UNIVERSIDADE DE PERNAMBUCO - UPE
ESCOLA POLITÉCNICA DE PERNAMBUCO - POLI

PLANO DE TRABALHO

ANOMALY DETECTION IN C2 BEACONING TRAFFIC USING PRIVACY-PRESERVING FEDERATED LEARNING

Aluno: Gabriel Souza Borges
Orientador: Prof. Bruno José Torres Fernandes

Recife-PE
2025

Cronograma de Atividades (Setembro 2025 - Janeiro 2026)

Tabela 1: Planejamento de atividades para submissão no IJCNN 2026.

Mês	**Etapa Principal**	**Atividades Específicas**	**Entregáveis**
Setembro 2025	Revisão Bibliográfica e Desenho da Metodologia	- Aprofundamento em artigos sobre deteção de *beaconing* e Aprendizagem Federada (FL).	- Resumo da literatura.
Outubro 2025	Configuração do Ambiente e Implementação Inicial	- Análise de datasets de referência (CTU-13, UGR'16). - Definição da arquitetura de FL e seleção dos modelos de ML/DL para os experimentos. - Configuração do ambiente de simulação de FL (e.g., Flower, TFF). - Implementação dos scripts para pré-processamento dos dados e simulação da distribuição não-IID. - Desenvolvimento da versão base do modelo de deteção local.	- Documento detalhado da metodologia proposta. - Ambiente de desenvolvimento configurado. - Scripts de pré-processamento de dados.
Novembro 2025	Desenvolvimento e Treinamento do Modelo Federado	- Implementação do ciclo completo de Aprendizagem Federada. - Início do treinamento do modelo global no ambiente simulado e monitoramento da convergência. - Primeiros testes de avaliação de desempenho (precisão, recall, F1-score).	- Código-fonte do framework de FL. - Logs de treinamento e resultados preliminares.

Tabela 1: Planejamento de atividades para submissão no IJCNN 2026.

Mês	**Etapa Principal**	**Atividades Específicas**	**Entregáveis**
Dezembro 2025	Análise de Segurança e Otimização	- Implementação de um ataque de envenenamento para avaliar a vulnerabilidade. - Implementação de uma regra de agregação como contramedida. - Execução de todos os cenários experimentais finais e compilação de resultados.	- Conjunto completo de resultados, gráficos e tabelas. - Rascunho das seções de Metodologia e Resultados do artigo.
Janeiro 2026	Finalização dos Experimentos e Escrita do Artigo	- Análise aprofundada dos resultados e elaboração das conclusões. - Escrita das seções de Introdução, Trabalhos Relacionados e Conclusão. - Revisão completa do texto, formatação e referências para submissão.	- Versão final do artigo para submissão no IJCNN 2026.

Planejamento de Publicações

Submissão em Conferência

- **Previsão:** Janeiro de 2026.
- **Conferência Sugerida:** IJCNN (International Joint Conference on Neural Networks) - WCCI 2026.
- **Título Provisório:** *"A Federated Learning Framework for Privacy-Preserving C2 Beaconing Detection on non-IID Data"*.

Submissão em Periódico

- **Previsão:** Segundo semestre de 2026.
- **Título Provisório:** *"Collaborative Anomaly Detection for C2 Beaconing: A Federated Learning Approach with Adversarial Considerations"*.