**PRÉ-PROPOSTA DE TRABALHO DE CONCLUSÃO DE CURSO**

**ENGENHARIA DA COMPUTAÇÃO**

| **IDENTIFICAÇÃO** |
| --- |

| **Aluno 1** | **Guilherme Palmanhani Valli** |
| --- | --- |
| Matrícula | **02010360** |
| E-mail | **guilherme.palmanhani@gmail.com** |
| Telefone | **(12)98180-8655** |
| Endereço | **12328140** |

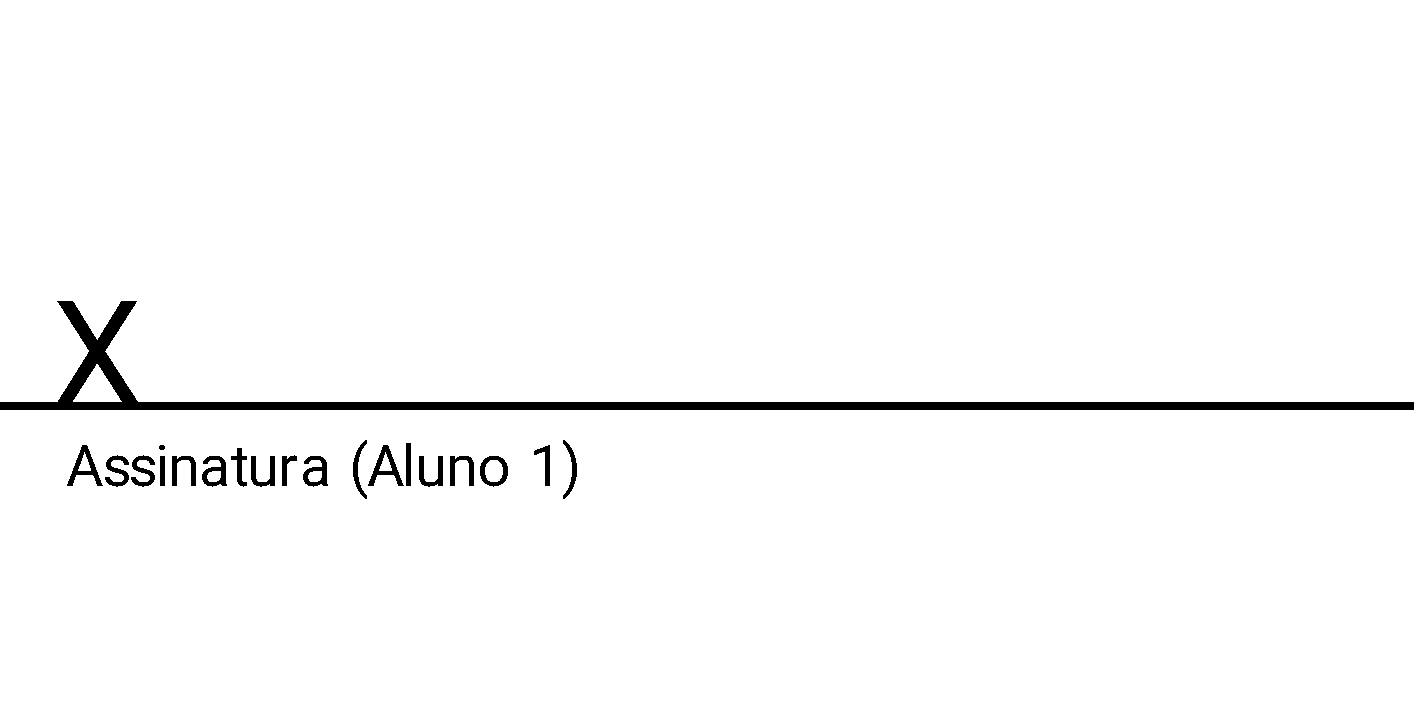
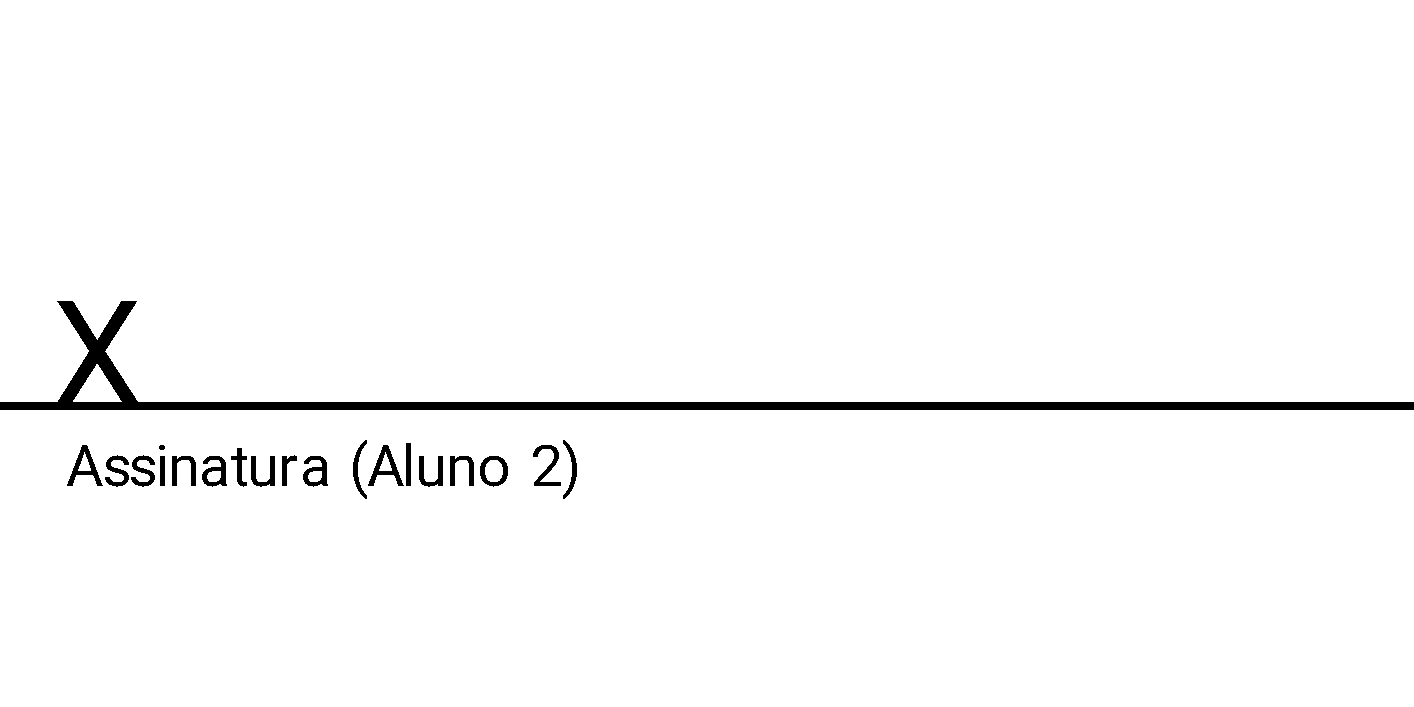
| **Aluno 2** |  |
| --- | --- |
| Matrícula |  |
| E-mail |  |
| Telefone |  |
| Endereço |  |

**DADOS DA PROPOSTA**

Envolve: ( ) Humanos ( ) Animais ( ) Pesquisa de Campos

Laboratório necessário:

**São José dos Campos, 25 de novembro de 2024.**

***4.1.* Título do projeto:** Explorando Vulnerabilidades em Sistemas IoT baseados em ESP32 e Propondo Soluções de Segurança

**Introdução e Justificativa:**

Nos últimos anos, a Internet das Coisas (IoT) tem se expandido rapidamente, conectando dispositivos físicos a redes digitais e criando novas oportunidades em diversas áreas, como automação residencial, saúde, agricultura e indústria. Entre os dispositivos mais utilizados em sistemas IoT está o ESP32, um microcontrolador de baixo custo, eficiente e com capacidade de se conectar a redes Wi-Fi e Bluetooth. Devido ao seu custo acessível e alta versatilidade, o ESP32 tornou-se uma escolha popular para diversos projetos IoT. No entanto, à medida que o uso desses dispositivos aumenta, surgem questões importantes relacionadas à segurança, uma vez que muitos desses sistemas não foram projetados com robustez suficiente para resistir a ataques cibernéticos. As vulnerabilidades nos dispositivos baseados em ESP32 podem ser exploradas para comprometer a privacidade dos usuários, roubo de dados sensíveis e até mesmo causar danos físicos a sistemas industriais e de saúde.

Dado o crescimento contínuo da IoT e a inserção cada vez mais ampla de dispositivos como o ESP32 em ambientes críticos, torna-se essencial investigar as falhas de segurança desses sistemas e propor soluções eficazes para protegê-los.

O tema proposto se justifica pela crescente dependência de dispositivos conectados e a necessidade de garantir que esses sistemas, especialmente os baseados em ESP32, sejam seguros contra ameaças cibernéticas. Com a rápida expansão da IoT, a segurança desses dispositivos se torna uma prioridade, pois falhas de segurança podem levar a consequências graves, como o comprometimento de dados privados, ataques a infraestruturas críticas e danos econômicos significativos.

A questão central deste trabalho é: quais são as principais vulnerabilidades de segurança presentes em sistemas IoT baseados em ESP32 e como podemos protegê-los de forma eficaz? Além disso, surgem outros questionamentos importantes, como: Quais são as limitações de segurança dos dispositivos ESP32 e quais soluções podem ser implementadas para mitigar essas falhas sem comprometer o desempenho e custo dos dispositivos? Essas perguntas são fundamentais para a evolução de práticas seguras no design e implementação de sistemas IoT.

Dado o crescente número de dispositivos conectados à internet e o aumento das ameaças cibernéticas, o tema deste trabalho é de grande relevância, pois contribui para o desenvolvimento de soluções práticas de segurança em IoT. O foco será em dispositivos de baixo custo, como o ESP32, que são amplamente utilizados, mas frequentemente carecem de recursos de segurança avançados.

A pesquisa será conduzida com uma análise das vulnerabilidades mais comuns em sistemas IoT baseados no ESP32, utilizando testes de segurança para identificar pontos fracos e, em seguida, propondo soluções viáveis para melhorar a proteção desses sistemas. Espera-se que os resultados deste trabalho ofereçam contribuições significativas para a segurança de dispositivos IoT, beneficiando áreas como automação residencial, saúde digital e outros setores dependentes de dispositivos conectados.

A segurança da informação é uma área crítica, especialmente com o crescimento da IoT, que está cada vez mais presente em sistemas críticos e em dispositivos usados no cotidiano. A proteção desses sistemas contra ataques cibernéticos é essencial para garantir a integridade dos dados, a privacidade dos usuários e a continuidade das operações. Este trabalho tem relevância direta na área de segurança cibernética e pode contribuir para a criação de práticas e ferramentas que ajudem a proteger dispositivos IoT em uma variedade de contextos, desde casas inteligentes até sistemas industriais e de saúde.

**Objetivos:**

O objetivo principal deste trabalho é analisar as vulnerabilidades de segurança em sistemas IoT baseados em ESP32 e propor soluções para mitigá-las, com o intuito de garantir a proteção desses dispositivos contra potenciais ataques cibernéticos. O estudo buscará identificar as falhas de segurança mais comuns nestes sistemas, considerando tanto as vulnerabilidades presentes nos protocolos de comunicação quanto nas características de hardware e software dos dispositivos.

Além disso, pretende-se investigar abordagens e técnicas de segurança aplicáveis a dispositivos IoT de baixo custo, como o ESP32, focando em estratégias que possam ser implementadas de forma eficiente e acessível. (*LIMA,* A pesquisa explorará soluções como criptografia, autenticação de dispositivos e segurança no gerenciamento de firmware, com a finalidade de proteger os sistemas IoT sem comprometer significativamente seu desempenho ou custo.

Outro objetivo relevante será avaliar o impacto da implementação dessas soluções no desempenho dos dispositivos, garantindo que as abordagens de segurança sejam viáveis e práticas para aplicações reais. Ao final, espera-se que o trabalho contribua com recomendações valiosas para o desenvolvimento de sistemas IoT mais seguros, ajudando a promover uma maior conscientização sobre a importância da segurança em dispositivos conectados e oferecendo uma base para práticas mais robustas na área.

**Cronograma de atividades:**

| **Atividades a serem desenvolvidas** | **Fev/25** | **Mar/25** | **Abr/25** | **Jun/25** | **Jul/25** | **Ago/25** | **Set/25** | **Out/25** | **Nov/25** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Levantamento de referencial teórico e definição do escopo do trabalho | X |  |  |  |  |  |  |  |  |
| Análise das vulnerabilidades do ESP32 e definição do protótipo inicial | X | X |  | X |  |  |  |  |  |
| Pesquisa e análise de soluções de segurança para IoT | X | X | X | X |  |  |  |  |  |
| Implementação inicial e testes do protótipo (incluindo falhas de segurança) |  | X | X | X | X |  |  |  |  |
| Implementação e ajuste de soluções de segurança no protótipo |  |  | X | X | X | X |  |  |  |
| Redação do TCC (Metodologia, Resultados, Discussão) |  |  | X | X | X | X | X |  |  |
| Revisão final, ajustes e preparação para defesa |  |  |  |  | X | X | X | X |  |

**Referências:**