Beatriz, Brenda, Maria Eduarda B. e Victor Hugo

Situação Desafiadora

- Revisão de termos -

Limeira – 2026

SITUAÇÃO-PROBLEMA INTEGRADORA - “Cruzamento 4.0”

O Desafio - A Prefeitura identificou um cruzamento crítico na região central onde:

● O semáforo falha durante horários de pico.

● A comunicação IoT entre os sensores e o controlador cai intermitentemente.

● O servidor local que processa dados de tráfego está lento e apresenta falhas de segurança.

● Requisitos antigos foram mal documentados, gerando confusão sobre como o sistema deveria reagir em situações excepcionais, como chuva intensa ou interrupção de energia.

A CET contratou sua equipe para:

Propor, documentar e prototipar uma solução mínima viável (MVP) que envolva:

1. Requisitos completos e revisados
2. Arquitetura de rede IoT funcional e segura
3. Rotinas de programação do algoritmo do semáforo inteligente
4. Validação operacional e segurança no sistema operacional escolhido

FASE 1 — LEVANTAMENTO DE REQUISITOS

REQUISITOS FUNCIONAIS

1. Deve detectar o volume de tráfego em cada via do cruzamento utilizando sensores.
2. Ajusta a duração dos sinais verde e amarelo com base no fluxo de tráfego em tempo real.
3. Permite o controle manual remoto dos sinais de tráfego por um operador.
4. Registra e armazena dados de tráfego, falhas de sensores e alarmes em um banco de dados central.
5. Entra em modo de alerta (amarelo piscante para todas as direções) se a comunicação com o servidor principal for perdida.
6. Aciona um modo de operação pré-programado em caso de falha de um ou mais sensores de tráfego.
7. Envia alertas automáticos por e-mail ou SMS para a equipe de manutenção em caso de falha do equipamento.
8. Adapta a temporização dos sinais em condições climáticas adversas detectadas via sensor de clima.

REQUISITOS NÃO FUNCIONAIS

1. **(Confiabilidade):** O sistema deve funcionar corretamente principalmente nos horários de pico.
2. **(Desempenho):** O tempo de resposta para ajustar a temporização do semáforo com base nos dados dos sensores.
3. **(Segurança):** A comunicação entre sensores, controlador e servidor deve ser criptografada.
4. **(Usabilidade):** A interface de gerenciamento deve ser intuitiva e requerer treinamento mínimo.
5. **(Escalabilidade):** O sistema deve suportar até 50 cruzamentos adicionais sem perda de desempenho.
6. **(Disponibilidade):** O controlador local deve ter uma fonte de alimentação ininterrupta que garanta pelo menos 2 horas de operação em caso de queda de energia.

HISTÓRIAS DE USUÁRIO

- Como **motorista**, o **tempo do sinal verde seja ajustado automaticamente** com base no fluxo de carros, para reduzir **o tempo de espera** no cruzamento.
- Como **técnico de manutenção**, **receber alertas imediatos no celular** quando um sensor falhar, para **consertá-lo rapidamente** e evitar problemas de tráfego.
- Como **operador de tráfego**, **acessar remotamente a interface do sistema** para **controlar manualmente o semáforo** em caso de emergências (como acidentes), para que **possa gerenciar o fluxo de forma segura**.

PRIORIZAÇÃO

- MUST HAVE (DEVE TER)
- SHOULD HAVE (DEVERIA TER)
- COULD HAVE (PODERIA TER)
- WON´T HAVE (NÃO TERÁ)

Requisito	Priorização	Explicação
RF1, RF2, RNF1, RNF2	**MUST HAVE**	Essenciais para a funcionalidade básica e segurança do semáforo inteligente.
RF5, RF6, RNF6	**MUST HAVE**	*Críticos para a operação em modo de falha e garantia de disponibilidade mínima.*
RNF3	**MUST HAVE**	Aborda as falhas de segurança identificadas no servidor antigo.
RF4, RF7	**SHOULD HAVE**	Importantes para manutenção proativa e análise de dados futuros.
RF3	**SHOULD HAVE**	Controle manual é importante, mas não a prioridade do sistema "inteligente".
RF8, RNF4, RNF5	**COULD HAVE**	Recursos adicionais que agregam valor.

FASE 2 — MODELAGEM DO SISTEMA E ARQUITETURA IOT

Topologia selecionada: Estrela

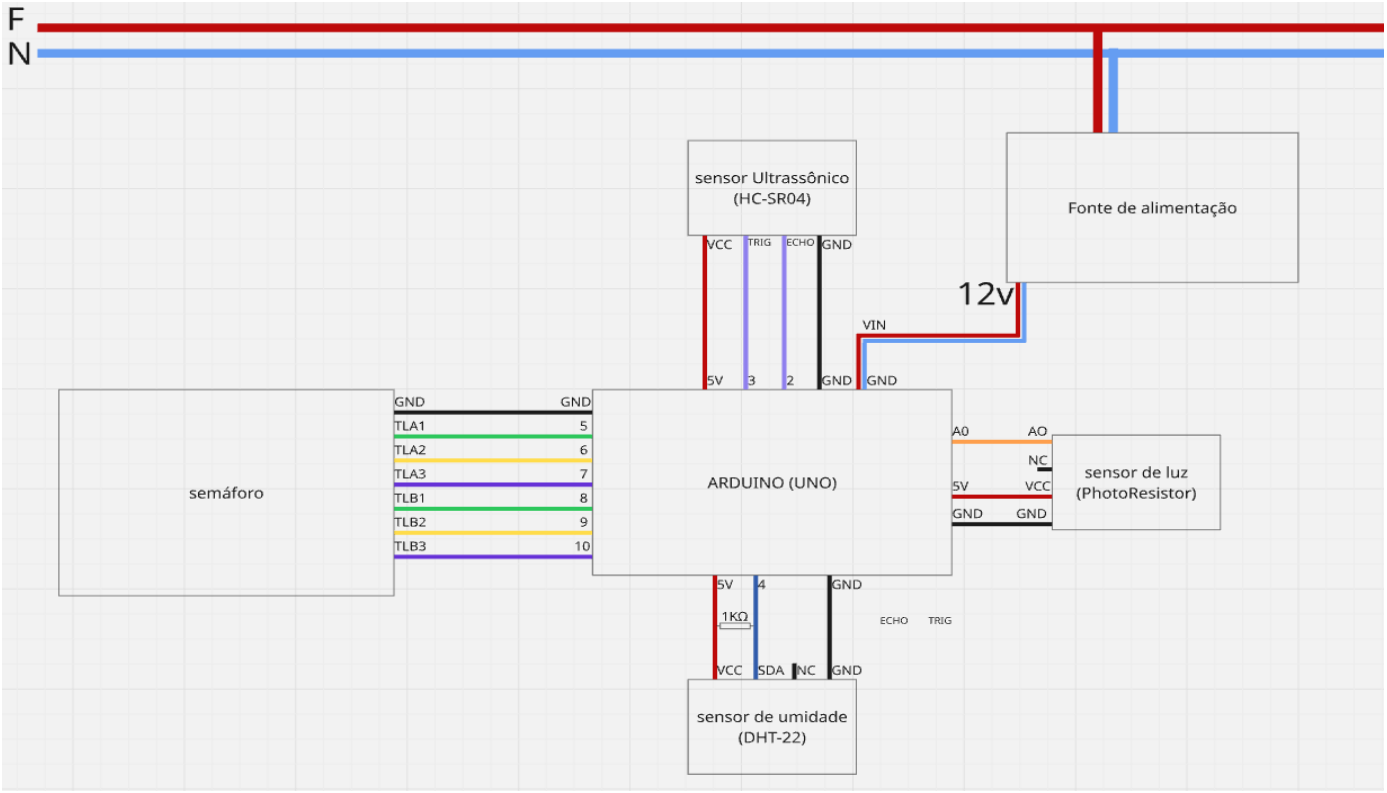
Motivos: O Arduino terá total controle dos demais dispositivos conectados dentro do circuito, tanto para capitação de dados através dos sensores, como controlar os LEDs presentes no semáforo, e atuar em casos de falha de sensores ou de conexão com o servidor.

Definição da Topologia Estrela:

A topologia estrela é uma arquitetura de rede onde todos os dispositivos são conectados a um nó central (hub ou switch), que gerencia e controla toda a comunicação. Cada dispositivo se comunica exclusivamente através deste ponto central, facilitando o gerenciamento e isolamento de falhas. Esta configuração oferece alta confiabilidade, pois a falha de um dispositivo não afeta os demais, apenas sua própria conexão com o nó central. (IT,2021)

PRÓS:	CONTRAS:
Gerenciamento conveniente de um local central	*Se o hub central falhar, toda a sua rede cairá*
Se um nó falhar, a rede ainda funciona	*O desempenho e a largura de banda são limitados pelo nó central*
Os dispositivos podem ser adicionados ou removidos sem interromper a rede	*Pode ser caro para operar*
Mais fácil de identificar e isolar problemas de desempenho	

DIAGRAMA FUNCIONAL

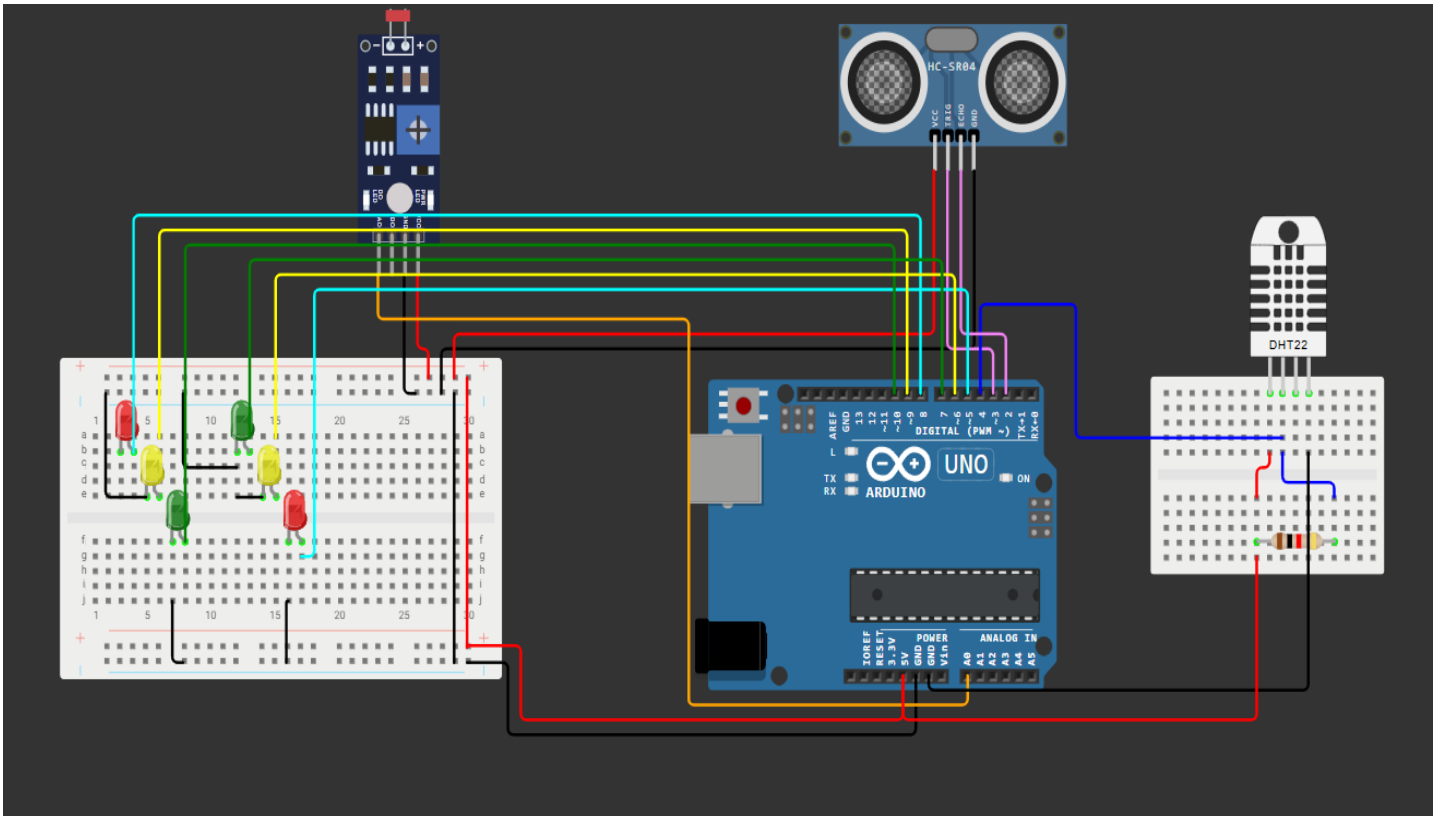


- **Arduino (UNO): O "cérebro" do sistema. É o microcontrolador responsável por ler os dados de todos os sensores e, com base na programação, controlar o acionamento das luzes do semáforo.**
- **Fonte de Alimentação: Responsável por converter a energia da rede elétrica (Fase F e Neutro N) para uma tensão contínua de 12V, alimentando o Arduino através do pino VIN para que ele funcione sem precisar da USB do computador.**
- **Semáforo (Atuador): O dispositivo de saída visual. Possui conexões para dois grupos de luzes (TLA1-3 e TLB1-3), sugerindo o controle de duas vias ou faixas diferentes, conectados aos pinos digitais 5 a 10.**
- **Sensor Ultrassônico (HC-SR04): Sensor de distância conectado aos pinos 2 e 3. Neste contexto, é geralmente utilizado para detectar a presença de veículos ou**

pedestres aguardando o sinal, permitindo um tempo de abertura inteligente.

- **Sensor de Luz (PhotoResistor/LDR): Conectado à porta analógica A0. Serve para medir a luminosidade do ambiente, permitindo que o sistema saiba se é dia ou noite (o que pode alterar o modo de operação do semáforo para economizar energia ou piscar em alerta).**
- **Sensor de Umidade (DHT-22): Conectado ao pino digital 4. Monitora a umidade relativa do ar e temperatura, agregando funções de monitoramento climático ao sistema de trânsito.**

Arquitetura de rede IoT:



Codigo:

```
#include <DHT.h>

// Definição de Pinos
#define PIN_TRIG 3
#define PIN_ECHO 2
#define LDR A0
#define PIN_DHT 4

// Configuração dos Semáforos (R, Y, G)
int tLightsA[3] = {5, 6, 7};
int tLightsB[3] = {8, 9, 10};

DHT dht(PIN_DHT, DHT22);

void setup() {
  Serial.begin(9600);
  pinMode(PIN_TRIG, OUTPUT);
  pinMode(PIN_ECHO, INPUT);
  dht.begin();

  // Inicializa pinos dos LEDs
  for(int i = 0; i <= 2; i++) {
    pinMode(tLightsA[i], OUTPUT);
    pinMode(tLightsB[i], OUTPUT);
  }
}

void loop() {
  float valueHumidity;

  while (true) {
    int distance = checkFlow();
    valueHumidity = dht.readHumidity();

    // 1. Verificação de Segurança (Chuva ou Erro de Sensor)
    if(valueHumidity >= 90 || distance == 0) {
      blinkYellowAlert();
      break; // Reinicia o loop para nova verificação
    }

```

Equipamentos de rede:

1. **Roteador:** Dispositivo responsável por conectar a rede local (LAN) à internet (WAN). Gerencia o tráfego de dados entre diferentes redes, atribuindo endereços IP aos dispositivos através do protocolo DHCP e realizando NAT (Network Address Translation) para permitir que múltiplos dispositivos compartilhem um único endereço IP público.
2. **Firewall:** Sistema de segurança que monitora e controla o tráfego de rede baseado em regras de segurança predefinidas. Protege a rede contra acessos não autorizados, ataques cibernéticos e malwares, filtrando pacotes de dados que entram e saem da rede. Pode ser implementado em hardware, software ou ambos.
3. **Servidor Local:** Computador ou sistema dedicado que fornece serviços, recursos e dados para outros dispositivos (clientes) na rede local. No contexto IoT, pode hospedar aplicações de gerenciamento, bancos de dados para armazenar leituras dos sensores, APIs para comunicação com dispositivos e interfaces de visualização de dados em tempo real.
4. **Switch:** Equipamento que conecta múltiplos dispositivos em uma rede local (LAN), operando na camada de enlace de dados. Encaminha dados apenas para o dispositivo de destino específico através de endereços MAC, otimizando o desempenho da rede ao reduzir colisões e criar domínios de colisão separados para cada porta.
5. **Access Point:** Dispositivo que cria uma rede sem fio (Wi-Fi) permitindo que dispositivos se conectem à rede local através de conexão wireless. Funciona como uma ponte entre a rede cabeada e os dispositivos sem fio, expandindo a cobertura da rede e possibilitando mobilidade aos usuários e dispositivos IoT compatíveis com Wi-Fi.

Referências Bibliográficas:

IT, I. Topologia de Rede: Conheça os principais tipos. Disponível em: https://www.internationalit.com/post/topologia-de-rede-conheça-os-principais-tipos.

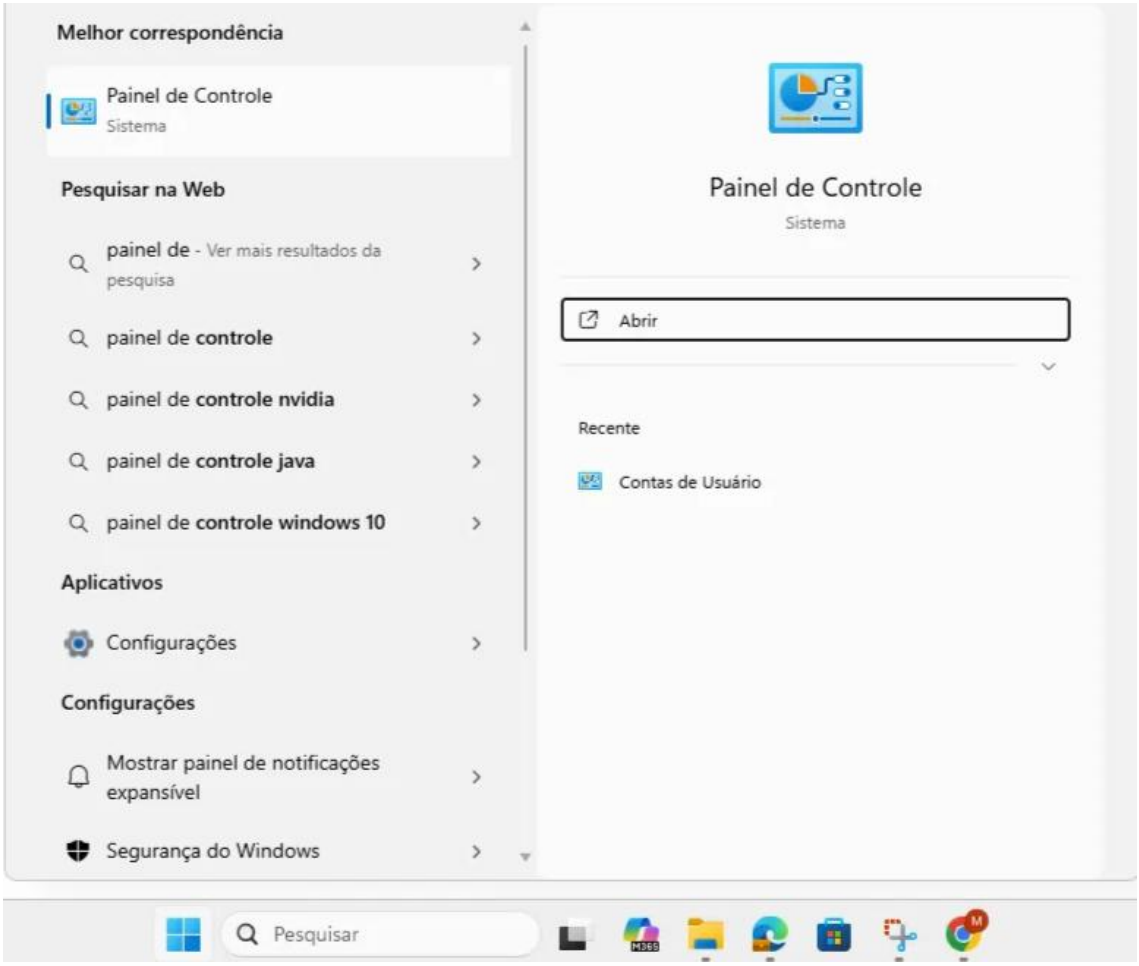
FASE 3 — SISTEMA OPERACIONAL E SEGURANÇA

Windows Server	Ubuntu Server
Custo: *Windows Server 2025 Datacenter (16 núcleos): cerca de R$ 58.000 a R$ 65.000* *(licença corporativa ampla).* *Ideal para datacenters com muitas máquinas virtuais.*	***Custo:*** *O sistema básico Ubuntu Server é totalmente gratuito para instalar e usar, sem custos de licenciamento. Você pode baixar, instalar e usar em servidores físicos ou virtuais sem pagar nada pelo sistema operacional.* *Em geral, planos de suporte corporativo começam em algo como US$ 500 por servidor/ano (~R$ 2.500+ por ano) para servidores com cobertura estendida.*
Segurança: • *É seguro quando bem configurado* • *Recebe atualizações frequentes da Microsoft* • *Tem controle centralizado (Active Directory e GPO)* • *Inclui firewall, antivírus e criptografia* • *Segurança depende de boa administração e manutenção* • *Mal configurado pode ser vulnerável.*	***Segurança:*** • *É muito seguro por padrão* • *Código aberto (auditoria constante da comunidade)* • *Atualizações rápidas de segurança* • *Usa permissões fortes (sudo, usuários separados)* • *Firewall simples e eficiente (UFW / iptables)* • *Poucos serviços ativos por padrão (menor superfície de ataque)* *Ubuntu Server é seguro, leve e confiável; a segurança depende principalmente de boa configuração e atualizações regulares.*

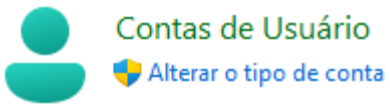
Suporte a IoT: • *Não é focado em IoT de borda* • *Usado como backend (banco de dados, AD, APIs, gerenciamento)* • *Integra bem com Azure IoT, MQTT, OPC UA* • *Windows IoT é o produto certo para dispositivos IoT, não o Windows Server* • *Windows Server gerencia e processa dados de IoT, mas* **não é feito para rodar diretamente nos dispositivos IoT.**	***Suporte a IoT:*** • *Muito usado em IoT* • *Pode rodar diretamente em dispositivos IoT (ARM, x86)* • *Ótimo para edge computing* • *Suporte nativo a dispositivos com poucos recursos, otimizando o uso de banda e energia por meio de protocolos como MQTT e OPC UA.* • *Base de muitas distros IoT (ex.: Ubuntu Core)* *Ubuntu Server é ideal para IoT, tanto nos dispositivos quanto no backend.*

Criar usuários

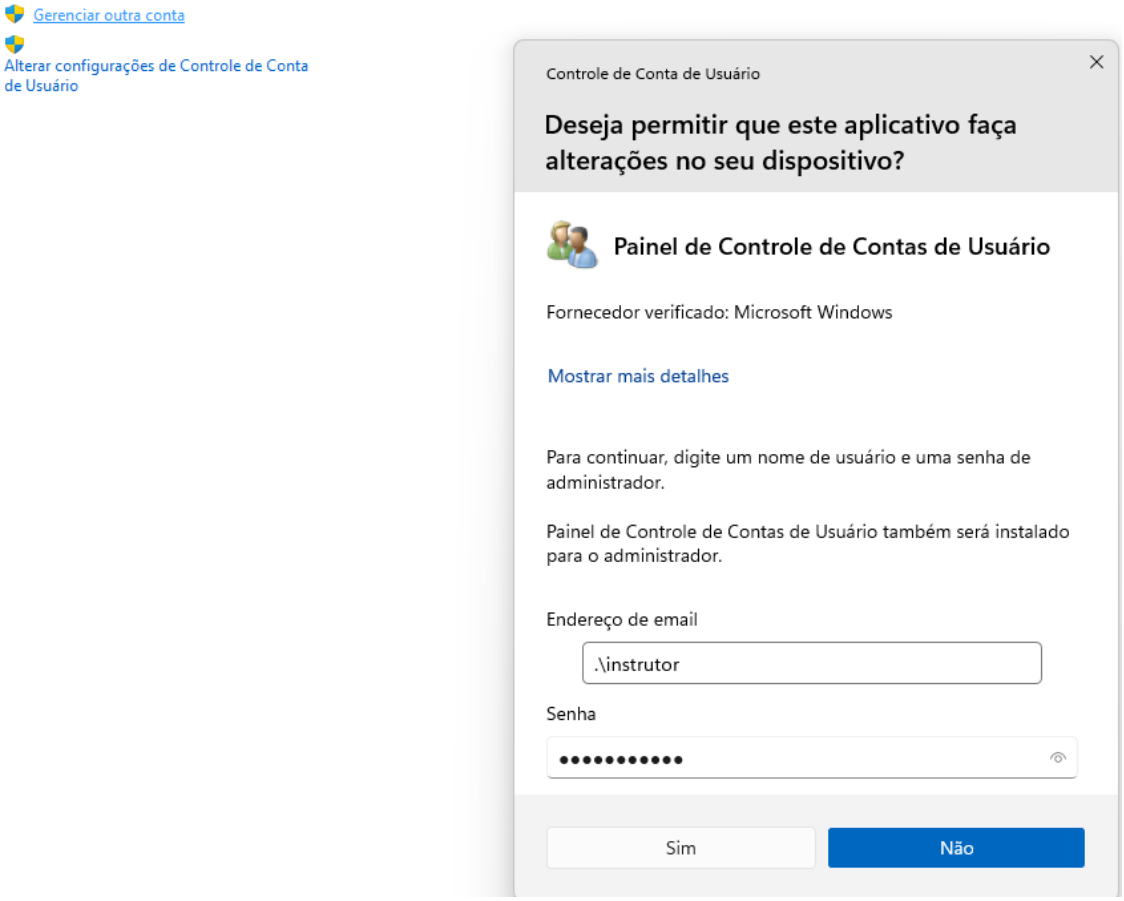
PASSO 1:



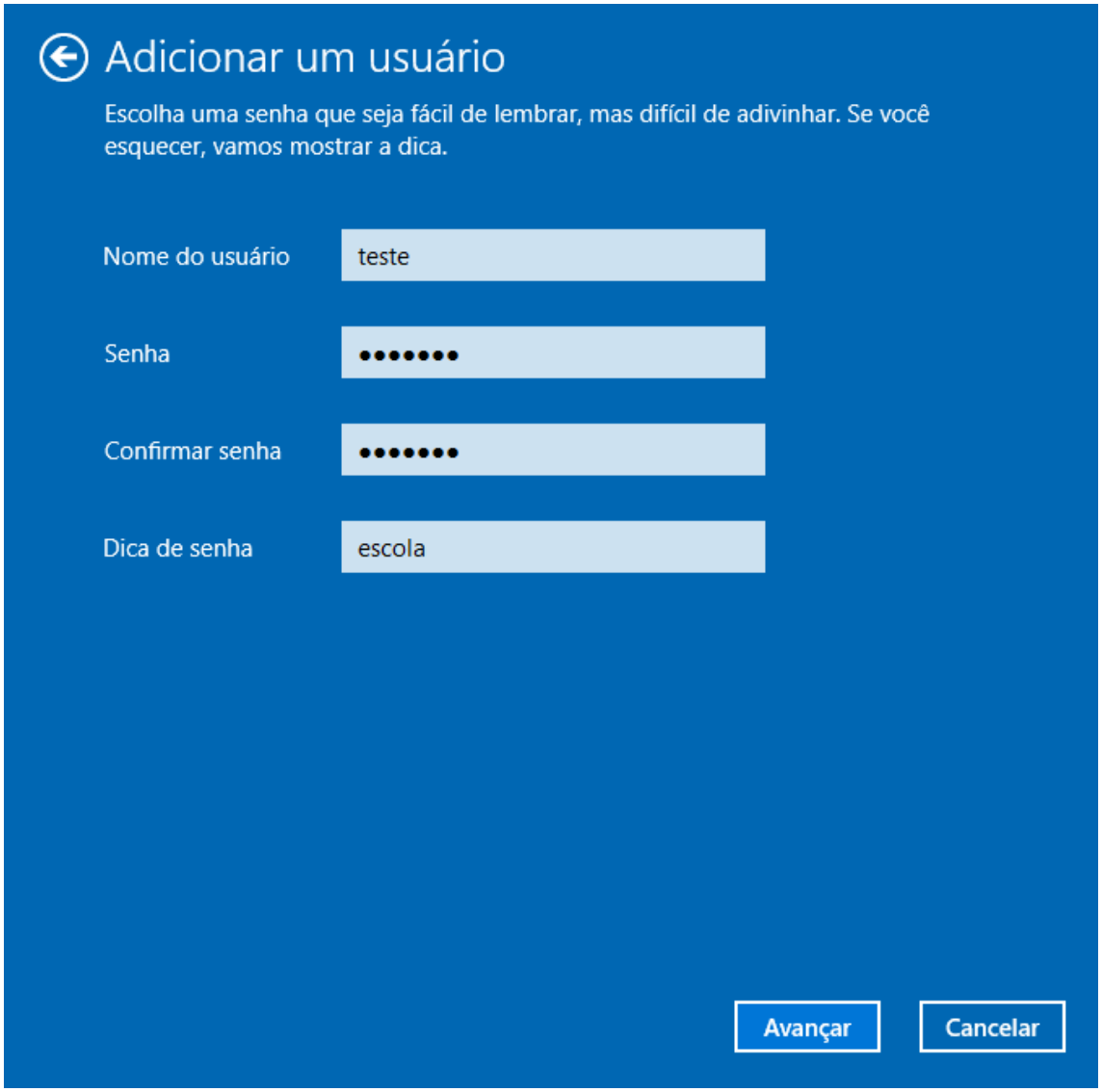
PASSO 2:



PASSO 3:

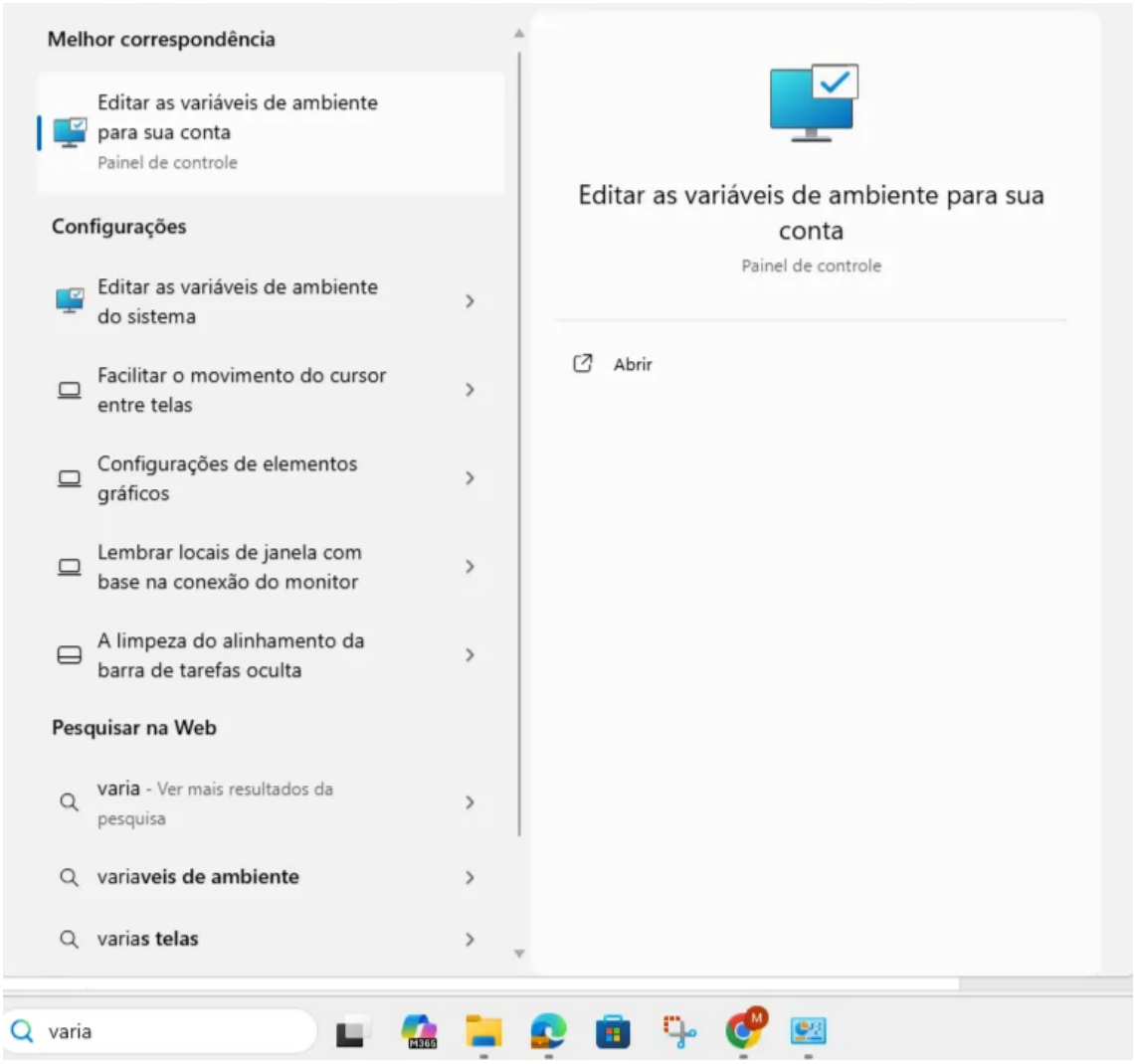

Gerenciar outra conta
Alterar configurações de Controle de Conta de Usuário
Controle de Conta de Usuário
Deseja permitir que este aplicativo faça alterações no seu dispositivo?
Painel de Controle de Contas de Usuário
Fornecedor verificado: Microsoft Windows
Mostrar mais detalhes
Para continuar, digite um nome de usuário e uma senha de administrador.
Painel de Controle de Contas de Usuário também será instalado para o administrador.
Endereço de email
.\instrutor
Senha
Sim
Não

PASSO 4:

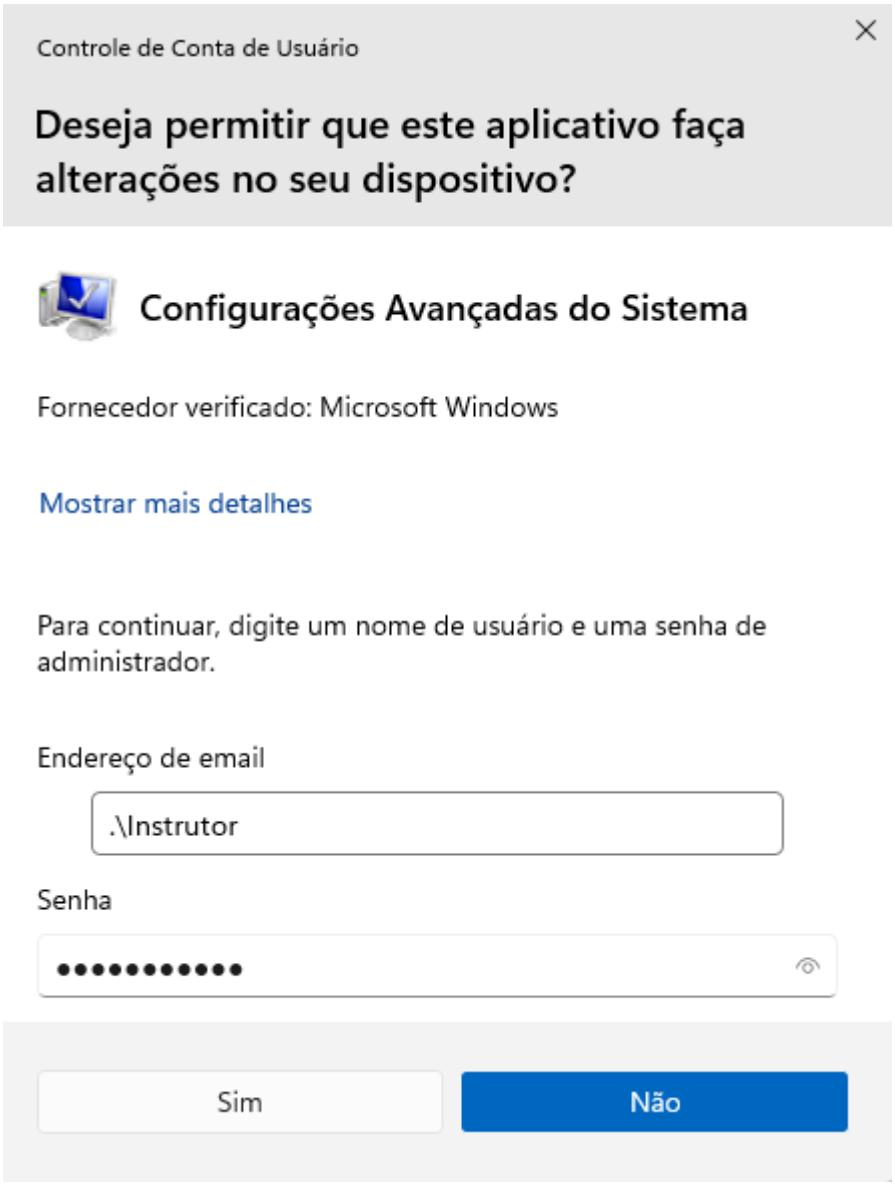

Adicionar um usuário
Escolha uma senha que seja fácil de lembrar, mas difícil de adivinhar. Se você esquecer, vamos mostrar a dica.
Nome do usuário
teste
Senha
Confirmar senha
Dica de senha
escola
Avançar
Cancelar

Ajustar variáveis de ambiente

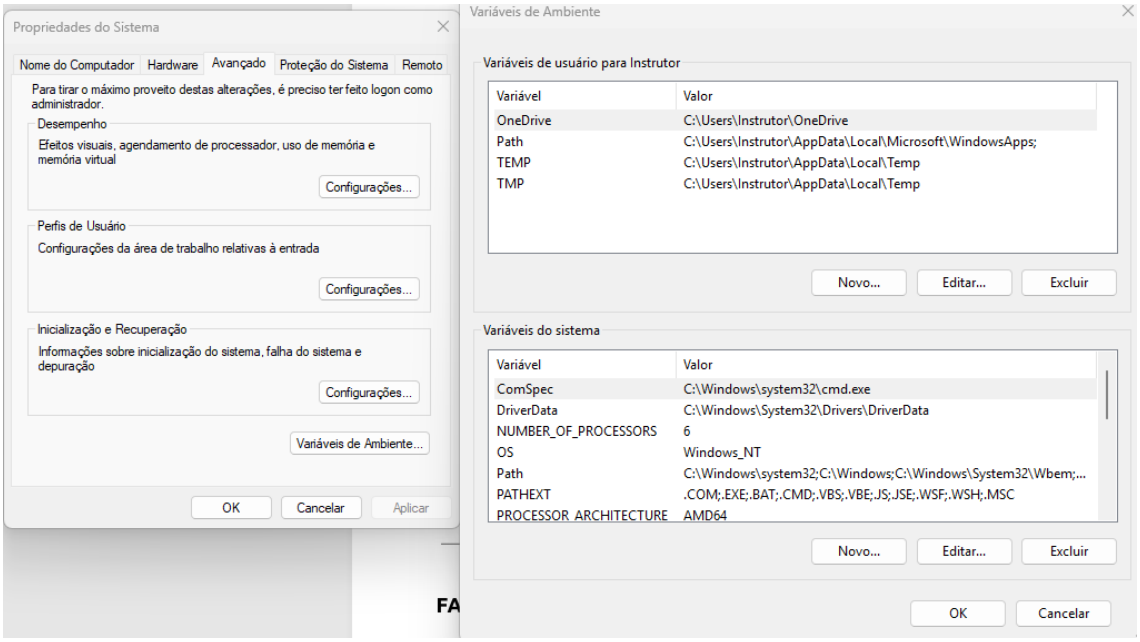
PASSO 1:



PASSO 2:

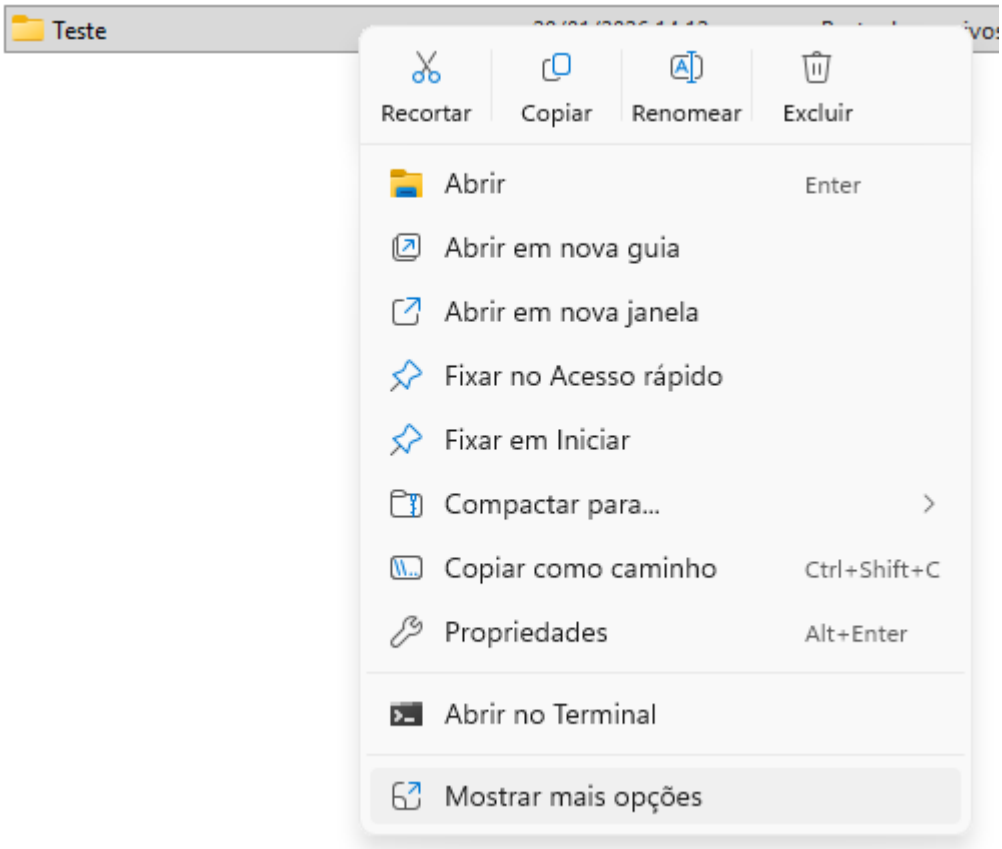

Controle de Conta de Usuário
Deseja permitir que este aplicativo faça alterações no seu dispositivo?
Configurações Avançadas do Sistema
Fornecedor verificado: Microsoft Windows
Mostrar mais detalhes
Para continuar, digite um nome de usuário e uma senha de administrador.
Endereço de email
.\Instrutor
Senha
Sim
Não

PASSO 3:

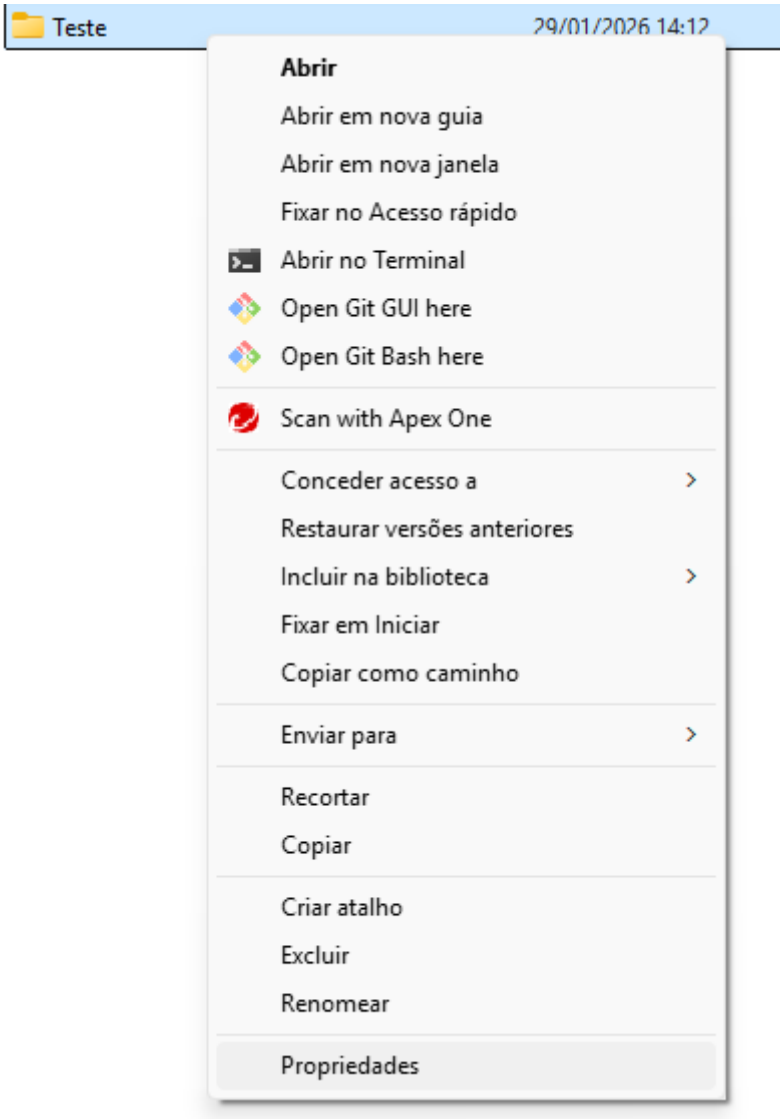


Configurar pastas compartilhadas

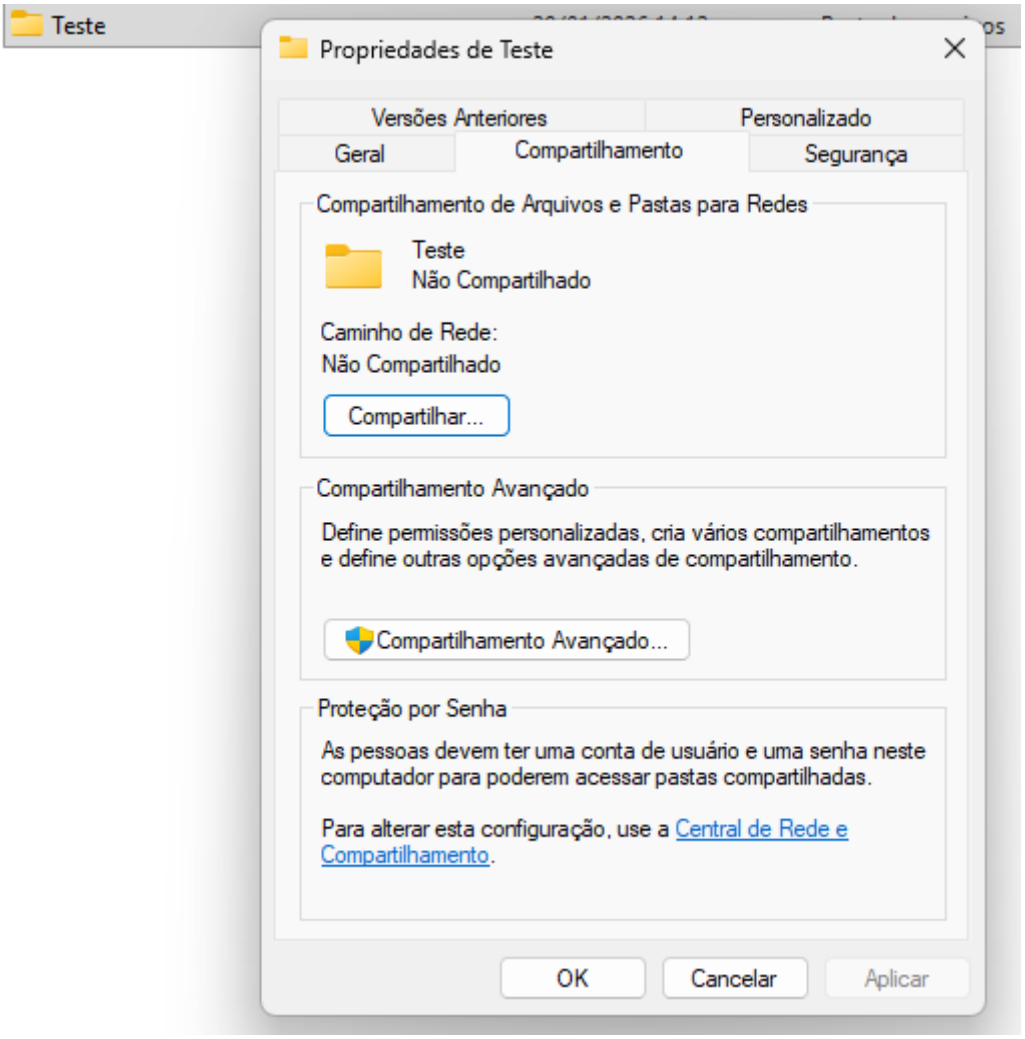
PASSO 1:



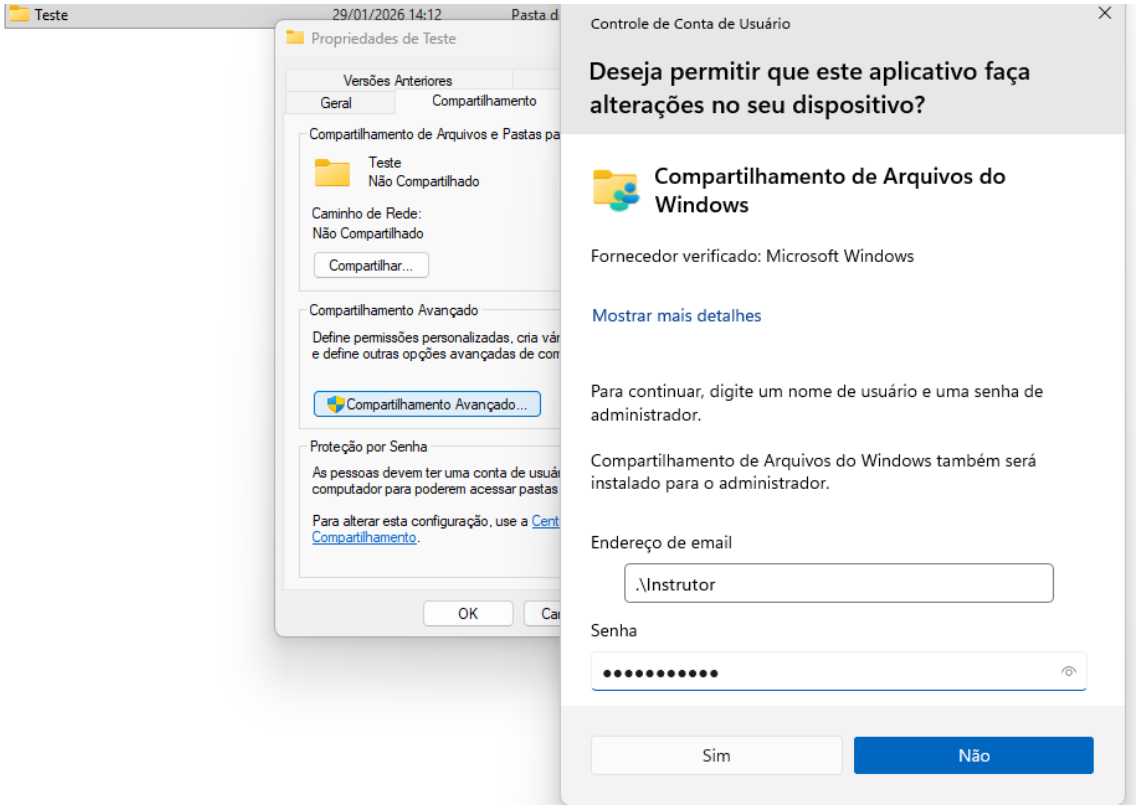
PASSO 2:


Teste
29/01/2026 14:12
Abrir
Abrir em nova guia
Abrir em nova janela
Fixar no Acesso rápido
Abrir no Terminal
Open Git GUI here
Open Git Bash here
Scan with Apex One
Conceder acesso a
Restaurar versões anteriores
Incluir na biblioteca
Fixar em Iniciar
Copiar como caminho
Enviar para
Recortar
Copiar
Criar atalho
Excluir
Renomear
Propriedades

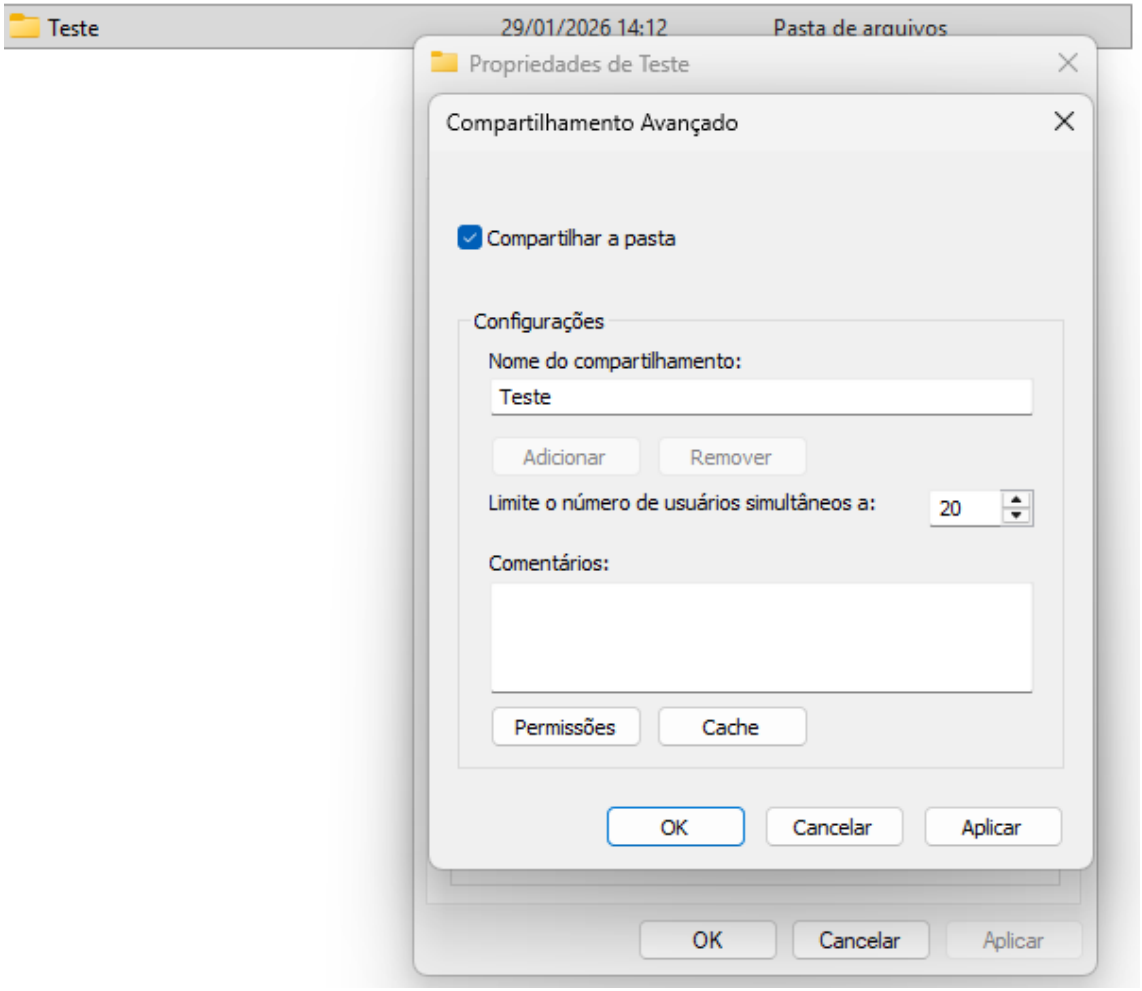
PASSO 3:


Teste
Propriedades de Teste
Versões Anteriores
Personalizado
Geral
Compartilhamento
Segurança
Compartilhamento de Arquivos e Pastas para Redes
Teste
Não Compartilhado
Caminho de Rede:
Não Compartilhado
Compartilhar...
Compartilhamento Avançado
Define permissões personalizadas, cria vários compartilhamentos e define outras opções avançadas de compartilhamento.
Compartilhamento Avançado...
Proteção por Senha
As pessoas devem ter uma conta de usuário e uma senha neste computador para poderem acessar pastas compartilhadas.
Para alterar esta configuração, use a Central de Rede e Compartilhamento.
OK
Cancelar
Aplicar

PASSO 4:

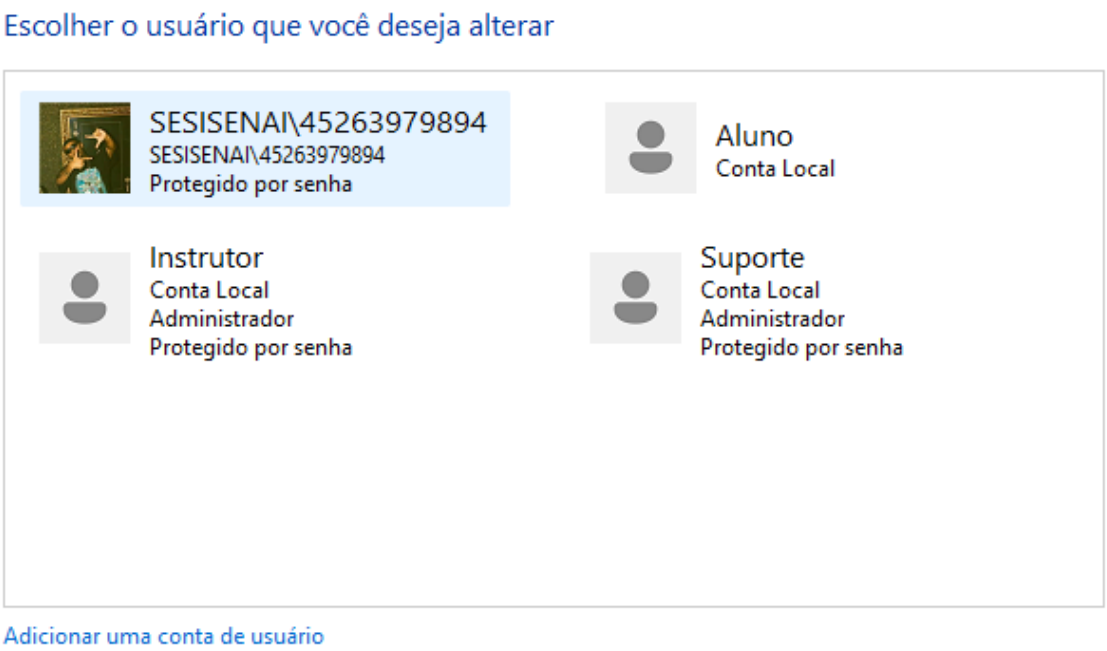

Teste
29/01/2026 14:12
Pasta d
Propriedades de Teste
Versões Anteriores
Geral
Compartilhamento
Compartilhamento de Arquivos e Pastas pa
Teste
Não Compartilhado
Caminho de Rede:
Não Compartilhado
Compartilhar...
Compartilhamento Avançado
Define permissões personalizadas, cria vár
e define outras opções avançadas de con
Compartilhamento Avançado...
Proteção por Senha
As pessoas devem ter uma conta de usuár
computador para poderem acessar pastas
Para alterar esta configuração, use a Cent
Compartilhamento.
OK
Ca
Controle de Conta de Usuário
Deseja permitir que este aplicativo faça alterações no seu dispositivo?
Compartilhamento de Arquivos do Windows
Fornecedor verificado: Microsoft Windows
Mostrar mais detalhes
Para continuar, digite um nome de usuário e uma senha de administrador.
Compartilhamento de Arquivos do Windows também será instalado para o administrador.
Endereço de email
.\Instrutor
Senha
Sim
Não

PASSO 5:


Teste
29/01/2026 14:12
Pasta de arquivos
Propriedades de Teste
Compartilhamento Avançado
Compartilhar a pasta
Configurações
Nome do compartilhamento:
Teste
Adicionar
Remover
Limite o número de usuários simultâneos a:
20
Comentários:
Permissões
Cache
OK
Cancelar
Aplicar
OK
Cancelar
Aplicar

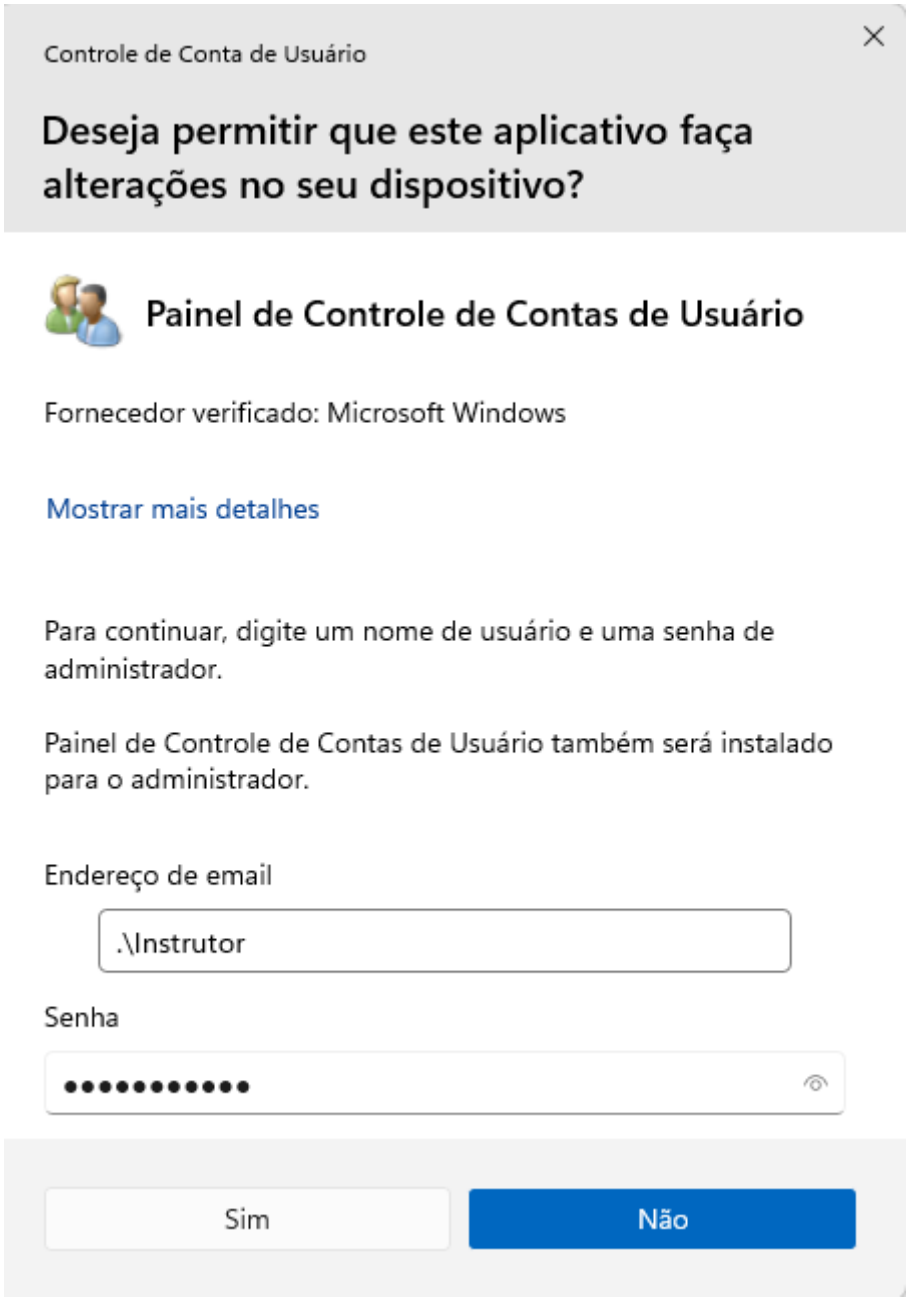
Definir permissões

PASSO 1:

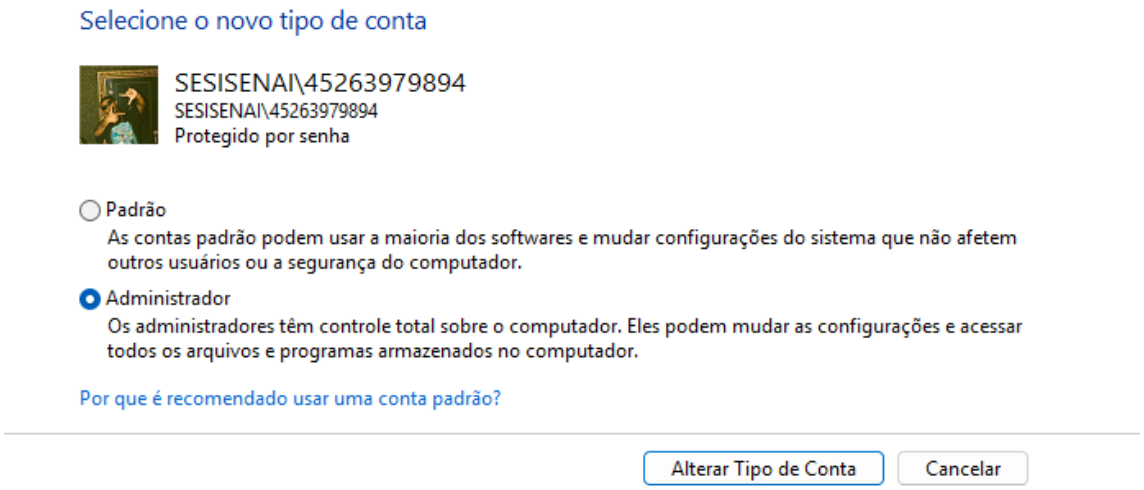


PASSO 2:

PASSO 3:

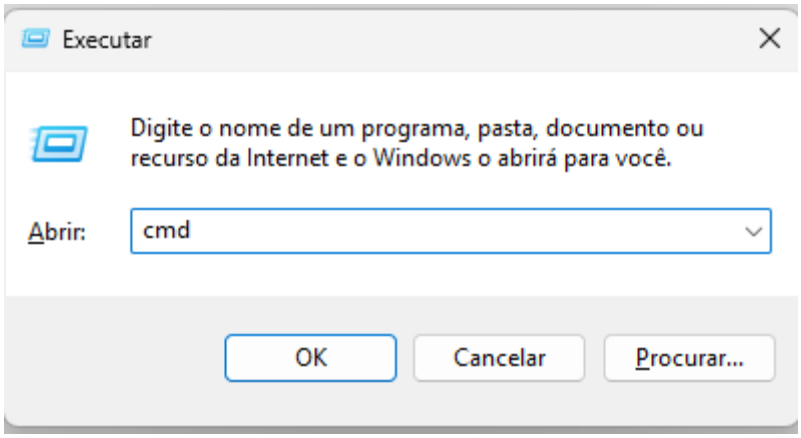

Controle de Conta de Usuário
Deseja permitir que este aplicativo faça alterações no seu dispositivo?
Painel de Controle de Contas de Usuário
Fornecedor verificado: Microsoft Windows
Mostrar mais detalhes
Para continuar, digite um nome de usuário e uma senha de administrador.
Painel de Controle de Contas de Usuário também será instalado para o administrador.
Endereço de email
.\Instrutor
Senha
Sim
Não

PASSO 4:

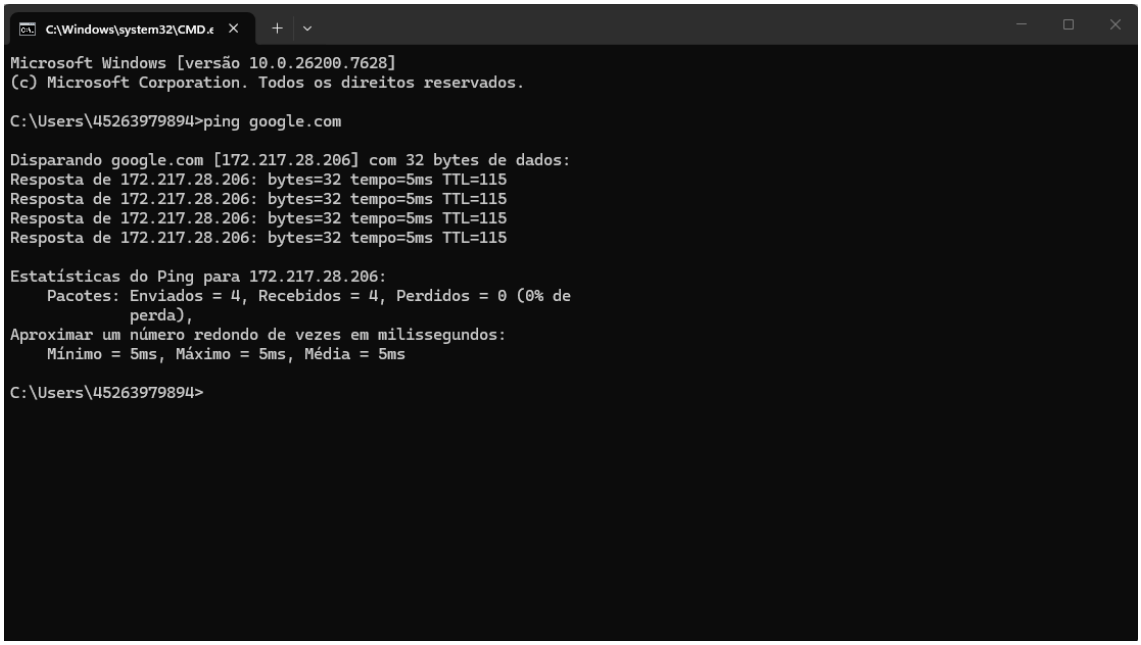


Testar navegação via terminal

PASSO 1:

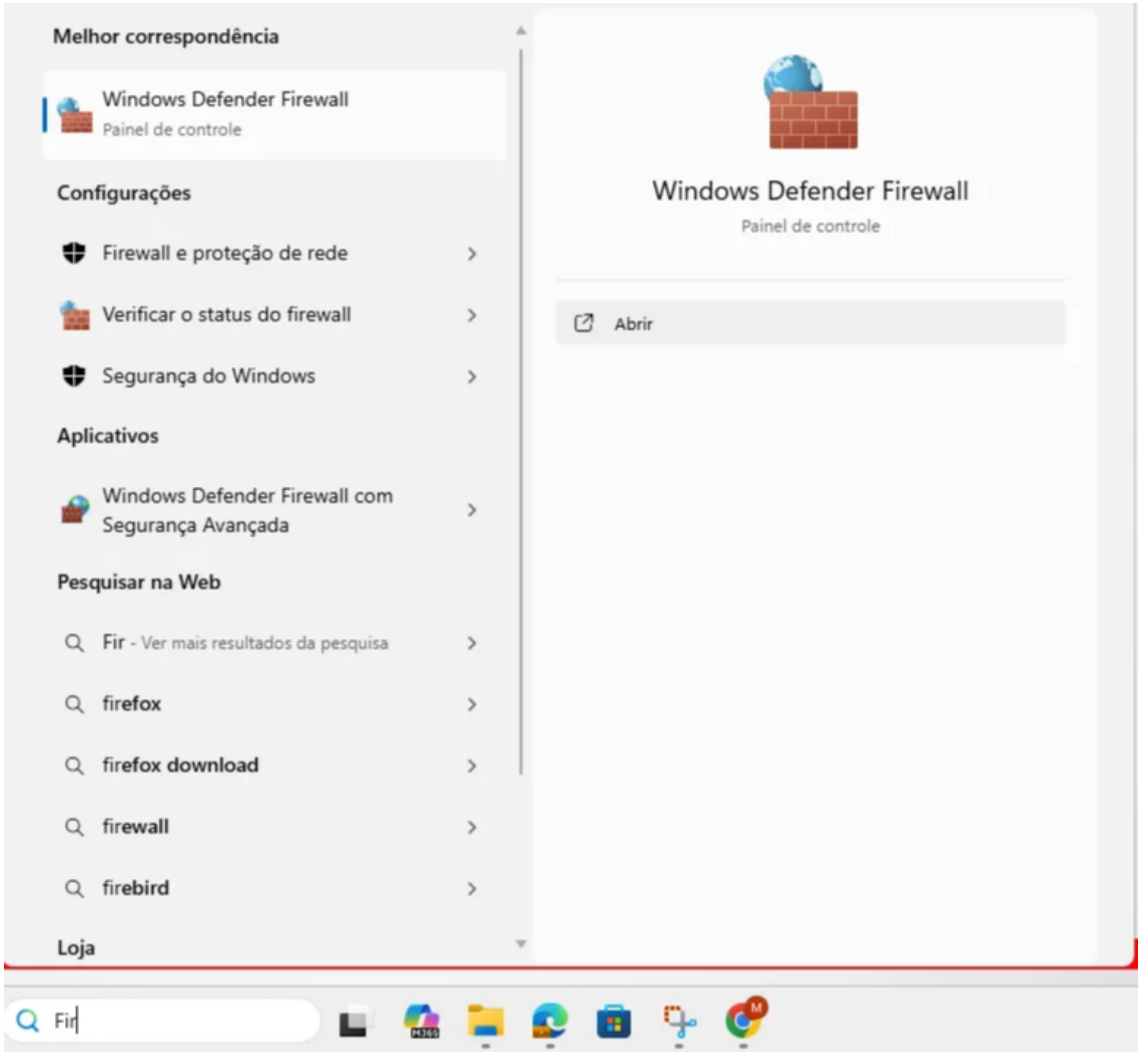


PASSO 2:


C:\Windows\system32\CMD.e
Microsoft Windows [versão 10.0.26200.7628]
(c) Microsoft Corporation. Todos os direitos reservados.
C:\Users\45263979894>ping google.com
Disparando google.com [172.217.28.206] com 32 bytes de dados:
Resposta de 172.217.28.206: bytes=32 tempo=5ms TTL=115
Resposta de 172.217.28.206: bytes=32 tempo=5ms TTL=115
Resposta de 172.217.28.206: bytes=32 tempo=5ms TTL=115
Resposta de 172.217.28.206: bytes=32 tempo=5ms TTL=115
Estatísticas do Ping para 172.217.28.206:
Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
perda),
Aproximar um número redondo de vezes em milissegundos:
Mínimo = 5ms, Máximo = 5ms, Média = 5ms
C:\Users\45263979894>

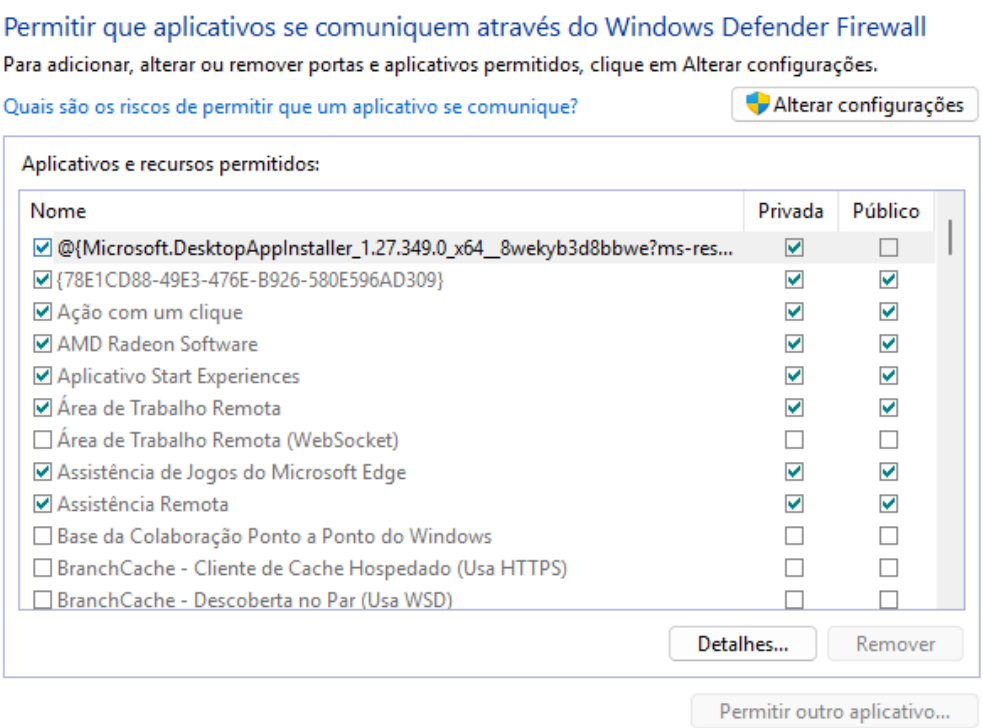
Configurar firewall permitindo somente portas usadas (ex.: 1883 para MQTT)

PASSO 1:



PASSO 2:

PASSO 3:



Mini Política de Segurança da Informação - (PSI)

Objetivo

Garantir a segurança básica do sistema, dos dados e dos equipamentos utilizados no laboratório.

Senhas

- **Utilizar senhas que não sejam fáceis de adivinhar.**
- **Não compartilhar senhas com outras pessoas.**
- **Trocar a senha quando houver suspeita de uso indevido.**

Acessos

- **Cada usuário deve ter seu próprio acesso.**
- **Apenas pessoas autorizadas podem usar o sistema.**
- **O acesso administrativo deve ser restrito.**

Backup

- **Os dados importantes devem ser salvos regularmente.**
- **Manter uma cópia de segurança em local seguro.**
- **O backup deve ser usado em caso de falha ou perda de dados.**

Procedimentos em Caso de Falha no Sensor

- **Verificar se o equipamento está ligado corretamente.**
- **Conferir conexões e funcionamento básico.**
- **Informar o responsável caso o problema continue.**

Proteção contra Engenharia Social

- **Não informar senhas ou dados pessoais.**
- **Desconfiar de mensagens ou pedidos suspeitos.**
- **Confirmar informações antes de fornecer qualquer dado.**

FASE 4 — ALGORITMO DO SEMÁFORO INTELIGENTE