UNIVERSIDADE FEDERAL DE SANTA CATARINA

CAMPUS ARARANGUÁ ou CENTRO CTS

DEPARTAMENTO DEC

CURSO ENGENHARIA DE COMPUTAÇÃO

Augusto Daleffe & João Victor Pavan

Auditor de Rede sem Fio

(Relatório pré-projeto)

**SUMÁRIO**

[**1. Visão Geral 3**](#_f3ir519p0snu)

[**2. Descrição do projeto final 4**](#_ind1s2eobe7n)

[**2.1. Aspectos a serem desenvolvidos 5**](#_2h8q793v81k8)

[2.1.1 Rede Wifi 5](#_5wqtr2ksjvv4)

[**2.2. Componentes de Hardware 5**](#_cgln4u8cchc6)

[2.2.1. Microcontrolador ESP32 5](#_36n6fvcccbg8)

[**2.3. Componentes de Software 5**](#_pjjftenxb4af)

[**2.4. Nível de conhecimento dos integrantes 5**](#_y9gigcy4js8z)

[**3. Descrição dos resultados a serem produzidos 6**](#_hd5hr0k1mmdo)

[**4. Análise e gerenciamento de riscos 6**](#_cnohfkshefbc)

[**5. Cronograma 6**](#_tnnphdelrvj8)

[**6. Protótipo inicial 6**](#_xoacm3vdivxg)

# 

# 

# Visão Geral

O projeto tem como intuito desenvolver um auditor para redes sem fio, a fim de trazer à tona vulnerabilidades comuns dentro do meio. Para isso, serão utilizados ESP32, componentes responsáveis pela simulação de uma rede sem fio e seus usuários.

Durante a simulação serão apresentados ataques direcionados tanto ao ponto de acesso quanto aos participantes do meio, mostrando seu funcionamento e como é possível identifica-lo e neutraliza-lo

## 

# Descrição do projeto final

​​O projeto proposto tem enfoque no desenvolvimento de um auditor de redes sem fio Wi-Fi utilizando a versatilidade dos microcontroladores ESP32. A proposta central é desenvolver uma solução robusta para identificar deficiências e vulnerabilidades em redes, simulando cenários de ataques e analisando o desempenho para garantir a segurança e eficiência da infraestrutura.

O projeto se baseia em uma topologia de rede estrela, onde um Ponto de Acesso (AP), também construído sobre um ESP32, será o responsável por realizar a auditoria na rede. Paralelamente, serão desenvolvidos algoritmos de Inteligência Artificial (IA) e/ou algoritmos clássicos para a análise profunda dos dados coletados, com o objetivo de identificar padrões e anomalias que possam indicar falhas de segurança.

Um dos pilares do projeto é a simulação de ataques reais utilizando clientes maliciosos que serão adicionados propositalmente à rede. Pretende-se abordar alguns dos ataques mais conhecidos, como Spoofing, Ataque de Desautenticação, Flooding, DHCP Starvation, entre outros. Espera-se que ao replicar esses cenários seja possível efetuar uma análise de desempenho precisa e a validação da eficácia do algoritmo desenvolvido.

O segundo pilar deste projeto é a construção da rede Wi-Fi. Optamos por uma topologia de rede estrela, que é a mais comum em ambientes domésticos e pequenos escritórios. Nela, um único Ponto de Acesso (AP) central se conecta a 'n' clientes, simplificando a gestão e o acesso. Essa escolha permite a simulação de cenários mais próximos ao cotidiano de redes Wi-Fi, tornando os resultados obtidos mais relevantes para análises futuras.

## 2.1. Aspectos a serem desenvolvidos

### **2.1.1 Rede Wifi**

A interface Wi-Fi é a espinha dorsal para o desenvolvimento deste projeto, dado que todo o projeto parte da premissa de que conseguiremos implementar uma rede Wi-Fi do tipo estrela. Inicialmente, a placa de desenvolvimento ESP32 será utilizada como o Ponto de Acesso (AP) central dessa rede. Essa escolha é estratégica pela sua versatilidade e baixo custo, facilitando a prototipagem e o desenvolvimento inicial. Contudo, já antecipamos que o projeto poderá enfrentar limitações relacionadas ao baixo poder de processamento do ESP32. Essa consideração é crucial para o planejamento das otimizações e para a análise dos resultados, que podem exigir soluções alternativas ou complementares em etapas futuras, como a utilização de um hardware mais robusto.s

### **2.1.2 Algoritmo Auditor**

Outro ponto crucial do nosso projeto é o desenvolvimento do Algoritmo Auditor, esse que por sua vez será responsável por identificar todas as anomalias na rede previstas durante a concepção do mesmo. A execução da análise de segurança no próprio hardware do ESP32 não só minimiza a latência de detecção, mas também otimiza o uso de recursos computacionais, proporcionando uma resposta ágil e eficaz frente a potenciais ameaças.

**2.1.3 Ataques Maliciosos**

Para a validação do nosso auditor, pretendemos implementar uma estratégia de simulação de ataques via clientes maliciosos. Esta etapa compreende a geração e manipulação de pacotes de rede específicos para replicar os ataques comumente usados no cenário de segurança de redes Wi-Fi. Pretende-se utilizar ataques Wi-Fi maliciosos para desautenticação, a injeção de pacotes para *flooding*, e a emissão de requisições DHCP forjadas para simular *DHCP starvation*. Essa abordagem nos permitirá uma análise de desempenho precisa e a validação empírica do algoritmo de auditoria desenvolvido.

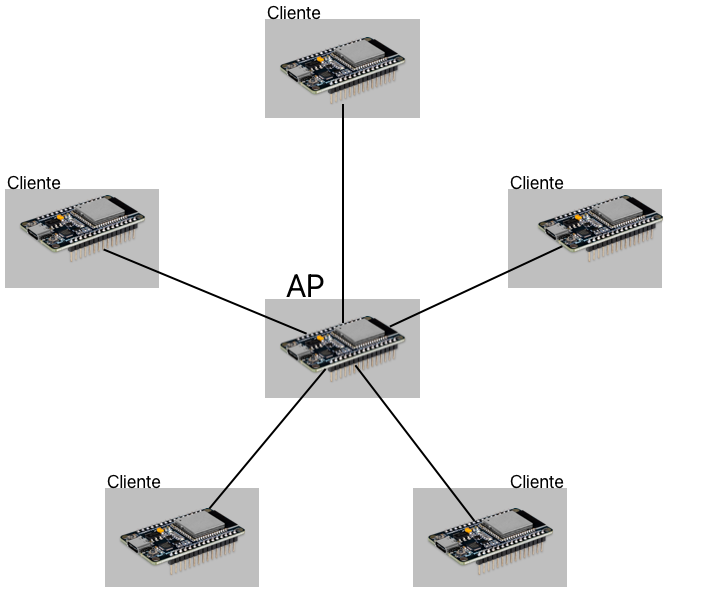
#### 

## 2.2. Componentes de Hardware

### **2.2.1. Microcontrolador ESP32**

O ESP32 é um chip versátil que possui diversas capacidades, incluindo conectividade Wi-Fi e Bluetooth, processamento dual-core, memória RAM e Flash, além de uma variedade de interfaces de comunicação e pinos GPIO.

No projeto será aplicado a topologia de rede estrela, onde, um ESP32 será configurado como ponto de acesso, enquanto demais ESP32 atuarão como clientes, que irão se conectar ao ponto de acesso, que posteriormente, simulam atividades maliciosas.



## 2.3. Componentes de Software

A implementação do projeto será realizada utilizando o Espressif IoT Development Framework (ESP-IDF), que é o framework oficial de desenvolvimento para a série ESP32. Os seguintes componentes são a base para o desenvolvimento do projeto:

* **Sistema Operacional (FreeRTOS):** O ESP-IDF é construído sobre o FreeRTOS.
* **Driver Wi-Fi(esp\_wifi):** Fundamental para configuração do wifi
* **LightWeight IP (LwIP):** Configuração do DHCP no ponto de acesso. Também usado para criar conexões TCP/UDP.
* **Eventos (esp event):** Sistema para despacho de eventos do sistema.

## 2.4. Nível de conhecimento dos integrantes

Ambos os membros do grupo possuem um conhecimento intermediário em programação C/C++ e com o microcontrolador ESP32, que foi adquirido através de cursos e projetos anteriores. Em relação a redes sem fio, mais especificamente Wi-Fi, o conhecimento é majoritariamente teórico obtido na disciplina. O projeto nos permitirá aprofundar os conhecimentos a priori, além de entender aspectos práticos de redes sem fios a partir análise do tráfego e vulnerabilidade do Wi-Fi simulado.

# Descrição dos resultados a serem produzidos

Com o projeto fim do projeto é esperado:

* Um protótipo funcional de um sistema de auditoria de redes Wi-Fi capaz de:
  + Permitir interação entre ESP32s via a rede Wi-Fi criada.
  + Identificar automaticamente a origem de pelo menos um dos ataques simulados.
* Amostragem e análise dos resultados dos ataques realizados durante a simulação.
* Uma breve análise da viabilidade de usar microcontroladores para hospedagem de uma rede Wi-Fi, considerando taxa de transmissão de dados e estabilidade da comunicação, além de como esses parâmetros são afetados durante ataques.
* Uma breve análise das capacidades e limitações do ESP32 para a proteção contra clientes maliciosos.

# Análise e gerenciamento de riscos

| **Risco** | **Probabilidade(0-10)** | **Impacto(0-10)** | **Resolução Proposta** |
| --- | --- | --- | --- |
| Limite de Processamento ESP32 | 5 | 4 | Limitar o uso de apenas funcionalidades que não ocupem totalmente os recursos do sistema;  Alteração para um Raspberry Pi, permitindo algoritmos mais complexos |
| Estabilidade da Rede | 3 | 9 | Uso de algum outro tipo de rede sem fio (Bluetooth, mesh, etc.) |
| Desenvolvimento dos algoritmos de auditoria | 7 | 5 | Implementação inicial de métodos clássicos, evolução para métodos de IA a partir de uma validação aceitável |
| Identificação dos Clientes Maliciosos | 8 | 4 | Identificação de um subconjunto de ataques |

# Cronograma

| **Início** | **Final** | **Progresso a ser feito** |
| --- | --- | --- |
| 06/06/2025 | 13/06/2025 | Implementação do ponto de acesso; Definição e implementação dos ataques efetuados pelos usuários. |
| 13/06/2025 | 20/06/2025 | Pesquisa e desenvolvimento de uma IA para identificação de ataques maliciosos no ponto de acesso |
| 20/06/2025 | 27/06/2025 | Montagem da simulação a partir das partes já desenvolvidas; Organização dos dados a serem apresentados durante a simulação |
| 27/06/2025 | 04/07/2025 | Testes |

# Protótipo inicial

Anexado junto a este documento.