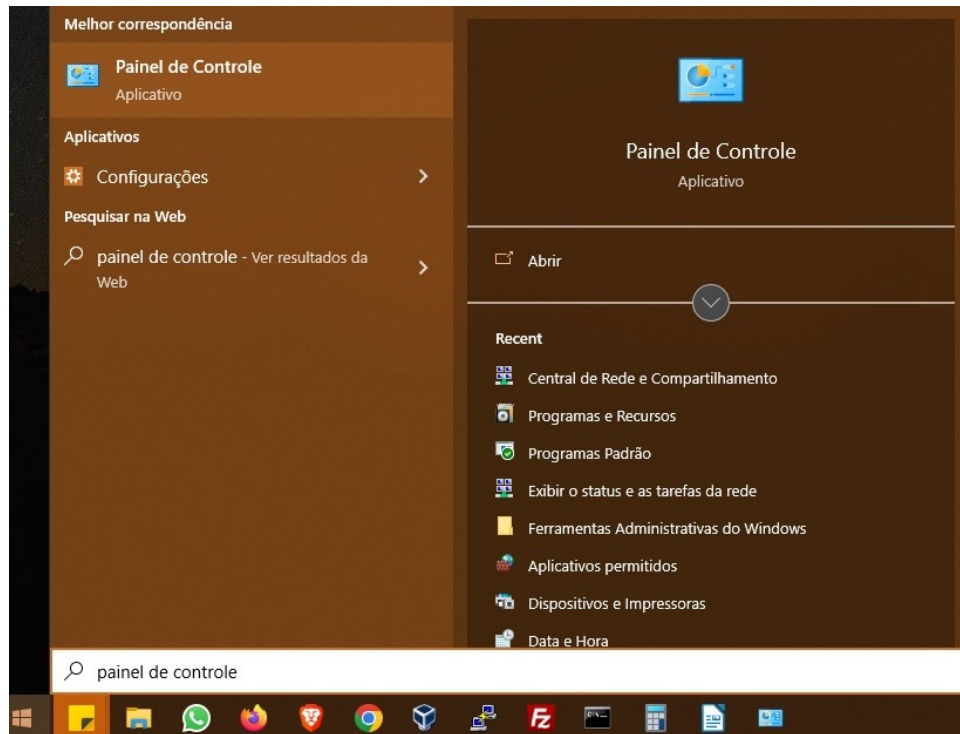
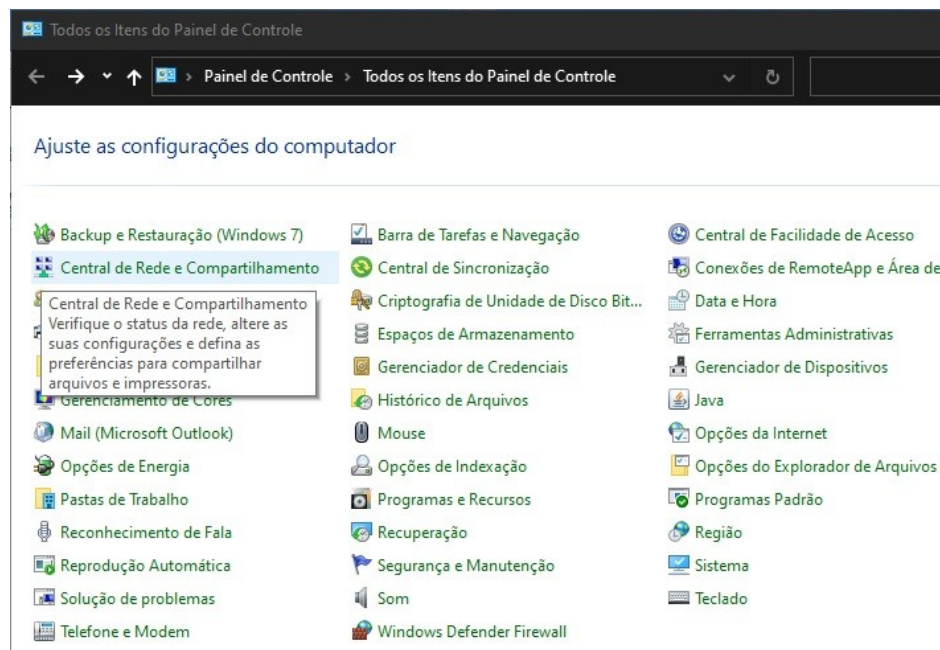


## Configurar o Equipamento (Windows 7, 8 e 10)

1. Clicar no botão iniciar do Windows para pesquisar e entrar no “Painel de Controle”:

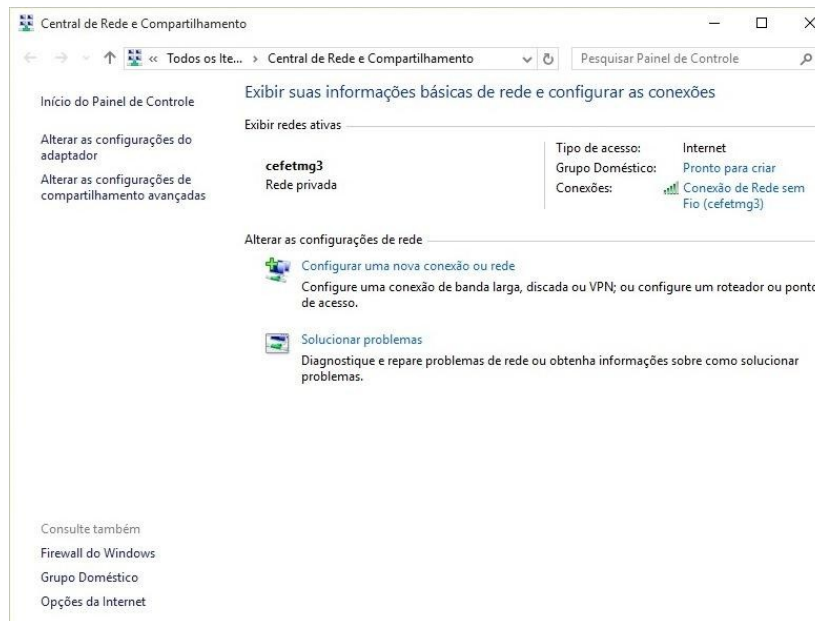


2. Clicar em “Central de Rede e Compartilhamento”:

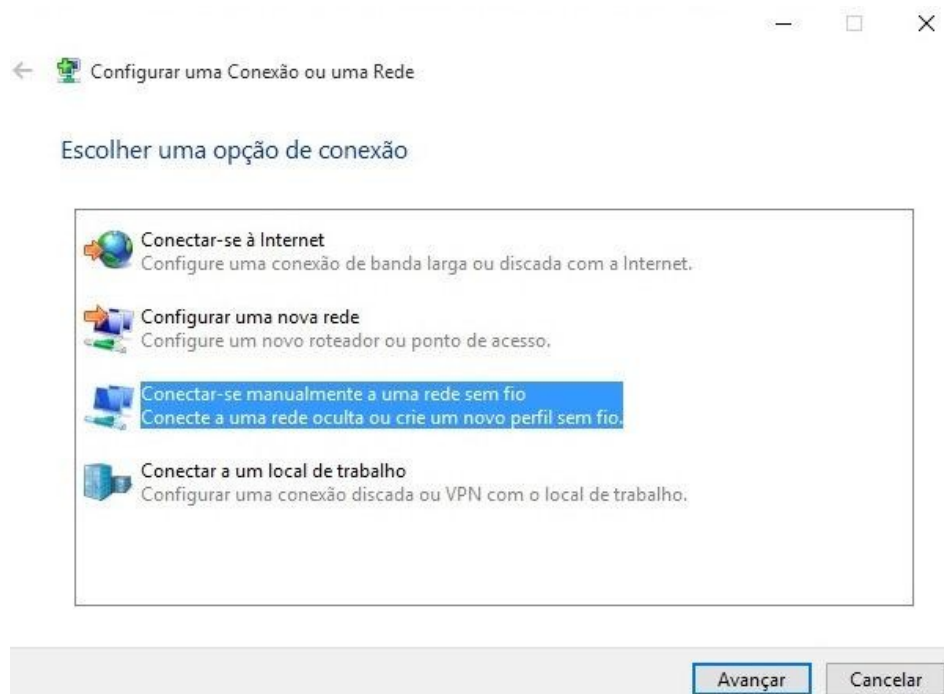




3. Clicar em “Configurar uma nova conexão ou rede”:



4. Clicar em “Conectar-se manualmente a uma rede sem fio”, clicar em “Avançar”:





5. Preencher o “Nome da rede”

- **Para aluno:** cefetmg\_aluno
- **Para funcionário:** cefetmg

Preencher as outras opções conforme a figura abaixo e clicar em “Avançar”:

6. Clicar em “Alterar configurações de conexão”:



7. Configurar as opções conforme figura abaixo e clicar na aba “Segurança”:

cefetmg\_aluno Propriedades de Rede Sem Fio

Conexão Segurança

Nome: cefetmg\_aluno  
SSID: cefetmg\_aluno  
Tipo de rede: Ponto de acesso  
Disponibilidade de rede: Todos os usuários

☒ Conectar automaticamente quando esta rede estiver ao alcance  
☐ Procurar outras redes sem fio enquanto estiver conectado a esta rede  
☐ Conectar mesmo que a rede não esteja difundindo seu nome (SSID)

OK Cancelar

8. Configurar as opções conforme figura abaixo e clicar em “Configurações”:

cefetmg\_aluno Propriedades de Rede Sem Fio

Conexão Segurança

Tipo de segurança: WPA2-Enterprise  
Tipo de criptografia: AES

Escolha um método de autenticação de rede:  
Microsoft: EAP protegido (PEAP) Configurações

☒ Lembrar minhas credenciais para esta conexão sempre que fizer login

Configurações avançadas

OK Cancelar



9. Configurar as opções conforme figura abaixo e clicar em “Configurar...”:

Propriedades EAP Protegidas

Ao conectar:

☐ Verificar a identidade do servidor validando o certificado

☐ Conectar a estes servidores (exemplos: srv1;srv2;.\*\srv3\com):

Autoridades de certificação raiz confiáveis:

- ☐ AddTrust External CA Root
- ☐ Autoridade Certificadora Raiz Brasileira v2
- ☐ Baltimore CyberTrust Root
- ☐ Class 3 Public Primary Certification Authority
- ☐ DigiCert Assured ID Root CA
- ☐ DigiCert Global Root CA
- ☐ DigiCert High Assurance EV Root CA

Notificações antes da conexão:

Informar o usuário se a identidade do servidor não puder ser ver

Selecionar Método de Autenticação:

Senha segura (EAP-MSCHAP v2) Configurar...

☐ Ativar Reconexão Rápida

☐ Desconectar se o servidor não tiver TLV com cryptobinding

☐ Habilitar Privacidade de Identidade

OK Cancelar

10. Configurar as opções conforme figura abaixo e clicar em “Ok”:

Propriedades de EAP MSCHAPv2

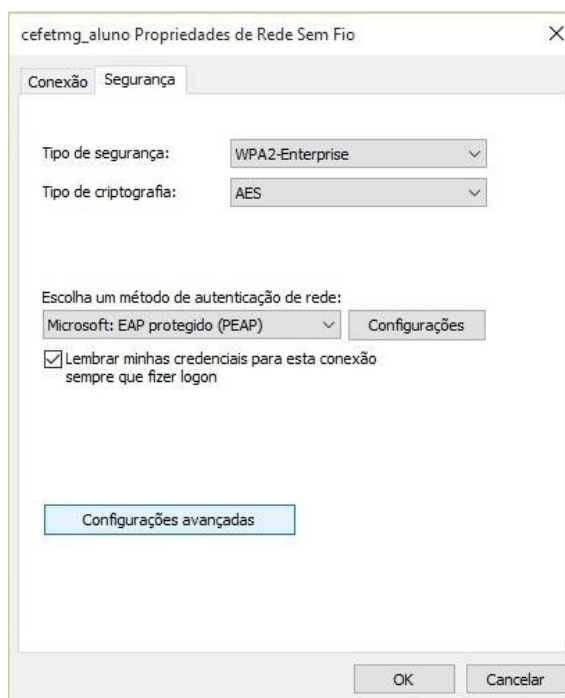
Ao se conectar:

☐ Usar automaticamente meu nome e senha de logon do Windows (e o domínio, se houver).

OK Cancelar



11. Clicar em “Ok” de novo e depois em “Configurações avançadas”:



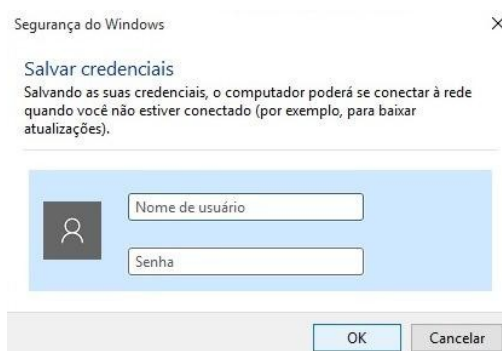
12. Configurar as opções conforme figura abaixo e clicar em “Salvar credenciais”:





13. Salvar o “Nome de usuário” e “Senha”

- **Usuário:** “CPF”
- **Senha:** senha cadastrada na Identificação Única (<https://iu.cefetmg.br>)



14. Clicar em todos os “Ok” até fechar tudo

**ATENÇÃO:** Se não funcionar tente excluir a rede “cefetmg” ou “cefetmg\_aluno” e refazer todos os passos de novo.