

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	<i>Críticos para a operação em modo de falha e garantia de disponibilidade mínima.</i>
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

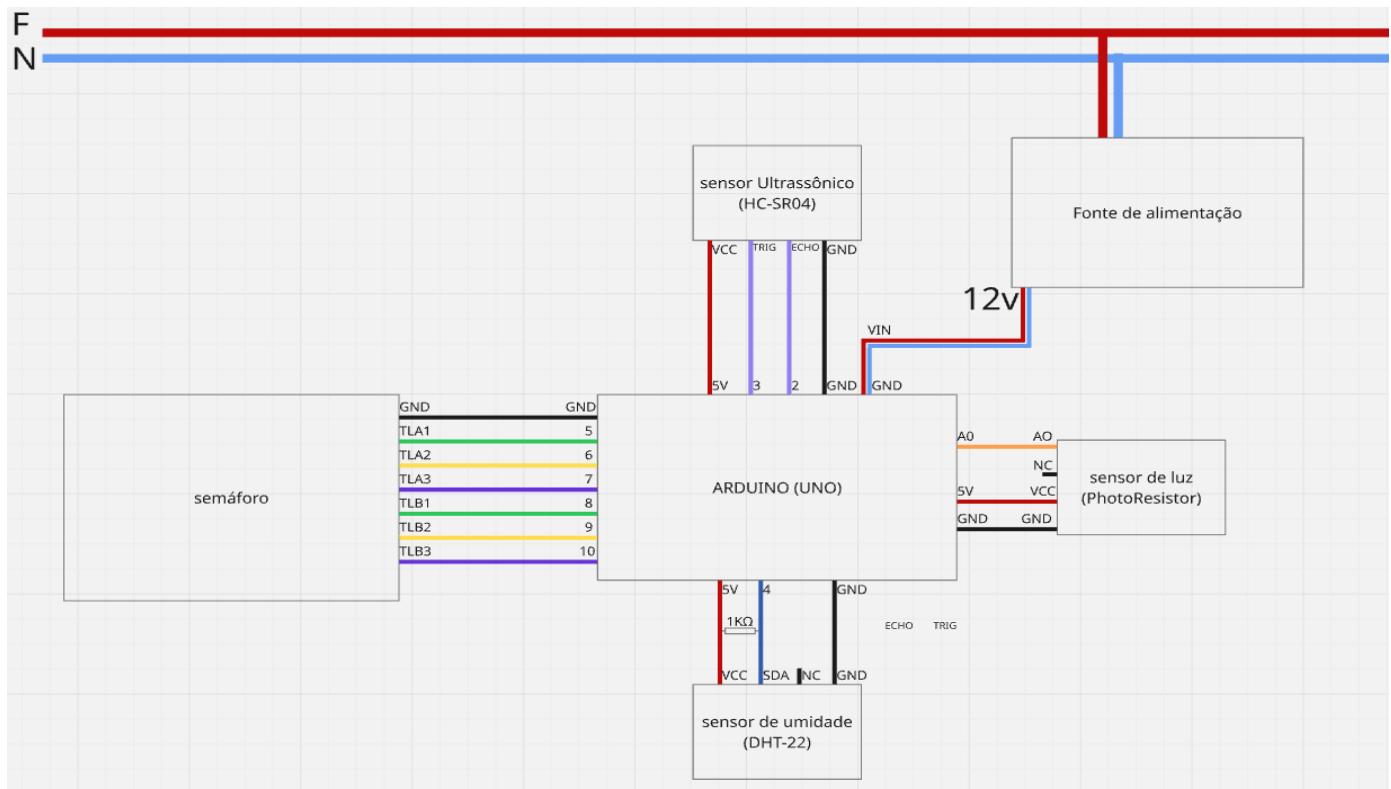
Motivos: O Arduino terá total controle dos demais dispositivos conectados dentro do circuito, tanto para captação de dados através dos sensores, como controlar os LEDs presentes no semáforo, e atuar em casos de falha de sensores ou de conexão com o servidor.

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

DIAGRAMA FUNCIONAL

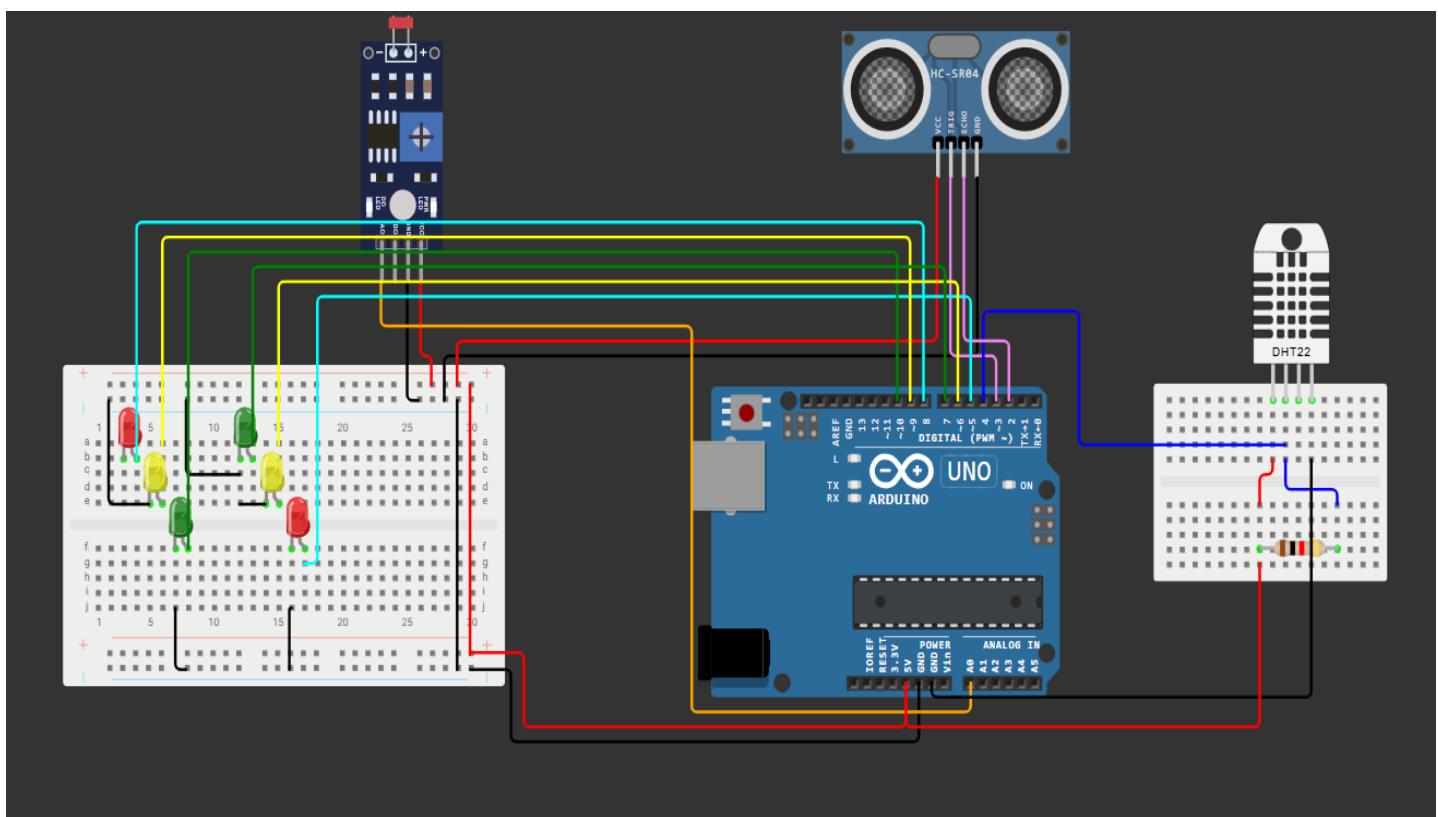


- **Arduino (UNO):** O "cérebro" do sistema. É o microcontrolador responsável por ler os dados de todos os sensores e, com base na programação, controlar o acionamento das luzes do semáforo.
- **Fonte de Alimentação:** Responsável por converter a energia da rede elétrica (Fase F e Neutro N) para uma 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:



Código:

```
● ● ●  
1 #include <DHT.h>  
2  
3 // Definição de Pinos  
4 #define PIN_TRIG 3  
5 #define PIN_ECHO 2  
6 #define LDR A0  
7 #define PIN_DHT 4  
8  
9 // Configuração dos Semáforos (R, Y, G)  
10 int tLightsA[3] = {5, 6, 7};  
11 int tLightsB[3] = {8, 9, 10};  
12  
13 DHT dht(PIN_DHT, DHT22);  
14  
15 void setup() {  
16     Serial.begin(9600);  
17     pinMode(PIN_TRIG, OUTPUT);  
18     pinMode(PIN_ECHO, INPUT);  
19     dht.begin();  
20  
21     // Inicializa pinos dos LEDs  
22     for(int i = 0; i <= 2; i++) {  
23         pinMode(tLightsA[i], OUTPUT);  
24         pinMode(tLightsB[i], OUTPUT);  
25     }  
26 }  
27  
28 void loop() {  
29     float valueHumidity;  
30  
31     while (true) {  
32         int distance = checkFlow();  
33         valueHumidity = dht.readHumidity();  
34  
35         // 1. Verificação de Segurança (Chuva ou Erro de Sensor)  
36         if(valueHumidity >= 90 || distance == 0) {  
37             blinkYellowAlert();  
38             break; // Reinicia o loop para nova verificação  
39         }  
40 }
```

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>.

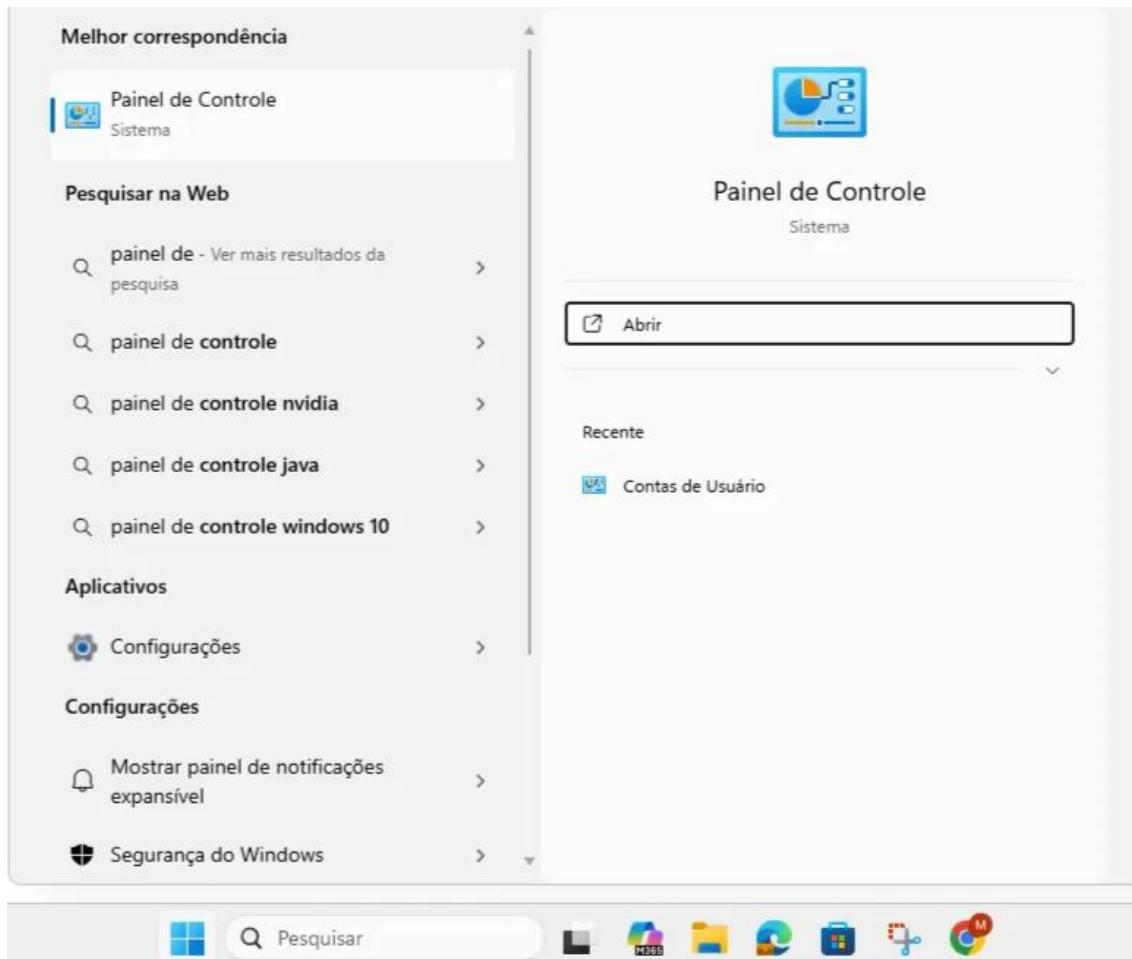
FASE 3 — SISTEMA OPERACIONAL E SEGURANÇA

Windows Server	Ubuntu Server
<p>Custo:</p> <p><i>Windows Server 2025 Datacenter (16 núcleos): cerca de R\$ 58.000 a R\$ 65.000 (licença corporativa ampla).</i></p> <p><i>Ideal para datacenters com muitas máquinas virtuais.</i></p>	<p>Custo:</p> <p><i>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.</i></p> <p><i>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.</i></p>
<p>Segurança:</p> <ul style="list-style-type: none"> • 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. 	<p>Segurança:</p> <ul style="list-style-type: none"> • 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) <p><i>Ubuntu Server é seguro, leve e confiável; a segurança depende principalmente de boa configuração e atualizações regulares.</i></p>

<p><i>Suporte a IoT:</i></p> <ul style="list-style-type: none"> • <i>Não é focado em IoT de borda</i> • <i>Usado como backend (banco de dados, AD, APIs, gerenciamento)</i> • <i>Integra bem com Azure IoT, MQTT, OPC UA</i> • <i>Windows IoT é o produto certo para dispositivos IoT, não o Windows Server</i> • <i>Windows Server gerencia e processa dados de IoT, mas não é feito para rodar diretamente nos dispositivos IoT.</i> 	<p><i>Suporte a IoT:</i></p> <ul style="list-style-type: none"> • <i>Muito usado em IoT</i> • <i>Pode rodar diretamente em dispositivos IoT (ARM, x86)</i> • <i>Ótimo para edge computing</i> • <i>Suporte nativo a MQTT, OPC UA, Docker, Kubernetes</i> • <i>Base de muitas distros IoT (ex.: Ubuntu Core)</i> <p><i>Ubuntu Server é ideal para IoT, tanto nos dispositivos quanto no backend.</i></p>
---	---

Criar usuários

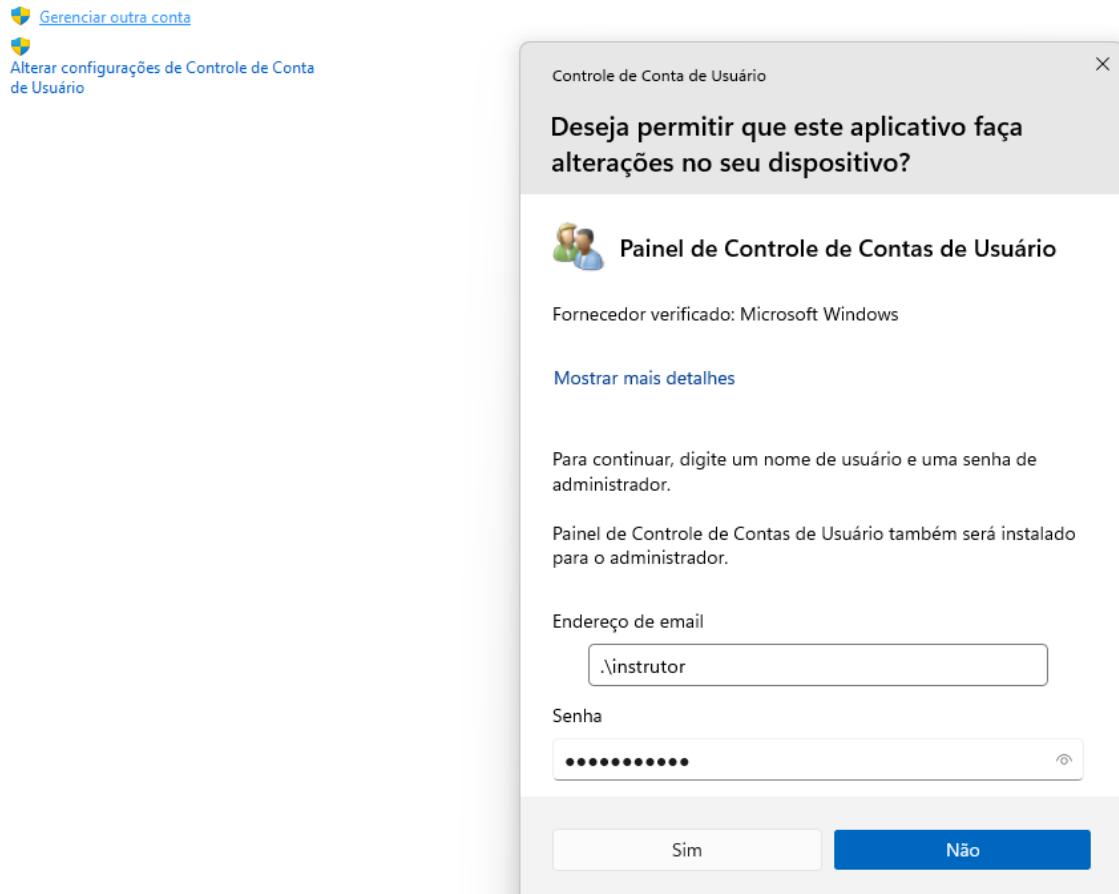
PASSO 1:



PASSO 2:



PASSO 3:



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

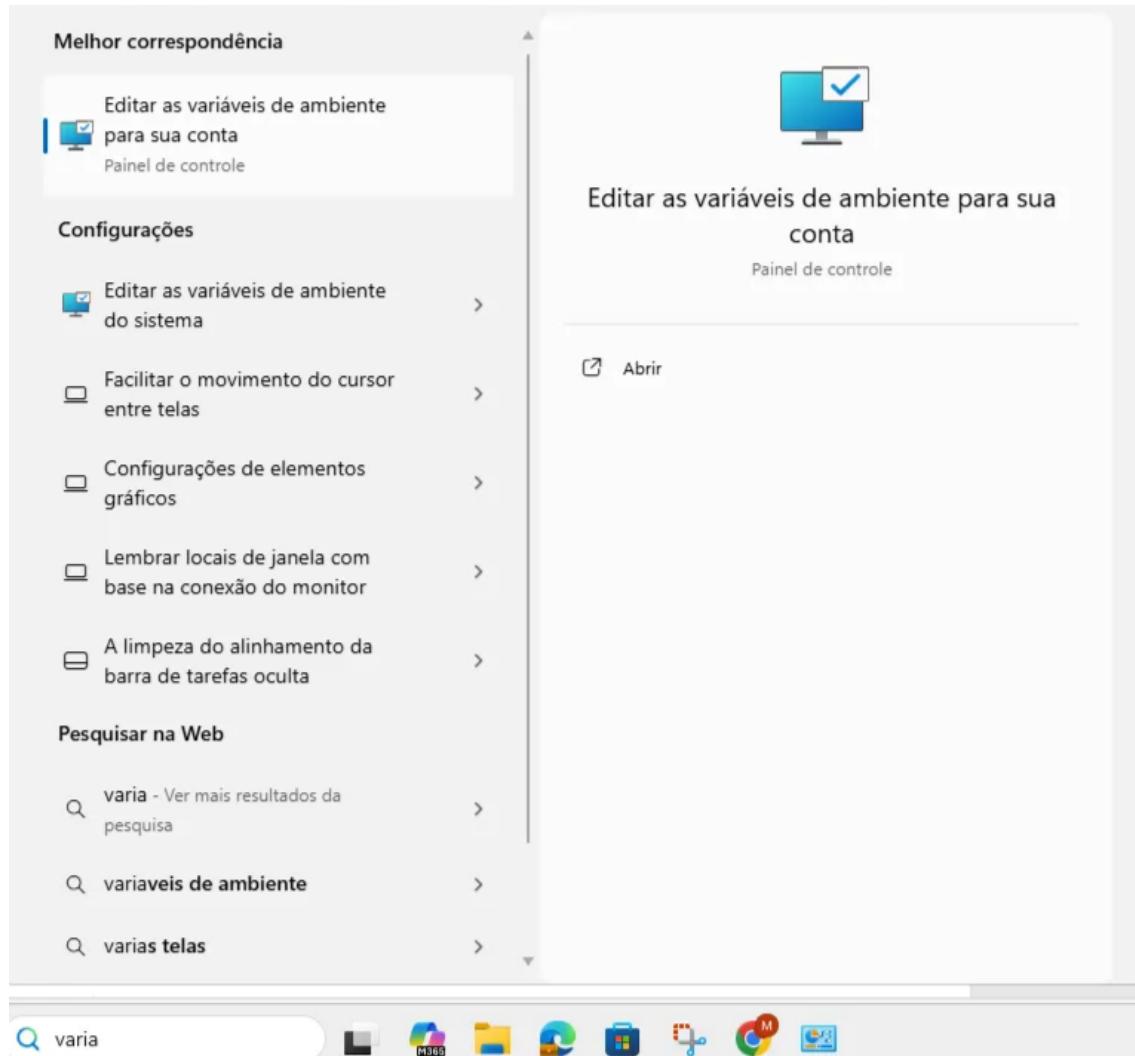
escola

Avançar

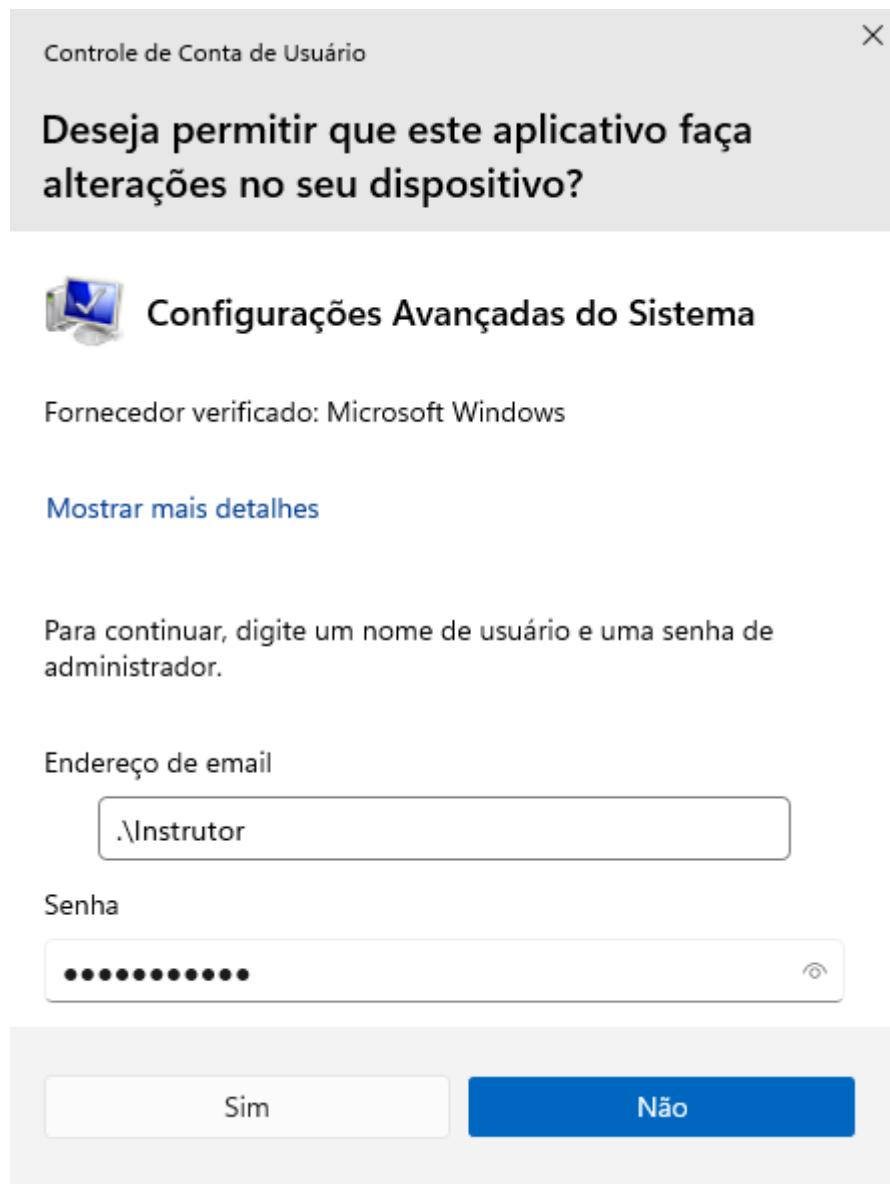
Cancelar

Ajustar variáveis de ambiente

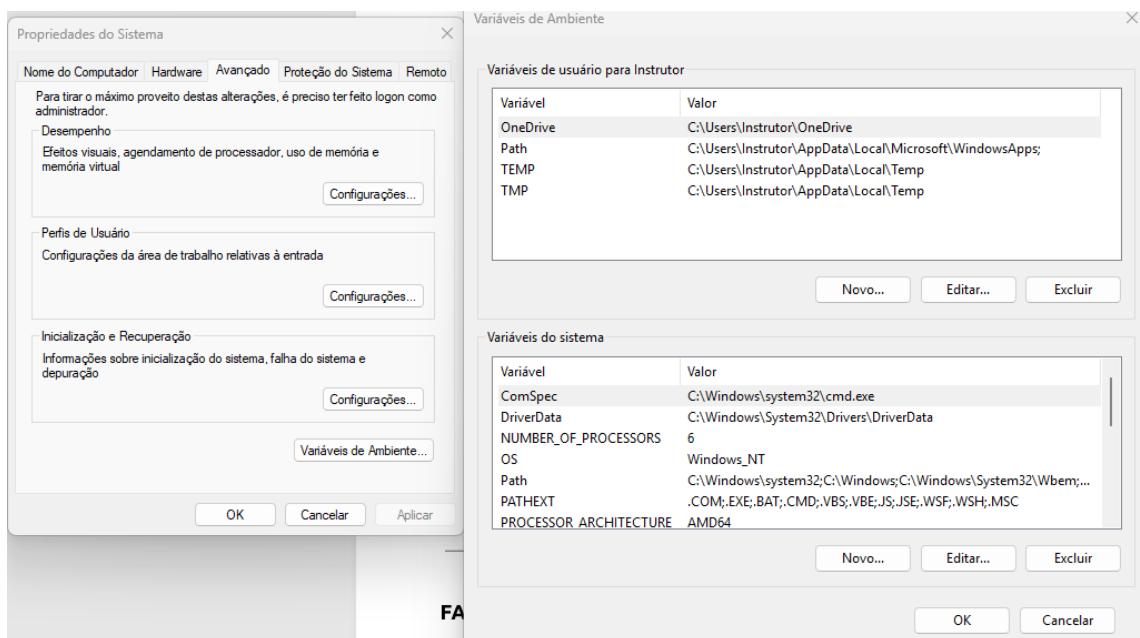
PASSO 1:



PASSO 2:

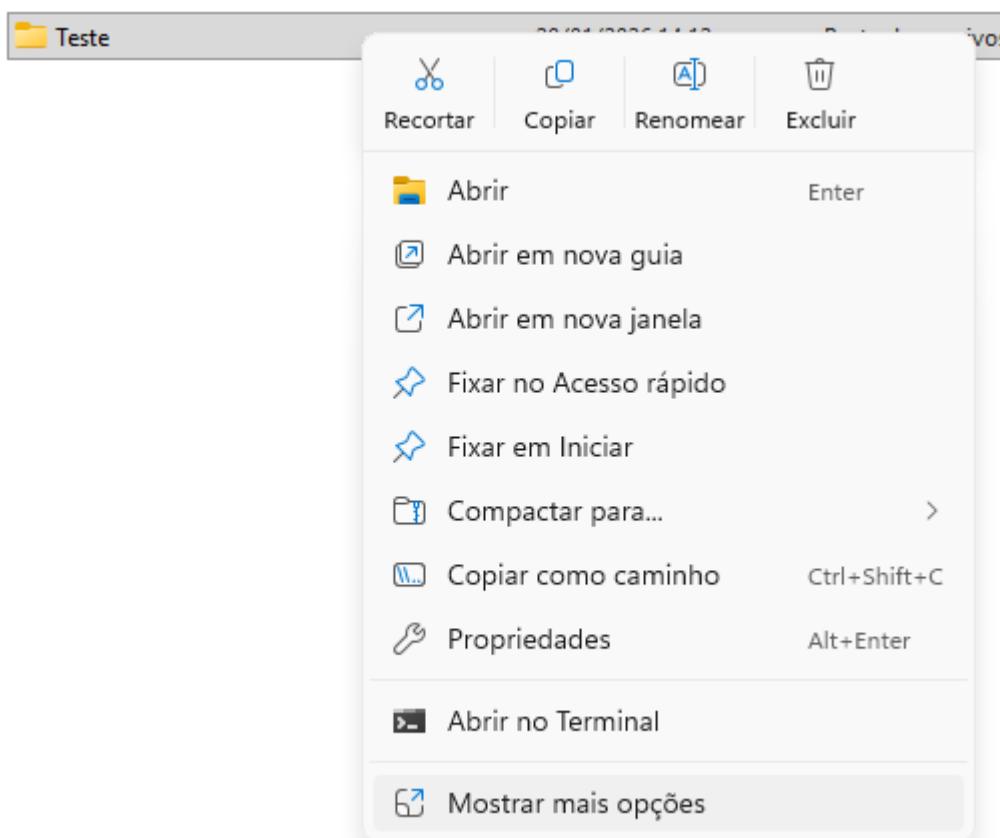


PASSO 3:

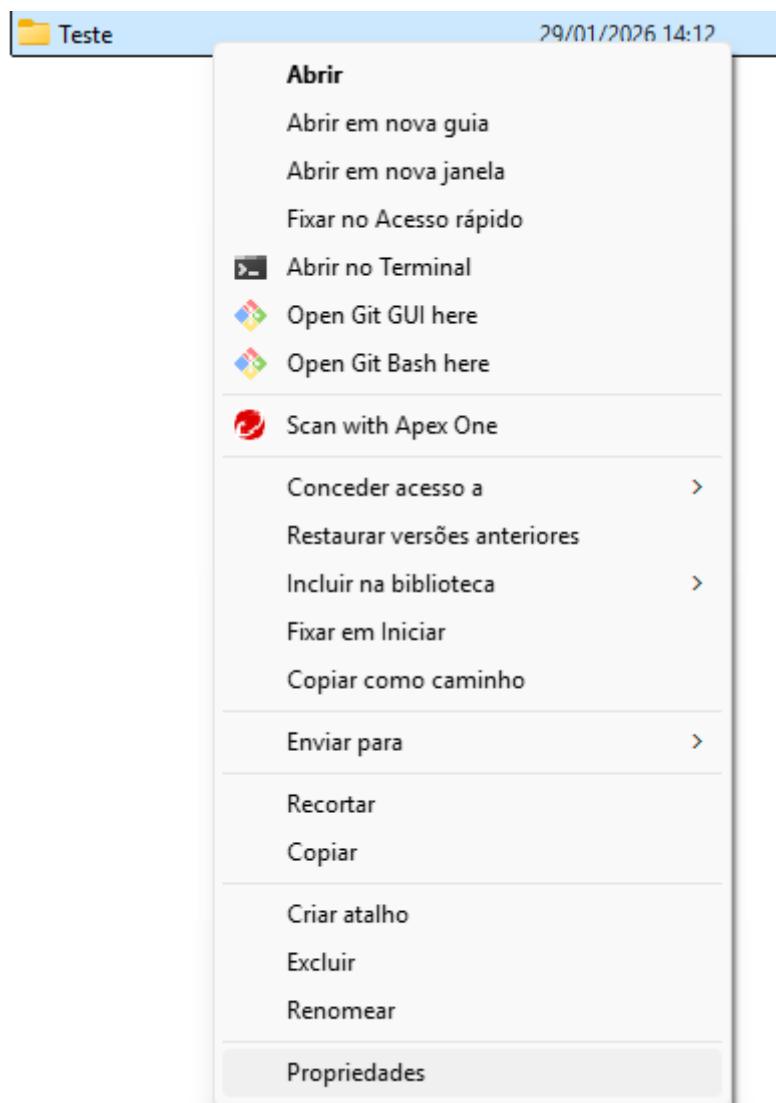


Configurar pastas compartilhadas

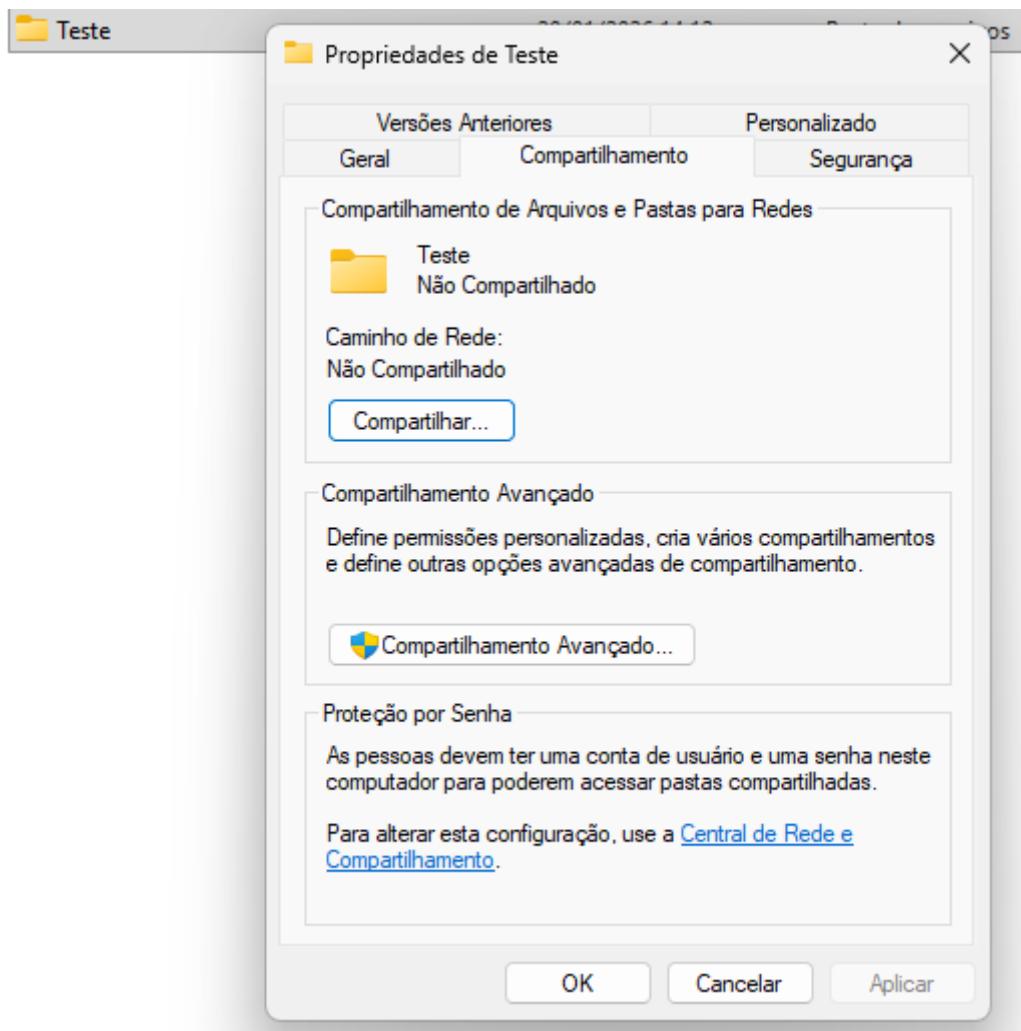
PASSO 1:



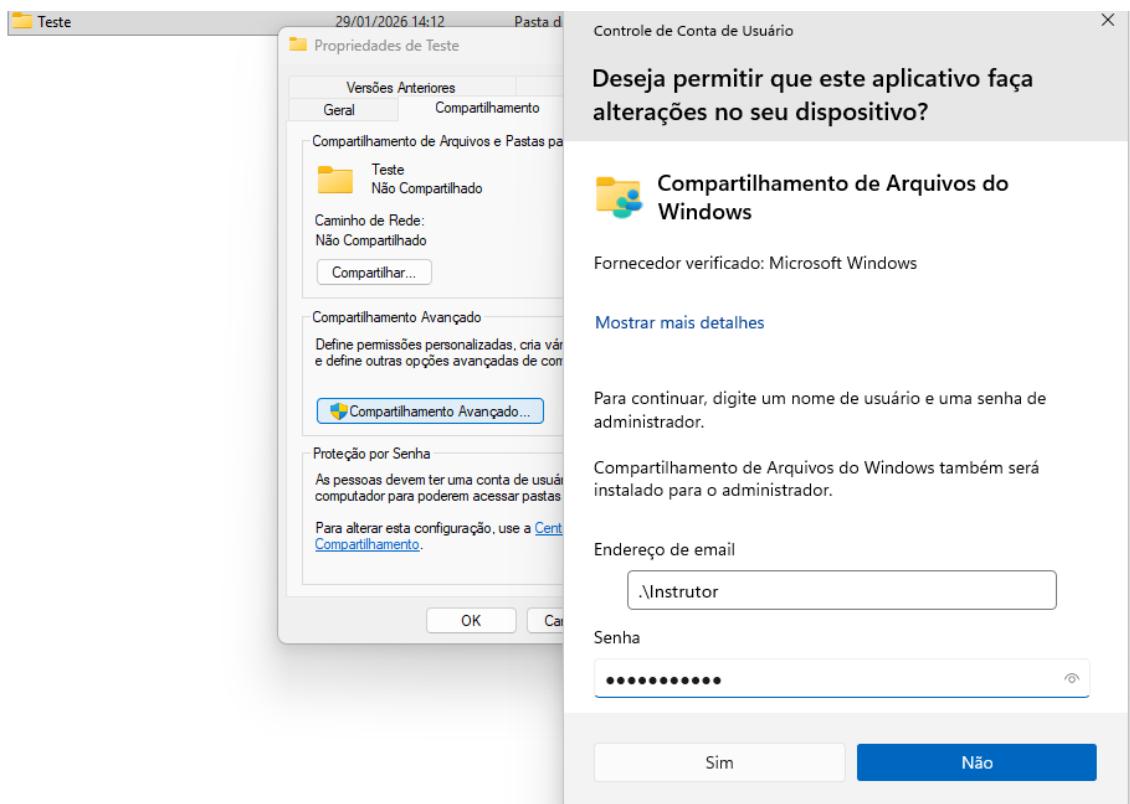
PASSO 2:



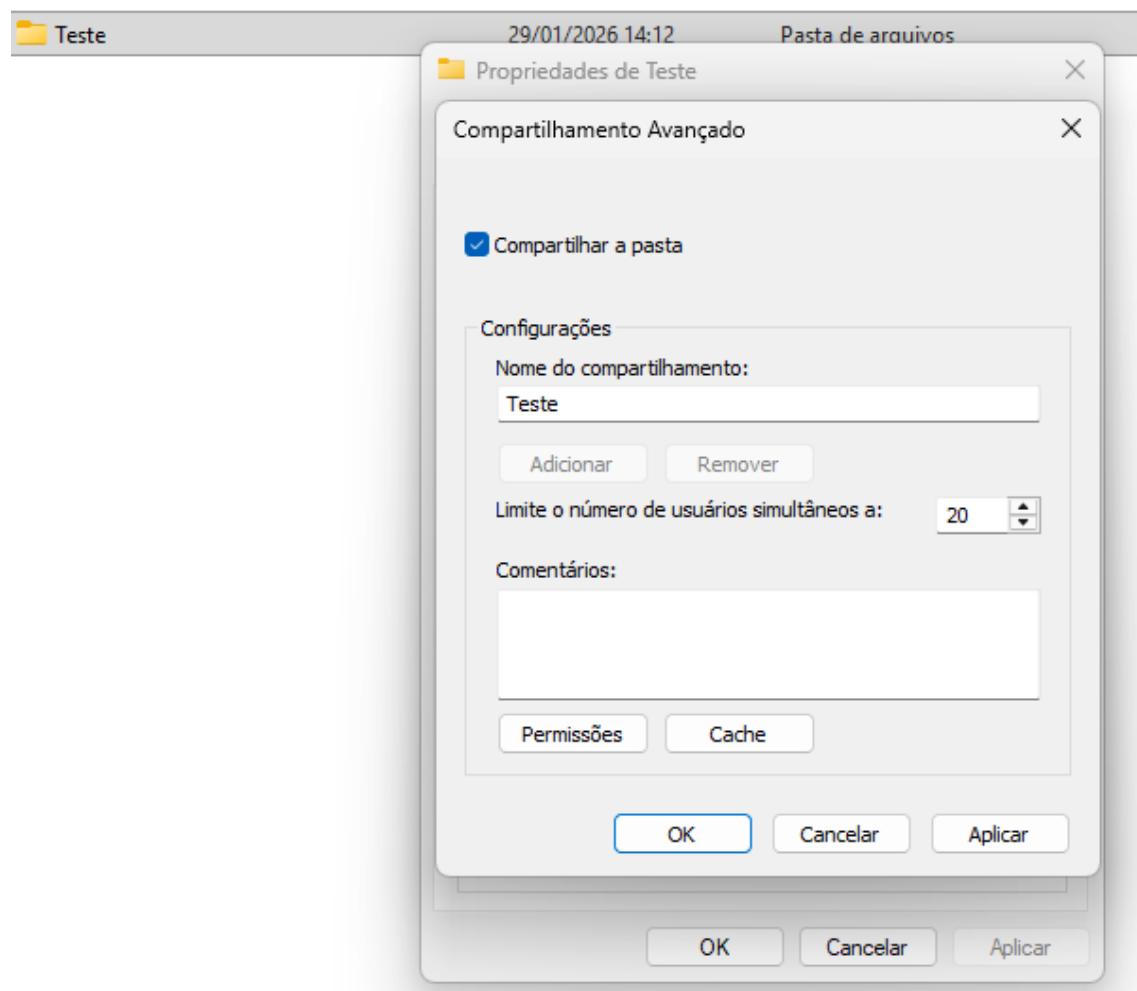
PASSO 3:



PASSO 4:



PASSO 5:



Definir permissões

PASSO 1:

Escolher o usuário que você deseja alterar

 SESISENAI\45263979894 SESISENAI\45263979894 Protegido por senha	 Aluno Conta Local
 Instrutor Conta Local Administrador Protegido por senha	 Suporte Conta Local Administrador Protegido por senha

[Adicionar uma conta de usuário](#)

PASSO 2:

Fazer alterações na conta de SESISENAI\45263979894

[Alterar o nome da conta](#)

[Alterar a senha](#)

[Alterar o tipo de conta](#)

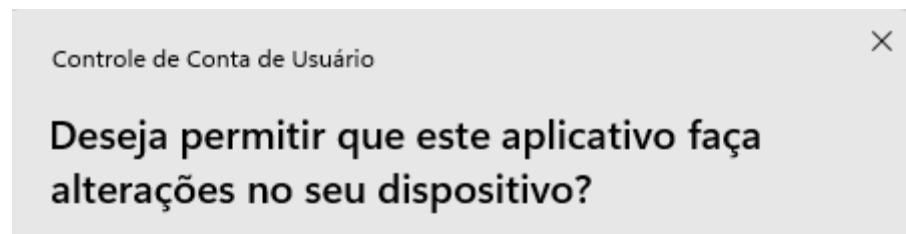
[Excluir a conta](#)

[Gerenciar outra conta](#)



SESISENAI\45263979894
SESISENAI\45263979894
Protegido por senha

PASSO 3:



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:

Selecione o novo tipo de conta



SESIENAI\45263979894

SESIENAI\45263979894

Protegido por senha

Padrão

As contas padrão podem usar a maioria dos softwares e mudar configurações do sistema que não afetem outros usuários ou a segurança do computador.

Administrador

Os administradores têm controle total sobre o computador. Eles podem mudar as configurações e acessar todos os arquivos e programas armazenados no computador.

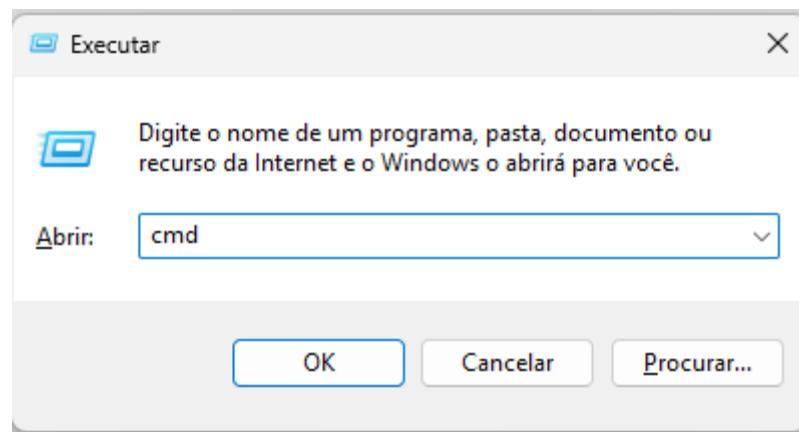
[Por que é recomendado usar uma conta padrão?](#)

[Alterar Tipo de Conta](#)

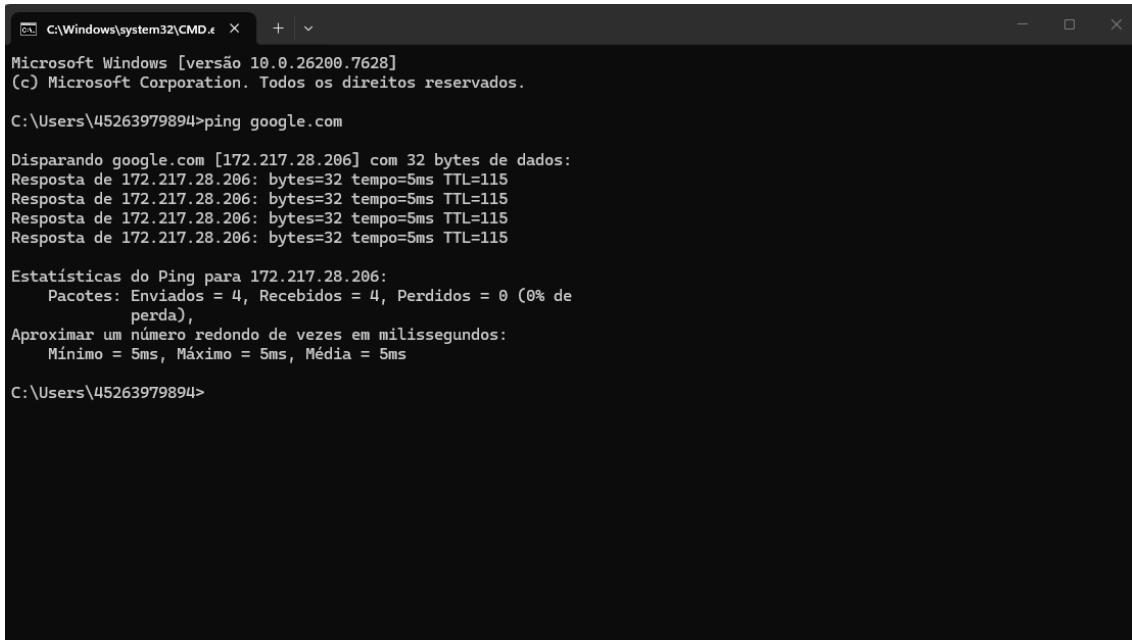
[Cancelar](#)

Testar navegação via terminal

PASSO 1:



PASSO 2:



```
C:\Windows\system32\cmd.exe + - x
Microsoft Windows [versão 10.0.26200.7628]
(c) Microsoft Corporation. Todos os direitos reservados.

C:\Users\45263979894>ping google.com

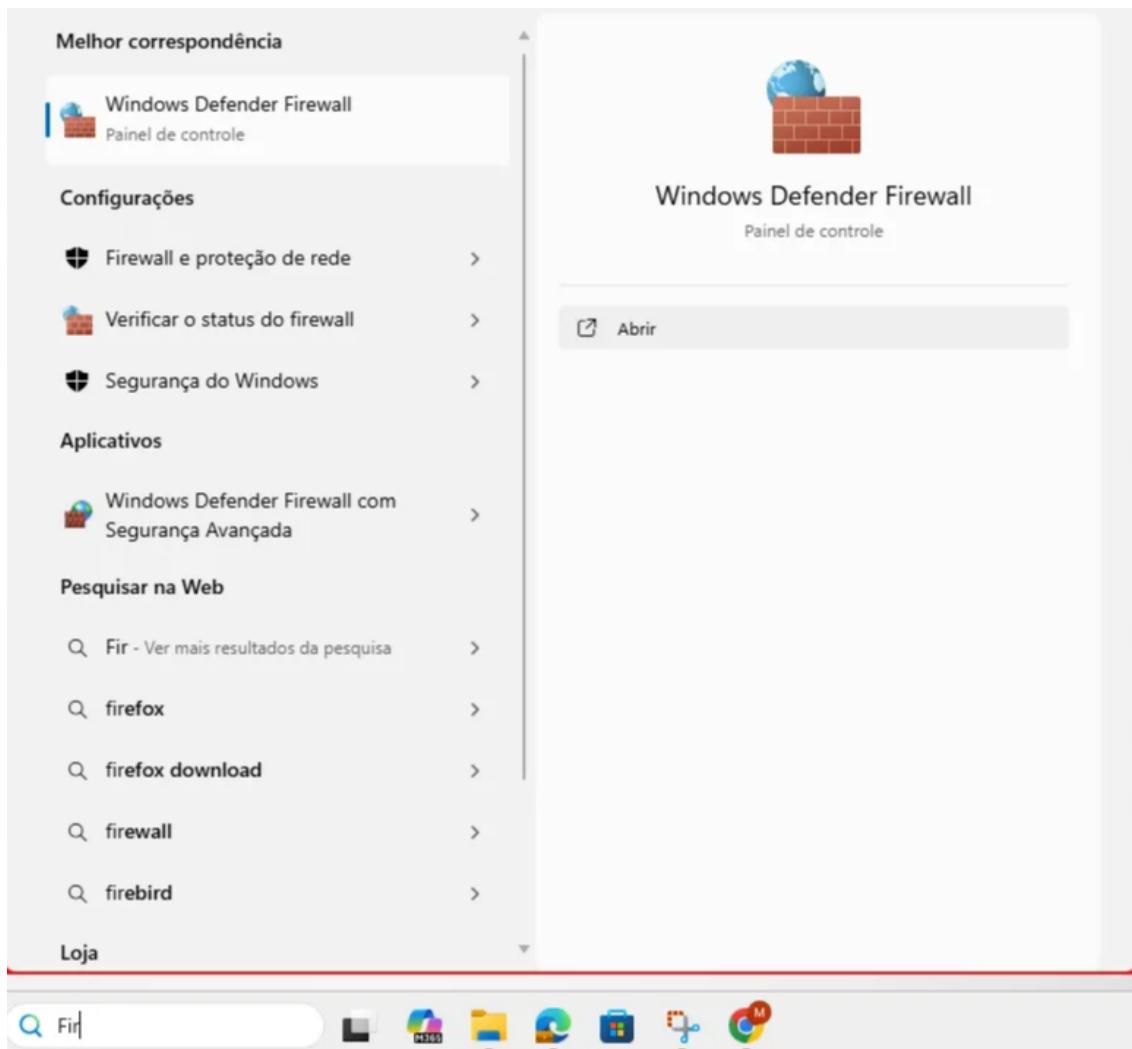
Disparando google.com [172.217.28.206] com 32 bytes de dados:
Resposta de 172.217.28.206: bytes=32 tempo=5ms TTL=115

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:

The screenshot shows the Windows Control Panel under 'Sistema e Segurança' (System and Security) and then 'Windows Defender Firewall'. On the left, there's a sidebar with links like 'Início do Painel de Controle', 'Permitir um aplicativo ou recurso através do Windows Defender Firewall', 'Alterar configurações de notificação', 'Ativar ou Desativar o Windows Defender Firewall', 'Restaurar padrões', 'Configurações avançadas', and 'Solucionar problemas com a rede'. The main area has a title 'Ajude a proteger o PC com o Windows Defender Firewall' with a note about Windows Defender Firewall helping to prevent unauthorized access. It includes a 'Usar configurações recomendadas' button. Below this, it shows network profiles: 'Redes privadas' (Not connected) and 'Redes públicas ou convidadas' (Connected). It also displays the state of the firewall (Desligado), connection rules (Block all incoming connections from untrusted apps), active public networks (sp.local), and notification settings (Notify me when the Windows Defender Firewall blocks a new app). A red box highlights the 'Redes privadas' section.

PASSO 3:

Permitir que aplicativos se comuniquem através do Windows Defender Firewall

Para adicionar, alterar ou remover portas e aplicativos permitidos, clique em Alterar configurações.

This screenshot shows the 'Aplicativos e recursos permitidos' (Allowed apps and resources) section. It lists various applications and services with checkboxes for 'Privada' (Private) and 'Público' (Public) network access. Some entries have checkboxes checked in both columns, while others are only checked in one. At the bottom, there are buttons for 'Detalhes...' (Details...), 'Remover' (Remove), and 'Permitir outro aplicativo...' (Allow another app...).

Nome	Privada	Público
@{Microsoft.DesktopAppInstaller_1.27.349.0_x64_8wekyb3d8bbwe?ms-res...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
{78E1CD88-49E3-476E-B926-580E596AD309}	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ação com um clique	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
AMD Radeon Software	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Aplicativo Start Experiences	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Área de Trabalho Remota	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Área de Trabalho Remota (WebSocket)	<input type="checkbox"/>	<input type="checkbox"/>
Assistência de Jogos do Microsoft Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Assistência Remota	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Base da Colaboração Ponto a Ponto do Windows	<input type="checkbox"/>	<input type="checkbox"/>
BranchCache - Cliente de Cache Hospedado (Usa HTTPS)	<input type="checkbox"/>	<input type="checkbox"/>
BranchCache - Descoberta no Par (Usa WSD)	<input type="checkbox"/>	<input type="checkbox"/>

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

