOCUMENTATION.md            # Este arquivo (documentação detalhada)
```

Tecnologias Utilizadas

Backend

- **Python 3.11**: Linguagem de programação
- **FastAPI**: Framework web moderno e rápido
- **Uvicorn**: Servidor ASGI de alta performance
- **Pydantic**: Validação de dados e configurações

Integração

- **ldap3**: Cliente LDAP/AD para Python
- **requests**: Cliente HTTP para API do Snipe-IT
- **backoff**: Retry automático com exponential backoff

Agendamento & Monitoramento

- **APScheduler**: Agendamento de tarefas periódicas
- **logging**: Sistema de logs do Python

Rate Limiting

- **Custom RateLimiter**: Limitador de taxa customizado
- **pyrate-limiter**: Biblioteca auxiliar de rate limiting

Container

- **Docker**: Containerização da aplicação
- **Docker Compose**: Orquestração de containers

Configuração

1. Variáveis de Ambiente

Crie um arquivo `.env` na raiz do projeto com as seguintes variáveis:

```
# LDAP/Active Directory Configuration
LDAP_SERVER=dc01.dominio.local
LDAP_PORT=636
LDAP_USE_SSL=true
LDAP_BIND_DN=CN=ServiceAccount,OU=ServiceAccounts,DC=dominio,DC=local
LDAP_BIND_PASSWORD=SenhaSegura123!
LDAP_BASE_DN=DC=dominio,DC=local
LDAP_USER_FILTER=(&(objectClass=user)(objectCategory=person))

# LDAP User Creation (Opcional)
LDAP_CREATE_USER_OU=OU=Colaboradores,DC=dominio,DC=local
LDAP_DEFAULT_PASSWORD=Senha@Padrao2024

# Snipe-IT Configuration
SNIPEIT_URL=https://snipeit.dominio.local
SNIPEIT_API_KEY=eyJ0eXAiOiJKV1QiLCJhbGc...
SNIPEIT_COMPANY_ID=1
SNIPEIT_VERIFY_SSL=true
SNIPEIT_DEACTIVATED_STATUS_ID=2

# Rate Limiting
CALLS_PER_MINUTE=55
ONE_MINUTE=60

# Webhook Configuration
WEBHOOK_SECRET=seu-secret-super-seguro-aqui
SYNC_INTERVAL_MINUTES=15
DRY_RUN=false

# Application Settings
APP_NAME=Snipe-IT LDAP Sync
APP_VERSION=1.0.0
LOG_LEVEL=INFO
```

2. Permissões no Active Directory

A conta de serviço configurada em `LDAP_BIND_DN` precisa das seguintes permissões:

Para Leitura (mínimo)

- Permissão de **Ler** no container base (BASE_DN)
- Permissão de **Listar conteúdo** no container base

Para Criação/Atualização de Usuários

- Permissão de **Criar objetos de usuário** na OU especificada
- Permissão de **Modificar** propriedades dos usuários
- Permissão de **Redefinir senha** (para criar usuários com senha)

Para Desativação de Usuários

- Permissão de **Modificar** o atributo `userAccountControl`

3. Configuração no Snipe-IT

1. Acesse **Settings** → **API**
2. Clique em **Create New Token**
3. Dê um nome descritivo (ex: "LDAP Sync Service")
4. Copie o token gerado e configure em `SNIPEIT_API_KEY`

Instalação e Execução

Opção 1: Docker (Recomendado)

```
# 1. Clone o repositório
git clone https://github.com/MoonAmon/WebhookSnipeIT_AD.git
cd WebhookSnipeIT_AD

# 2. Configure o arquivo .env
cp .env.example .env
nano .env

# 3. Inicie o container
docker-compose up -d

# 4. Verifique os logs
docker-compose logs -f
```

Opção 2: Ambiente Local

```
# 1. Clone o repositório
git clone https://github.com/MoonAmon/WebhookSnipeIT_AD.git
cd WebhookSnipeIT_AD

# 2. Crie um ambiente virtual
python -m venv venv
source venv/bin/activate  # Linux/Mac
# ou
.\venv\Scripts\activate  # Windows

# 3. Instale as dependências
pip install -r requirements.txt

# 4. Configure o .env
cp .env.example .env
nano .env

# 5. Execute a aplicação
uvicorn app.main:app --host 0.0.0.0 --port 8000 --reload
```

Endpoints da API

Root

```
GET /
```

Retorna informações básicas da aplicação e links para outros endpoints.

Resposta:

```
{
  "app": "Snipe-IT LDAP Sync",
  "version": "1.0.0",
  "status": "running",
  "timestamp": "2024-11-15T10:30:00.000Z",
  "endpoints": {
    "health": "/health",
    "sync_manual": "/webhook/sync",
    "sync_report": "/webhook/sync/report",
    "last_sync": "/status"
  }
}
```

Health Check

```
GET /webhook/health
```

Verifica conectividade com o LDAP e status da aplicação.

Resposta de sucesso:

```
{
  "status": "healthy",
  "ldap": "connected",
  "timestamp": "2024-11-15T10:30:00.000Z"
}
```

Resposta de erro:

```
{
  "detail": "Service unhealthy: Connection refused"
}
```

Status

```
GET /status
```

Retorna status detalhado da aplicação, incluindo informações sobre a última sincronização e próxima execução agendada.

Resposta:

```
{
  "app_status": "running",
  "ldap_server": "dc01.dominio.local:636",
  "snipeit_server": "https://snipeit.dominio.local",
  "sync_interval_minutes": 15,
  "scheduler_running": true,
  "next_scheduled_sync": "2024-11-15T10:45:00.000Z",
  "last_sync": {
    "timestamp": "2024-11-15T10:30:00.000Z",
    "status": "success",
    "result": {
```

```
      "total_ldap_users": 150,
      "users_created": 5,
      "users_updated": 12,
      "users_deactivated": 2,
      "errors": []
    }
  },
  "current_timestamp": "2024-11-15T10:32:00.000Z"
}
```

Info

```
GET /info
```

Retorna informações de configuração da aplicação (dados não sensíveis).

Resposta:

```
{
  "application": {
    "name": "Snipe-IT LDAP Sync",
    "version": "1.0.0",
    "log_level": "INFO"
  },
  "ldap": {
    "server": "dc01.dominio.local",
    "port": 636,
    "use_ssl": true,
    "bind_dn": "CN=ServiceAccount,OU=ServiceAccounts,DC=dominio,DC=local"
  },
  "snipeit": {
    "url": "https://snipeit.dominio.local",
    "company_id": 1
  },
  "sync": {
    "interval_minutes": 15,
    "scheduler_running": true
  }
}
```

🔁 Sincronização Manual: LDAP → Snipe-IT

```
POST /webhook/to/snipeit?dry_run=false
Headers:
  x-webhook-secret: seu-secret-aqui
```

Sincroniza usuários do Active Directory para o Snipe-IT.

Parâmetros:

- `dry_run` (bool, opcional): Se `true`, apenas simula sem fazer alterações

Resposta:

```
{
  "total_ldap_users": 150,
  "user_created": 5,
```

```
  "user_updated": 12,
  "user_skipped": 0,
  "user_deactivated": 2,
  "users_created_in_ad": 0,
  "errors": [],
  "timestamp": "2024-11-15T10:30:00.000Z"
}
```

Sincronização Manual: Snipe-IT → LDAP

```
POST /webhook/to/ldap?dry_run=false
Headers:
  x-webhook-secret: seu-secret-aqui
```

Sincroniza usuários do Snipe-IT para o Active Directory.

Parâmetros:

- `dry_run` (bool, opcional): Se `true`, apenas simula sem fazer alterações

Resposta:

```
{
  "status": "success",
  "direction": "Snipe-IT -> LDAP",
  "dry_run": false,
  "total_snipeit_users": 145,
  "total_ldap_users": 150,
  "users_created": 3,
  "users_updated": 8,
  "users_deactivated": 1,
  "errors": []
}
```

Relatório de Sincronização

```
GET /webhook/sync/report
Headers:
  x-webhook-secret: seu-secret-aqui
```

Gera um relatório detalhado de pré-sincronização sem fazer alterações.

Resposta:

```
{
  "ldap_users": [
    {
      "username": "john.doe",
      "email": "john.doe@dominio.local",
      "name": "John Doe",
      "enabled": true
    }
  ],
  "snipeit_users": [
    {
      "username": "john.doe",
      "email": "john.doe@dominio.local",
```

```
      "name": "John Doe",
      "activated": true
    }
  ],
  "matches": [
    {
      "ldap_username": "john.doe",
      "snipeit_username": "john.doe",
      "match_type": "username"
    }
  ],
  "new_users": [
    {
      "username": "jane.smith",
      "email": "jane.smith@dominio.local",
      "name": "Jane Smith"
    }
  ],
  "to_deactivate": [],
  "conflicts": []
}
```

Modelos de Dados

LDAPUser

Representa um usuário do Active Directory.

```python
class LDAPUser(BaseModel):
    username: str                          # sAMAccountName
    first_name: Optional[str] = None       # givenName
    last_name: Optional[str] = None        # sn
    display_name: Optional[str] = None     # displayName
    email: Optional[EmailStr] = None       # mail
    department: Optional[str] = None       # department
    title: Optional[str] = None            # title
    phone_number: Optional[str] = None     # telephoneNumber
    phone: Optional[str] = None            # telephoneNumber (alias)
    last_modified: Optional[datetime] = None
    enabled: bool = True                   # userAccountControl
```

SnipeITUser

Representa um usuário do Snipe-IT.

```python
class SnipeITUser(BaseModel):
    username: str                          # Nome de usuário único
    first_name: Optional[str] = None       # Primeiro nome
    last_name: Optional[str] = None        # Sobrenome
    email: EmailStr = None                 # Email (obrigatório)
    department: Optional[str] = None       # Departamento
    company_id: Optional[int] = None       # ID da empresa
    job_title: Optional[str] = None        # Cargo/função
    phone: Optional[str] = None            # Telefone
    enabled: bool = True                   # Status ativo/inativo
```

SyncResult

Representa o resultado de uma operação de sincronização.

```
class SyncResult(BaseModel):
    total_ldap_users: int                    # Total de usuários no LDAP
    user_created: int                        # Usuários criados
    user_updated: int                        # Usuários atualizados
    user_skipped: int                        # Usuários ignorados
    user_deactivated: int                    # Usuários desativados
    users_created_in_ad: int = 0            # Usuários criados especificamente
no AD
    errors: list[str] = []                   # Lista de erros ocorridos
    timestamp: datetime                      # Timestamp da operação
```

🔍 Lógica de Correspondência de Usuários

O sistema usa uma estratégia em cascata para encontrar usuários correspondentes:

1. Por Username (Prioridade Alta)

Compara `sAMAccountName` (LDAP) com `username` (Snipe-IT), ignorando maiúsculas/minúsculas.

```
if ldap_user.username.lower() == snipeit_user['username'].lower():
    return snipeit_user  # Match encontrado
```

2. Por Email (Prioridade Média)

Se username não corresponder, compara emails.

```
if ldap_user.email.lower() == snipeit_user['email'].lower():
    return snipeit_user  # Match encontrado
```

3. Por Nome Completo (Prioridade Baixa)

Se email não corresponder, compara nome completo.

```
ldap_fullname = f"{ldap_user.first_name} {ldap_user.last_name}".lower()
snipeit_fullname = f"{snipeit_user['first_name']}
{snipeit_user['last_name']}".lower()

if ldap_fullname == snipeit_fullname:
    return snipeit_user  # Match encontrado
```

Esta abordagem garante máxima correspondência mesmo quando os dados não estão perfeitamente alinhados.

Sistema de Logs

Os logs são armazenados em arquivos diários no diretório `logs/`:

Características

- **Formato de arquivo**: `YYYY-MM-DD.log`
- **Níveis**: DEBUG, INFO, WARNING, ERROR
- **Rotação**: Automática por dia
- **Saída**: Console + Arquivo

Formato de Log

```
%(asctime)s - %(name)s - %(levelname)s - %(message)s
```

Exemplo de Log

```
2024-11-15 10:30:00 - app.services.sync_service - INFO -
============================================================
2024-11-15 10:30:00 - app.services.sync_service - INFO - SCHEDULED SYNC IN
PROGRESS
2024-11-15 10:30:00 - app.services.sync_service - INFO - Last sync timestamp:
2024-11-15T10:15:00
2024-11-15 10:30:00 - app.services.sync_service - INFO -
============================================================
2024-11-15 10:30:01 - app.services.ldap_service - INFO - Connected to LDAP
server.
2024-11-15 10:30:02 - app.services.ldap_service - INFO - LDAP Search - Base
DN: DC=dominio,DC=local
2024-11-15 10:30:02 - app.services.ldap_service - INFO - LDAP Search - Filter:
(&(objectClass=user)(objectCategory=person))
2024-11-15 10:30:03 - app.services.ldap_service - INFO - Found 150 users in
LDAP.
2024-11-15 10:30:04 - app.services.snipeit_service - INFO - Total 145 users
retrieved from SnipeIT.
2024-11-15 10:30:15 - app.services.sync_service - INFO - LDAP user john.doe
created in SnipeIT.
2024-11-15 10:30:16 - app.services.sync_service - INFO - LDAP user jane.smith
updated in SnipeIT.
2024-11-15 10:30:20 - app.services.sync_service - INFO -
============================================================
2024-11-15 10:30:20 - app.services.sync_service - INFO - SYNC INFOS
2024-11-15 10:30:20 - app.services.sync_service - INFO - LDAP Total: 150
2024-11-15 10:30:20 - app.services.sync_service - INFO - Users Created in
SnipeIT: 5
2024-11-15 10:30:20 - app.services.sync_service - INFO - Users Created in AD:
0
2024-11-15 10:30:20 - app.services.sync_service - INFO - Users Updated: 12
2024-11-15 10:30:20 - app.services.sync_service - INFO - Users Skipped: 0
2024-11-15 10:30:20 - app.services.sync_service - INFO - Users Deactivated: 2
2024-11-15 10:30:20 - app.services.sync_service - INFO -
============================================================
```

Níveis de Log Recomendados

Ambiente	Nível	Uso
Desenvolvimento	DEBUG	Ver todos os detalhes e debug de código
Homologação	INFO	Ver operações normais e importantes
Produção	WARNING	Ver apenas avisos e erros

Rate Limiting

O sistema implementa rate limiting para proteger as APIs e evitar sobrecarga.

Snipe-IT API

Configuração

```
CALLS_PER_MINUTE=55
ONE_MINUTE=60
```

Comportamento

- **Limite**: 55 chamadas por minuto (configurável)
- **Janela**: 60 segundos deslizantes
- **Ação**: Aguarda automaticamente quando o limite é atingido
- **Retry**: Exponential backoff em caso de erro 429

Implementação

```
class RateLimiter:
    def __init__(self, max_calls: int, period: int):
        self.max_calls = max_calls
        self.period = period
        self.calls = deque()
        self.lock = Lock()
```

LDAP

- Sem limite rígido (geralmente LDAP suporta muitas conexões simultâneas)
- Conexões são abertas e fechadas adequadamente para evitar esgotamento de recursos
- Cada operação abre uma nova conexão e a fecha ao finalizar

Retry com Backoff

Para requisições ao Snipe-IT, o sistema usa retry automático:

```
@backoff.on_exception(
    backoff.expo,
    HTTPError,
    max_tries=5,
    giveup=lambda e: e.response is not None and
                     e.response.status_code not in [429, 500, 502, 503, 504]
)
def _make_request(self, method, endpoint, **kwargs):
    # ... código da requisição
```

- **Estratégia**: Exponential backoff
- **Tentativas máximas**: 5
- **Códigos para retry**: 429, 500, 502, 503, 504

Sincronização Periódica

A aplicação executa sincronização automática usando APScheduler.

Quando Sincroniza

1. **Na inicialização**: Executa uma sincronização imediatamente ao iniciar
2. **Periódica**: A cada `SYNC_INTERVAL_MINUTES` (padrão: 15 minutos)
3. **Manual**: Via endpoints da API

Configuração

```
scheduler = BackgroundScheduler(timezone="America/Sao_Paulo")

scheduler.add_job(
    scheduled_sync,
    "interval",
    id="sync_snipeit_to_ldap",
    name="Auto sync SnipeIT -> LDAP",
    minutes=settings.SYNC_INTERVAL_MINUTES,
    replace_existing=True
)
```

Informações da Última Sincronização

O sistema mantém registro da última sincronização:

```
last_sync_info = {
    "timestamp": "2024-11-15T10:30:00",
    "status": "success",  # ou "error", "pending"
    "result": {
        "total_ldap_users": 150,
        "users_created": 5,
        "users_updated": 12,
        "users_deactivated": 2,
        "errors": []
    }
}
```

Verificar Status

```
# Via API
curl http://localhost:8000/status

# Via logs
tail -f logs/$(date +%Y-%m-%d).log
```

Modo Dry-Run

O modo dry-run permite testar a sincronização sem fazer alterações reais nos sistemas.

Quando Usar

- **Testes iniciais**: Verificar o que seria feito antes de executar
- **Validação**: Confirmar que a lógica está correta
- **Auditoria**: Ver quais usuários seriam afetados

- **Troubleshooting**: Diagnosticar problemas sem risco

Como Usar

Via API

```
# LDAP → Snipe-IT (dry-run)
curl -X POST "http://localhost:8000/webhook/to/snipeit?dry_run=true" \
  -H "x-webhook-secret: seu-secret-aqui"

# Snipe-IT → LDAP (dry-run)
curl -X POST "http://localhost:8000/webhook/to/ldap?dry_run=true" \
  -H "x-webhook-secret: seu-secret-aqui"
```

Via Configuração Global

```
DRY_RUN=true
```

Isso fará com que TODAS as sincronizações (incluindo periódicas) executem em modo dry-run.

O Que Acontece

- Busca usuários normalmente
- Compara dados e identifica diferenças
- Registra nos logs o que seria feito
- NÃO cria usuários
- NÃO atualiza dados
- NÃO desativa contas

Exemplo de Log

```
2024-11-15 10:30:15 - app.services.sync_service - INFO - [DRY-RUN] LDAP user
john.doe would be created in SnipeIT.
2024-11-15 10:30:16 - app.services.sync_service - INFO - [DRY-RUN] LDAP user
jane.smith would be updated in SnipeIT.
2024-11-15 10:30:17 - app.services.sync_service - INFO - [DRY-RUN] SnipeIT
user bob.jones would be deactivated.
```

Monitoramento

Health Check para Sistemas de Monitoramento

1. Health Check HTTP

```
# Deve retornar status 200
curl -f http://localhost:8000/webhook/health || exit 1
```

Script de monitoramento:

```
#!/bin/bash
# check_webhook_health.sh
```

```
WEBHOOK_URL="http://localhost:8000/webhook/health"
RESPONSE=$(curl -s -o /dev/null -w "%{http_code}" $WEBHOOK_URL)

if [ $RESPONSE -eq 200 ]; then
    echo "OK - Webhook is healthy"
    exit 0
else
    echo "CRITICAL - Webhook is unhealthy (HTTP $RESPONSE)"
    exit 2
fi
```

2. Status da Última Sincronização

```
# Verificar se última sincronização foi bem-sucedida
curl -s http://localhost:8000/status | jq -r '.last_sync.status'
```

Script de monitoramento:

```
#!/bin/bash
# check_last_sync.sh

STATUS_URL="http://localhost:8000/status"
LAST_SYNC_STATUS=$(curl -s $STATUS_URL | jq -r '.last_sync.status')

case $LAST_SYNC_STATUS in
    "success")
        echo "OK - Last sync was successful"
        exit 0
        ;;
    "error")
        echo "CRITICAL - Last sync failed"
        exit 2
        ;;
    "pending")
        echo "WARNING - Sync is pending"
        exit 1
        ;;
    *)
        echo "UNKNOWN - Unable to determine sync status"
        exit 3
        ;;
esac
```

Documentação de Referência

- FastAPI Documentation
- ldap3 Documentation
- Snipe-IT API Documentation
- Active Directory LDAP