



MANUAL PARA
CONFIGURAÇÃO DE SEGUNDO FATOR
DE AUTENTICAÇÃO NA CONTA
MICROSOFT 365



Histórico de Revisões

Data	Versão	Elaboração	Aprovação	Descrição
07/2025	1.0	CGSII		Elaboração do documento



SUMÁRIO

1. PÚBLICO-ALVO	4
2. OBJETIVO	4
3. CONFIGURAR O SEGUNDO FATOR DE AUTENTICAÇÃO	4
3.1. LOGIN	4
3.2. CONFIGURAR APLICATIVO NO DISPOSITIVO MÓVEL	5
3.3. TESTE A CONFIGURAÇÃO	8
4. RECONFIGURAR O SEGUNDO FATOR DE AUTENTICAÇÃO	8



1. PÚBLICO-ALVO

Usuários internos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), que utilizam conta no *Microsoft* 365.

- **Pré-Requisitos**

- **Dispositivo Móvel/Celular** - para uso do TFA é necessário um dispositivo móvel para instalação de um aplicativo;
- **Navegador** - para validação da configuração.

2. OBJETIVO

Configurar o segundo fator de autenticação, conhecido por 2FA ou TFA (*Two-Factor Authentication*) que é uma medida de segurança extra que ajuda a proteger sua conta, exigindo mais do que apenas a senha, tornando-a mais segura contra ataques e consequentemente, protegendo a Rede CAPES contra invasões.

3. CONFIGURAR O SEGUNDO FATOR DE AUTENTICAÇÃO

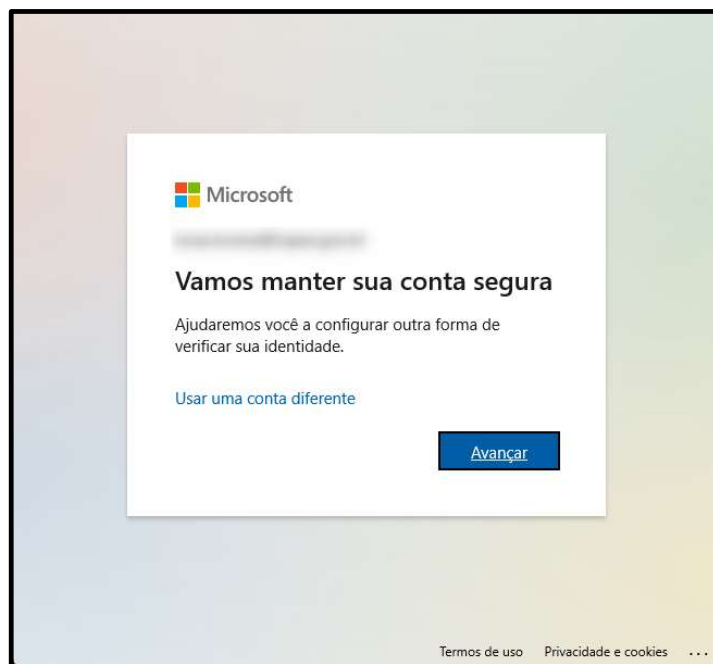
Ao ser exigida a configuração do TFA para sua conta, tanto o *Microsoft Teams* quanto o *Microsoft Outlook* solicitarão que a conta ative a medida de segurança. Mensagem como a abaixo, poderá ser exibida:

✖ Precisamos que você entre novamente. Isto pode ser uma solicitação do seu departamento de TI ou do Teams, ou o resultado de uma atualização de senha.

3.1. LOGIN

Caso não apareça de forma automática a tela de *login*, você pode acessar o endereço <https://mysignins.microsoft.com/security-info>.

- Entre com sua conta (*e-mail* da CAPES)
- Avance com a configuração para manter a conta segura

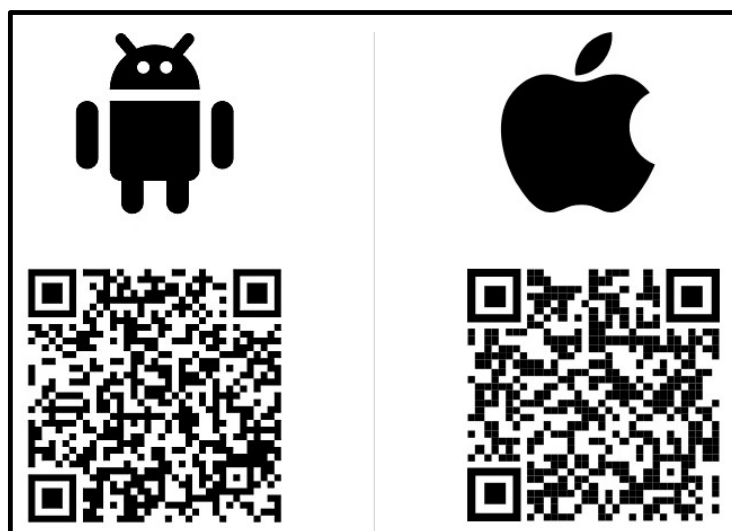


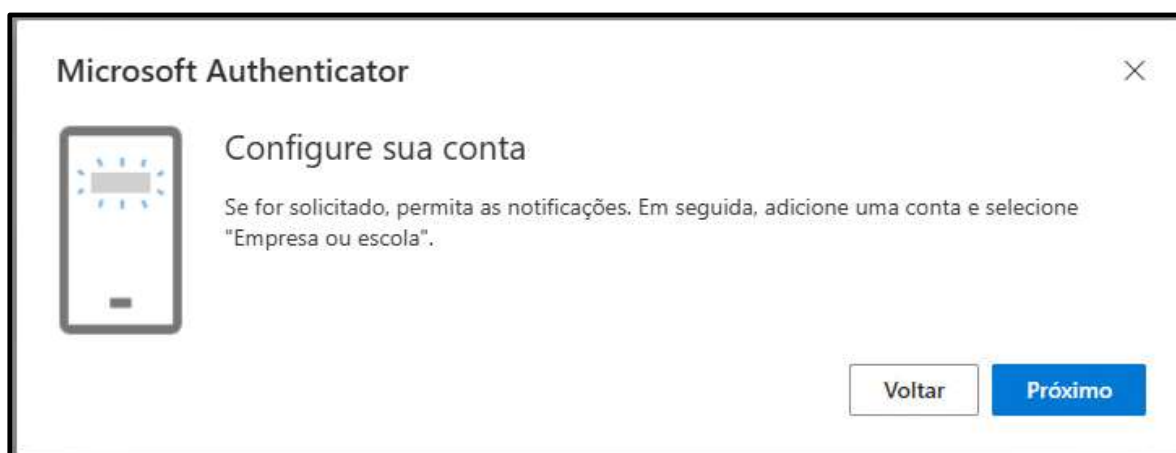
3.2. CONFIGURAR APLICATIVO NO DISPOSITIVO MÓVEL

Nesta etapa, caso não tenha instalado, instale o aplicativo *Microsoft Authenticator* para prosseguir com a configuração do TFA no seu dispositivo móvel.

Links para os aplicativos:

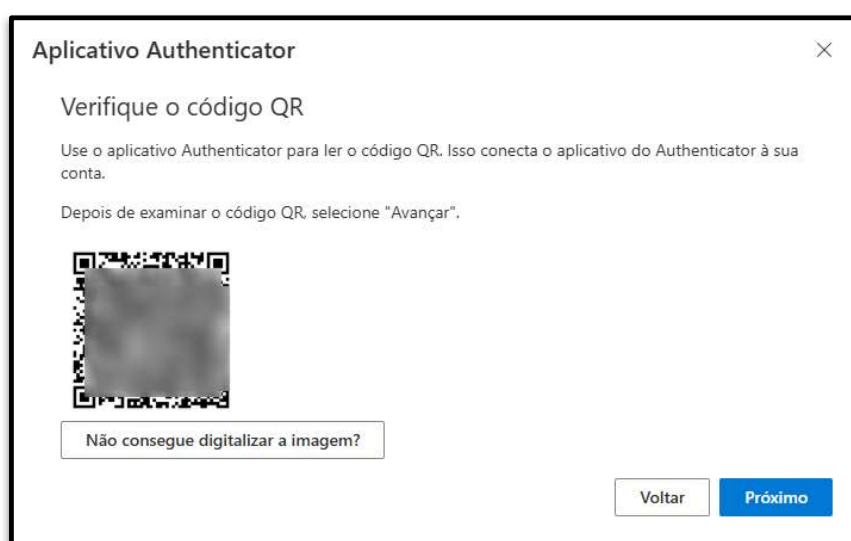
- [Android:](#)
- [IOS](#)





Depois de instalar o aplicativo e avançar, irá aparecer um código QR. Utilize o aplicativo "*Microsoft Authenticator*" para ler o código.

⚠ Não compartilhe esse código QR com ninguém.



Digite os números da página no "*Microsoft Authenticator*" e finalize a configuração.

Mantenha sua conta segura

Microsoft Authenticator



Vamos experimentar

Aprove a notificação que estamos enviando para o seu aplicativo inserindo o número mostrado abaixo.

[Voltar](#)[Próximo](#)[Desejo configurar um método diferente](#)

Mantenha sua conta segura

Microsoft Authenticator



✔ Notificação aprovada

[Próximo](#)[Desejo configurar um método diferente](#)

Mantenha sua conta segura

Êxito!

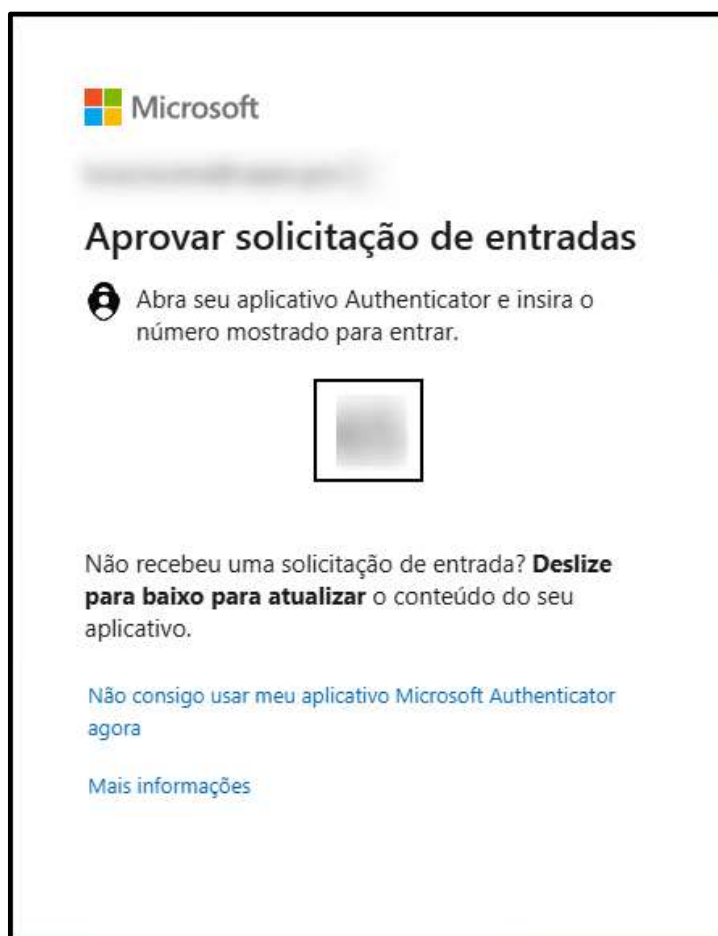
Ótimo! Você configurou com êxito as informações de segurança. Selecione "Concluído" para continuar a entrada.

Método de entrada padrão:

Microsoft Authenticator

[Concluído](#)

A partir de agora, sempre que você fizer *login* com sua conta *Microsoft* da CAPES no *e-mail*, *Teams* ou algum outro produto do *Microsoft 365*, será solicitada uma aprovação pelo seu aplicativo *Microsoft Authenticator*, como a abaixo.



3.3. TESTE A CONFIGURAÇÃO

- Faça *logout* de sua conta da *Microsoft*.
- Faça *login* novamente. Durante o processo de *login*, você será solicitado a inserir seu código de verificação.
- Pronto! Agora, sua conta da CAPES estará mais segura.

4. RECONFIGURAR O SEGUNDO FATOR DE AUTENTICAÇÃO

Para os casos de troca ou perda do dispositivo móvel é necessário entrar em contato com a equipe do suporte DTI para o *reset* do segundo fator de autenticação.



Caso tenha perdido o dispositivo, informe imediatamente a equipe da DTI.