TUTORIAL

# Configurando o Múltiplo Fator de Autenticação (MFA)


**ÍNDICE**

# Introdução

O uso de senhas é bastante comum para a autenticação em sites na Internet ou em contas de rede corporativas. No entanto, muitas vezes sua utilização pode ser insuficiente para garantir a segurança da identidade do usuário. Uma alternativa para **ampliar** a segurança dessas operações é a utilização do **Múltiplo Fator de Autenticação** (MFA), também conhecido como Verificação em Duas Etapas, "*two-factor authentication*", aprovação de login, verificação ou autenticação em dois fatores ou, ainda, verificação ou autenticação em dois passos.

Esse processo adiciona uma segunda camada de proteção no acesso a uma conta. Trata-se de um recurso que exige que o usuário, além da utilização da senha correta, valide seu acesso por meio de um segundo código verificador temporário, normalmente enviado por SMS ou produzido por um dispositivo eletrônico paralelo (como um *smartphone* ou *token*). Dessa forma, para garantir a identidade do usuário, o MFA exige algo que o usuário **sabe** (a senha) e algo que ele **tem** (o dispositivo que gera o código).

Com a disponibilização de diversos serviços hospedados em nuvem, a JF3R está tomando a iniciativa de habilitar o **Múltiplo Fator de Autenticação** para as contas de rede de seus usuários, ampliando assim o nível de segurança dessas contas e contribuindo para evitar ataques, invasões e perda de dados.

Neste tutorial, você poderá acompanhar todos os passos necessários para ativar o MFA na sua conta de rede da JF3R.

# Pré-requisitos

Para utilização desse manual **é necessário** que você tenha as seguintes informações:

1. Credenciais (usuário e senha) de acesso válidas na rede da JF3R.
2. **Fator de autenticação por SMS:** Número de telefone celular com DDD, para configurar a opção de recuperação ou fator de autenticação;
3. **Fator de autenticação por aplicativo**[1]**:** *Smartphone* com aplicativo **Microsoft Authenticator** já instalado. Esse aplicativo está disponível para sistemas Android e iOS e pode ser obtido através do link:

   https://www.microsoft.com/pt-br/account/authenticator

4. Utilizar preferencialmente o **Microsoft Edge.**

**Observação importante:**

O usuário deve configurar o seu MFA seguindo apenas **um procedimento** (SMS ou aplicativo), não é necessário realizar os dois métodos.

[1] O fator de autenticação por aplicativo é uma alternativa ao método de verificação por SMS e seu uso está detalhado no final do manual.

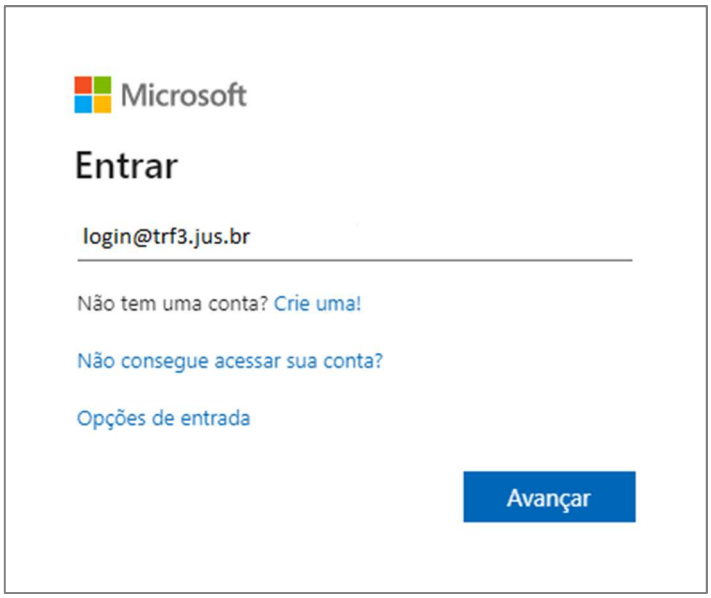
# Procedimento de Autenticação via SMS

A partir de seu computador, acesse a página de configurações do MFA :

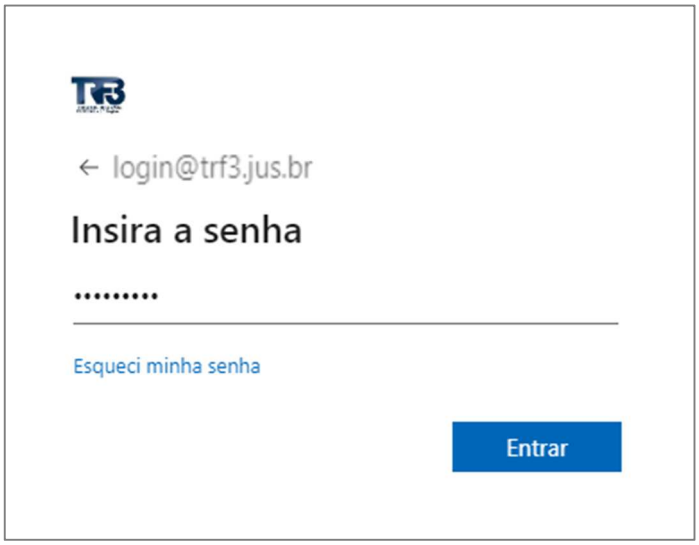
https://aka.ms/MFASetup

Se apresentar tela de erro, tecle F5 (atualizar) e aguarde.

1. Caso ainda não esteja autenticado no ambiente de nuvem da Microsoft, preencha o formulário apresentado com o seu endereço de e-mail da JF3R (Por ex.: login@trf3.jus.br).

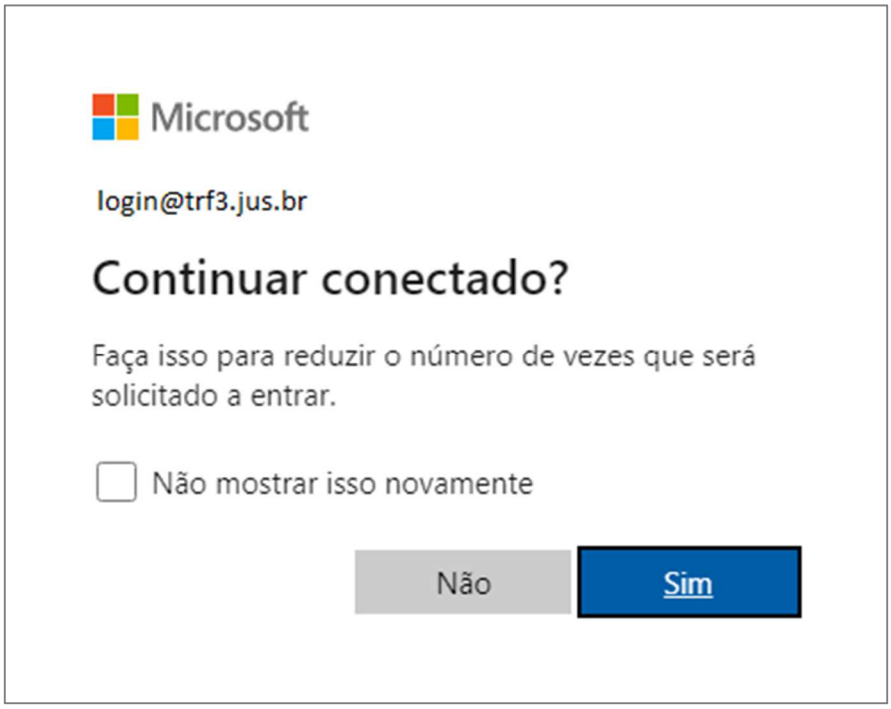



2. Pressione o botão Avançar e, na tela seguinte, insira sua senha da rede JF3R.

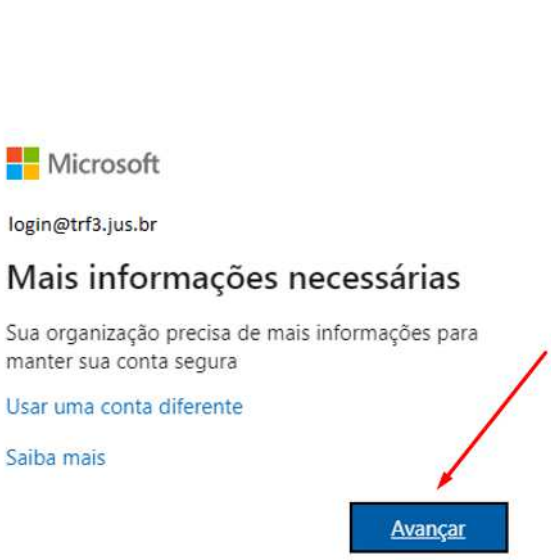


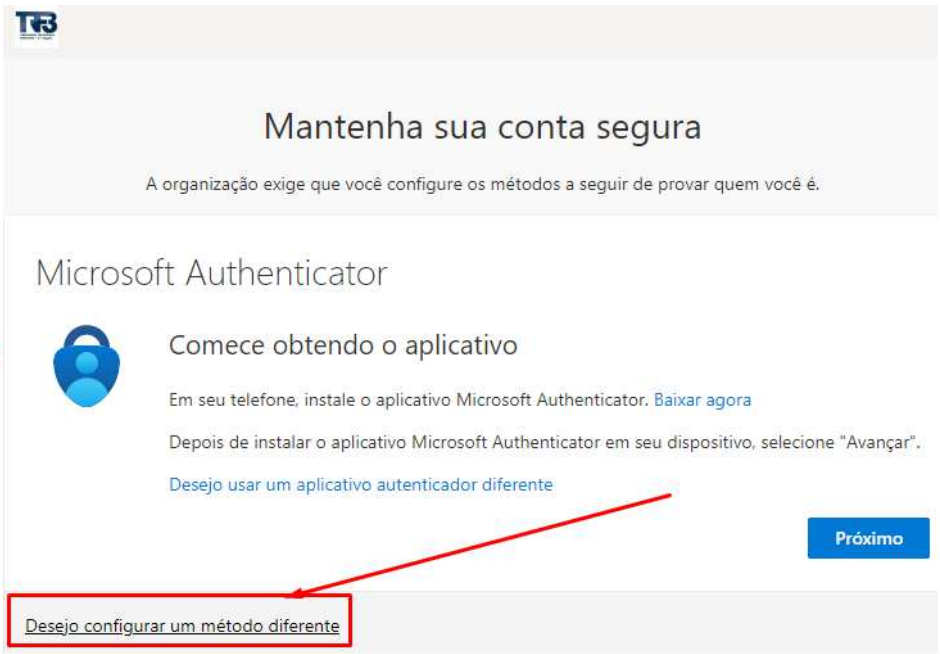

3. Pressione o botão Entrar.

4. Na tela seguinte, escolha a melhor opção, de acordo com a sua conveniência. Se você escolher Sim, a sua conexão permanecerá ativa e autenticada no computador onde você estiver realizando a operação.

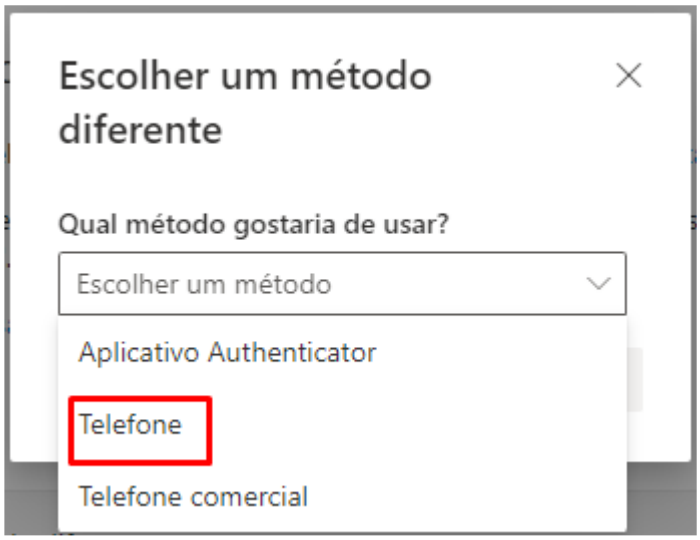



5. Irá aparecer uma das telas a seguir:

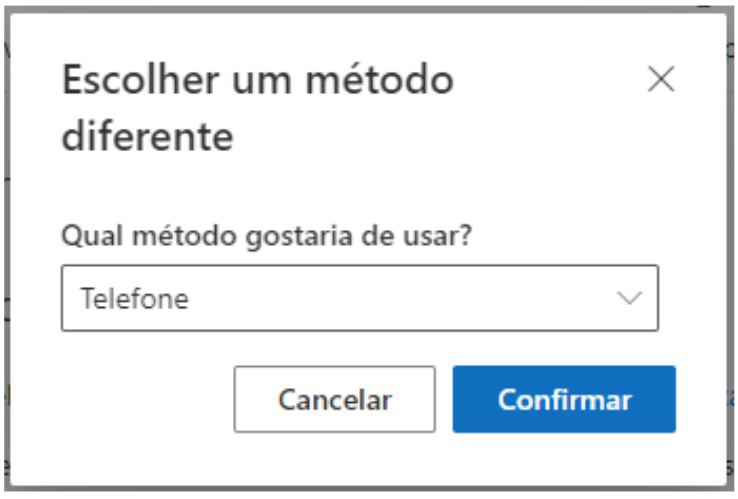


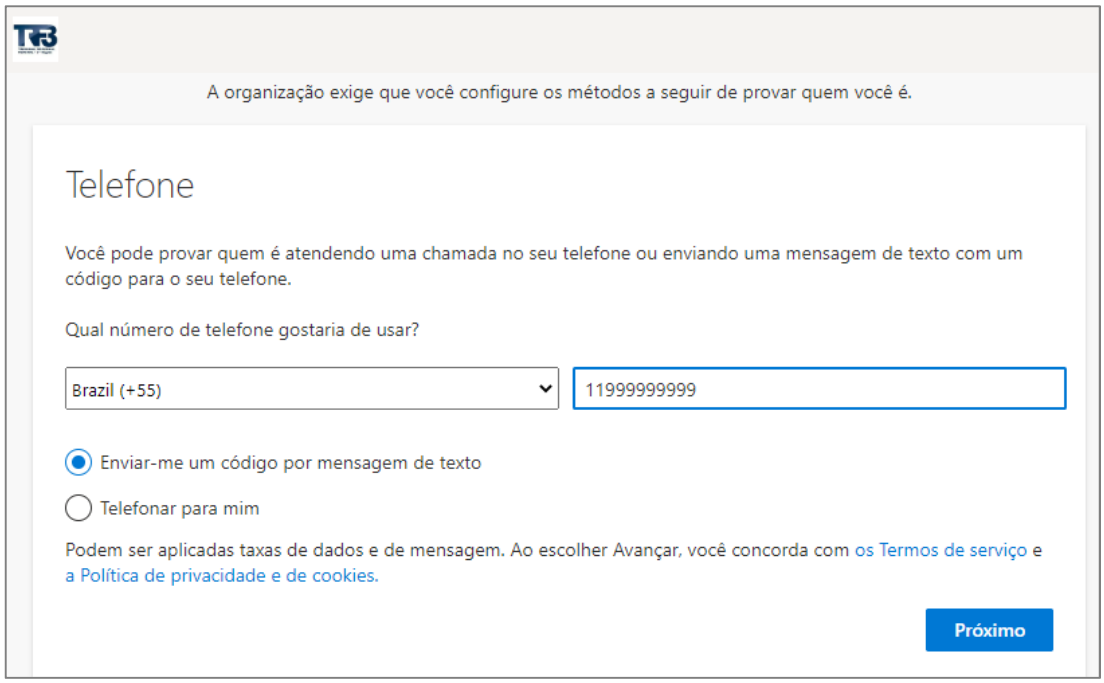



6. A tela seguinte contém todas as opções de configuração para o **Múltiplo Fator de Autenticação** disponíveis. Caso você nunca tenha feito nenhuma configuração ou tenha aberto um chamado para limpar as configurações existentes, a sua tela estará como a apresentada a seguir.

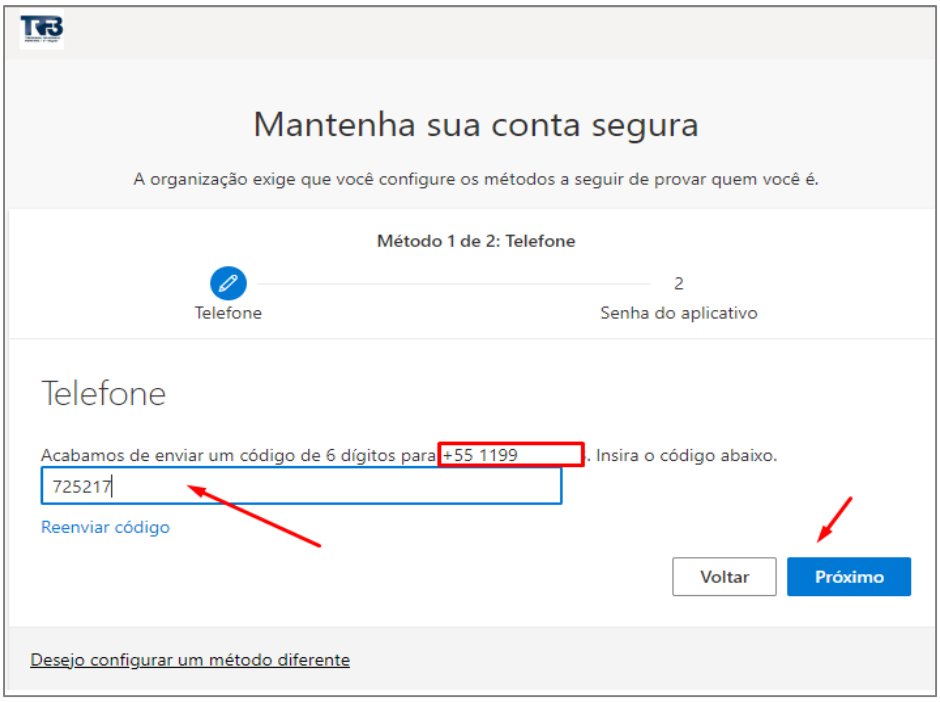



7. A seguir, você deverá escolher "**Telefone**" como método de Múltiplo Fator de Autenticação. Desta forma, sempre que você tentar acessar o ambiente de nuvem da Microsoft, será disparada uma notificação no seu celular com um código de verificação, via SMS.



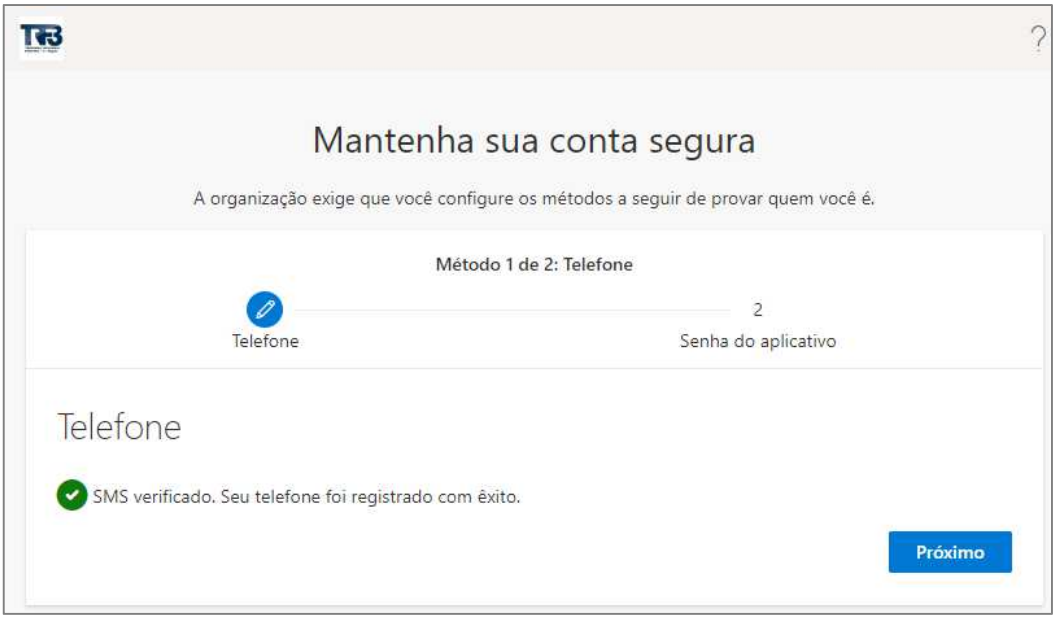


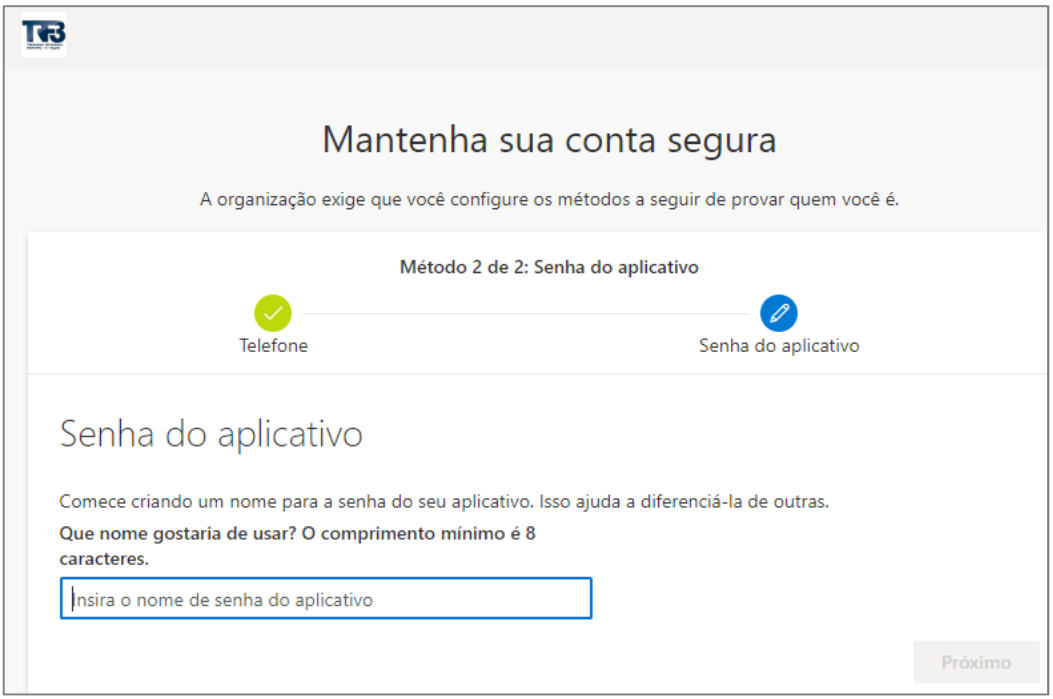

8. Selecione **Brasil (+55)**.
9. Preencha o campo seguinte com o número do seu celular, **incluindo DDD**.
10. Marque "Envie-me um código por mensagem de texto".
11. Verifique as informações e pressione o botão Próximo.
12. Será enviado um código, via SMS, para o celular cadastrado. Verifique a mensagem, digite o código no campo em destaque e pressione o botão Próximo.




**Atenção:** O código tem validade e caso não funcione, clique em "**Reenviar código**"

13. As configurações do Múltiplo Fator de Autenticação de sua conta estão finalizadas. As telas a seguir podem ser fechadas:



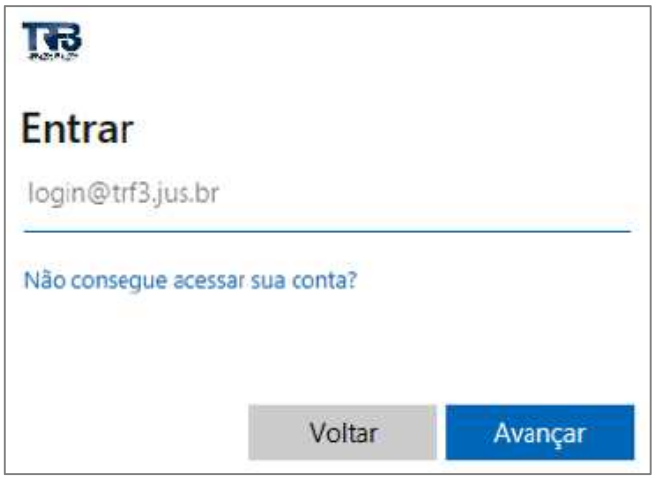

A partir desse momento, pode levar até duas horas para que as configurações feitas entrem em vigor.

Depois desse período, sempre que você se autenticar para utilizar os serviços em nuvem da Microsoft, vinculados à sua conta de rede na JF3R, será necessário utilizar o Múltiplo Fator de Autenticação que você escolheu nas configurações realizadas com o auxílio deste manual.

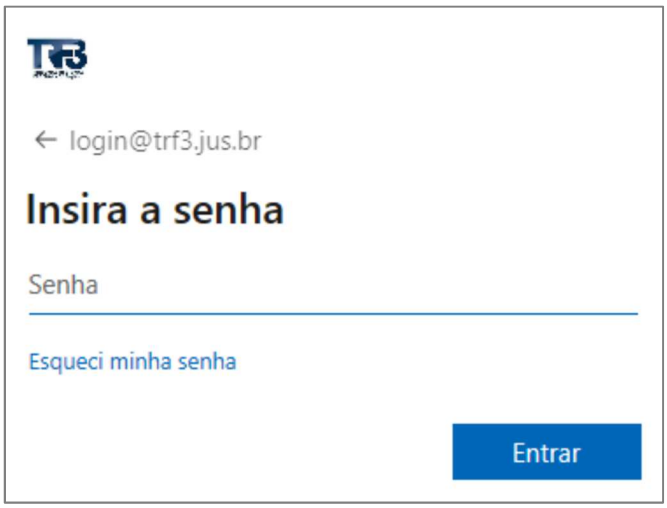
Para utilizar serviços como o **Teams, OneDrive, Office 365, será solicitado o Múltiplo Fator de Autenticação,** como segue:

1. Para se autenticar nos serviços descritos, caso ainda não esteja autenticado no ambiente de nuvem da Microsoft, será solicitado o logon. Preencha o formulário apresentado com o seu endereço de e-mail da JF3R.

(Por ex.: login@trf3.jus.br).




2. Pressione o botão Avançar e, na tela seguinte, insira sua senha da rede JF3R.




3. Pressione o botão Entrar. Na tela seguinte, para a verificação de sua identidade, escolha a opção Texto +XX XXXXXXXX09


4. Será enviado um código, via SMS, para o celular cadastrado. Verifique a mensagem, digite o código no campo em destaque e pressione o botão Verificar.


5. Pronto, a verificação da identidade através do Múltiplo fator de autenticação foi realizada com sucesso.
6. Logo após a configuração, a autenticação MFA será solicitada com frequência e irá diminuindo com o tempo usando o mesmo dispositivo

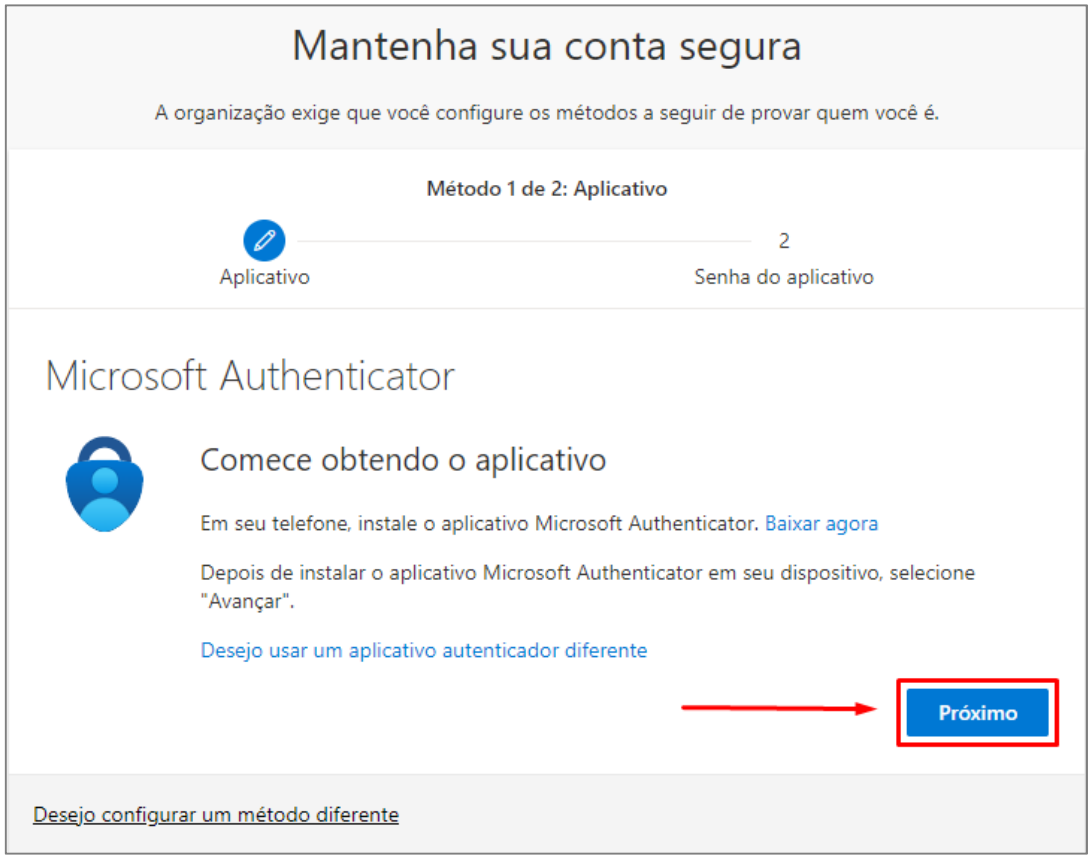
Caso haja dúvidas ou algum problema no procedimento de configuração do Múltiplo Fator de Autenticação, proceda a abertura de chamado.

# Procedimentos de Autenticação por aplicativo

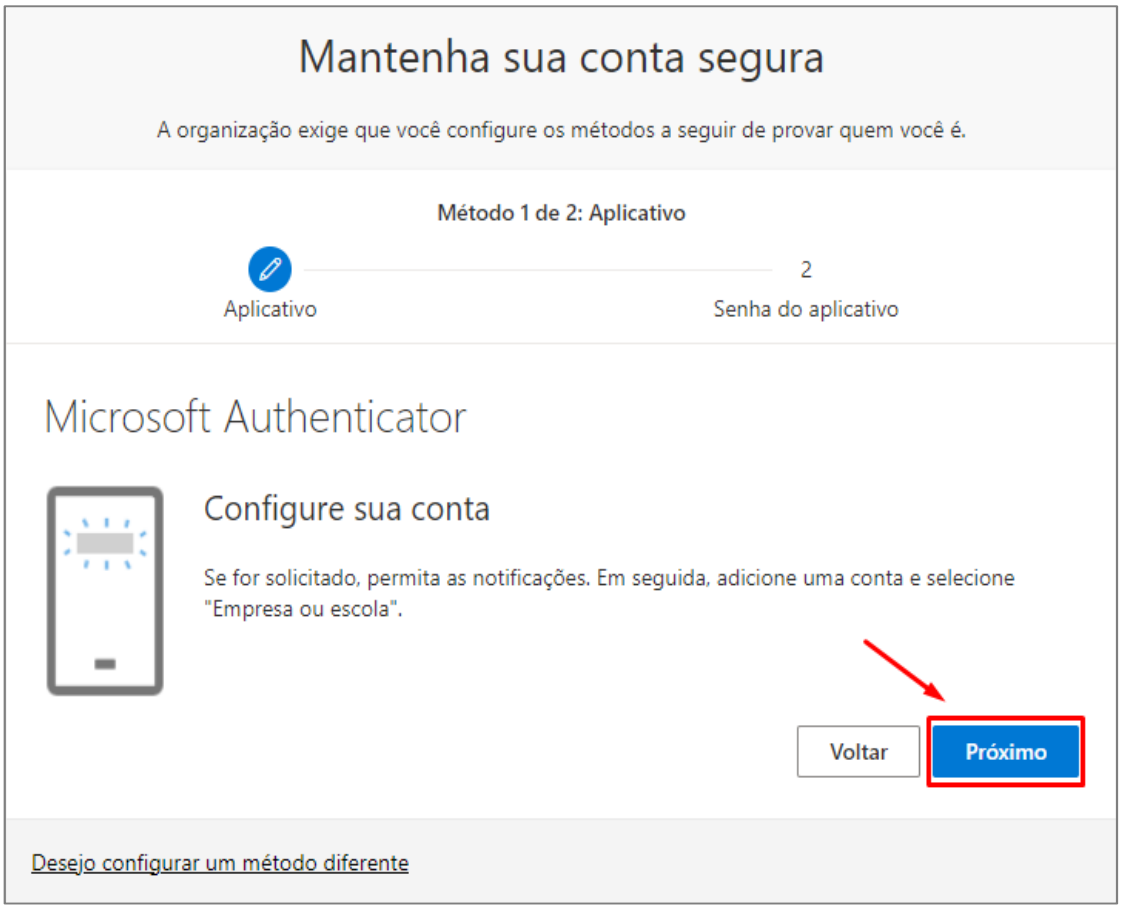
Como **alternativa** ao fator de autenticação por SMS, há o fator de autenticação por aplicativo. Para utilizá-lo, deve-se instalar o aplicativo Microsoft Authenticator no *smartphone*, conforme apontado na seção de requisitos.

O procedimento segue o mesmo até o passo 5 do manual e segue conforme a seguir:

1. Na tela "Mantenha sua conta segura", realize o download do aplicativo "Microsoft Authenticator" no seu *smartphone* e, após isso, clique no botão "Próximo".




2. Irá aparecer uma tela com instruções para cadastro do MFA no aplicativo Microsoft Authenticator no *smartphone*.

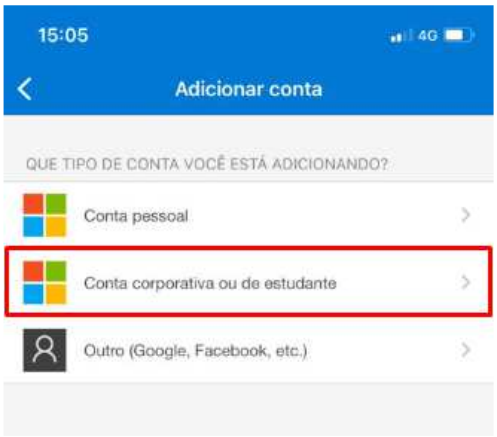



3. Conforme orientado na imagem, siga as seguintes instruções no aplicativo:

a) Abra o aplicativo Microsoft Authenticator no *smartphone*.

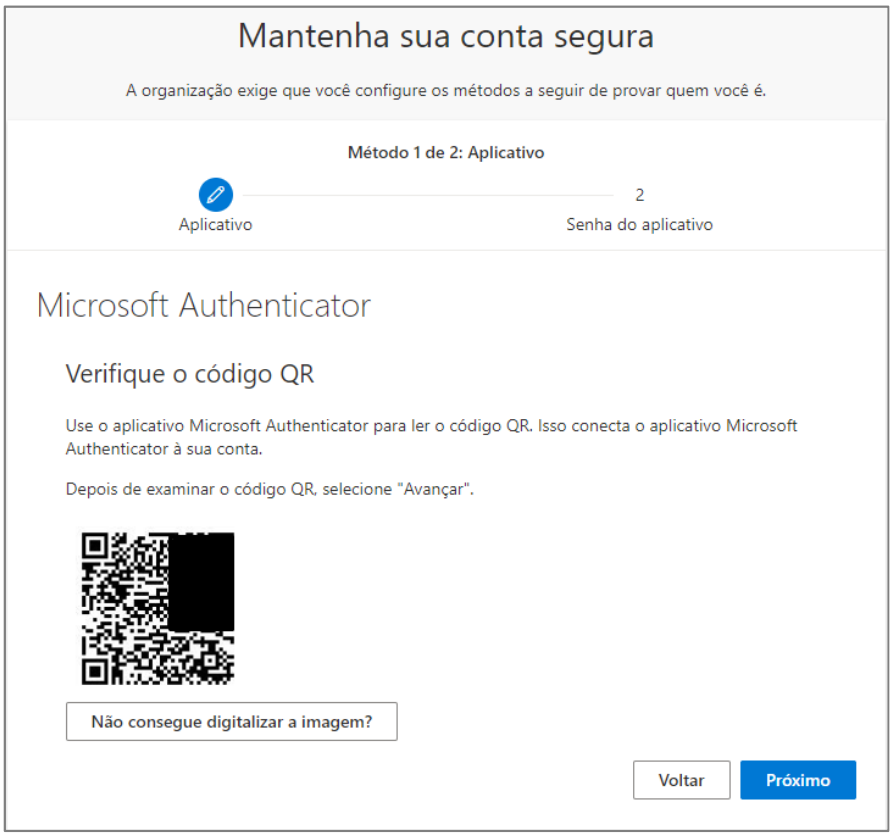
b) Selecione o símbolo + no canto superior direito do aplicativo.


c) Selecione a opção "Conta corporativa ou de estudante".

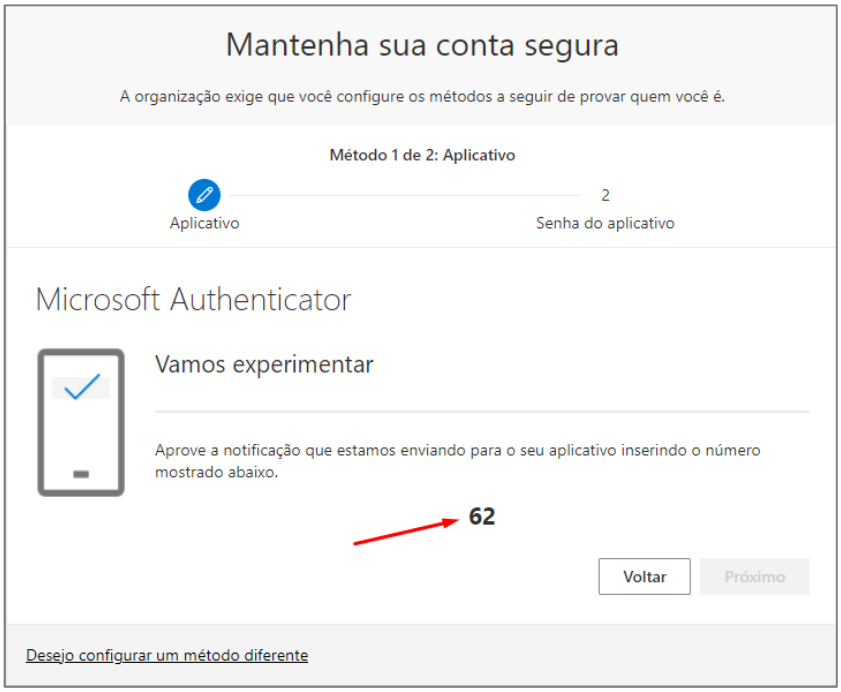


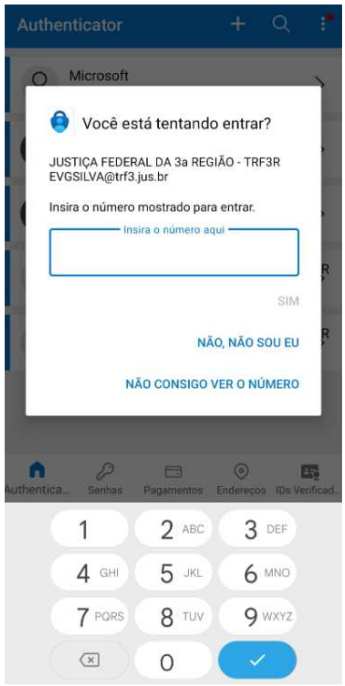
d) Selecione a opção "**Digitalizar código QR**".


4. Na tela do navegador onde está sendo realizada a configuração, após ter clicado em próximo, uma tela com um QR Code será exibida.

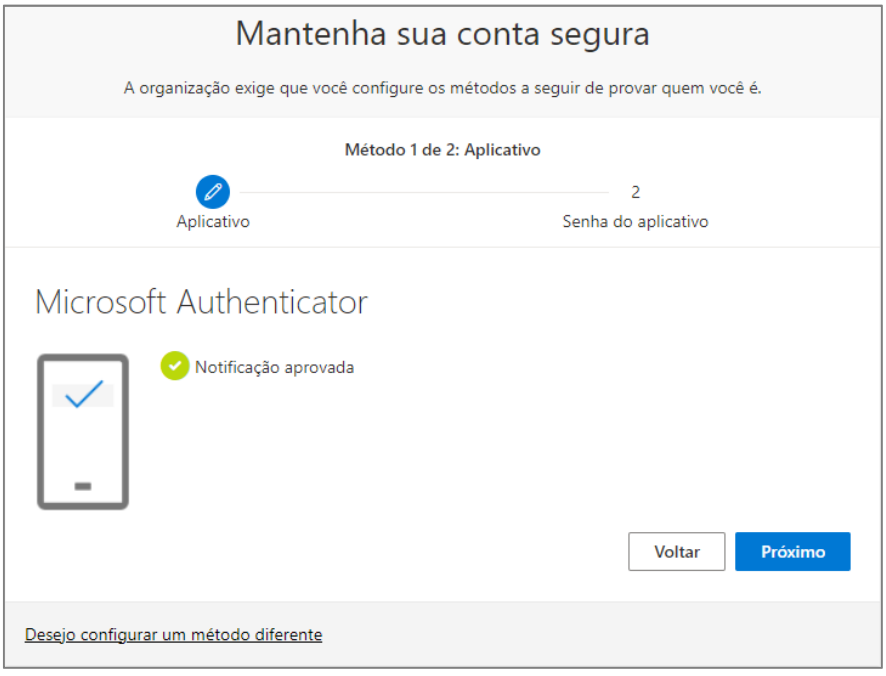


5. Aponte a câmera do *smartphone* para o QR Code. Uma tela de teste da configuração será exibida na tela com um número de dois dígitos e no *smartphone* uma notificação aparecerá, solicitando inserir o número exibido.

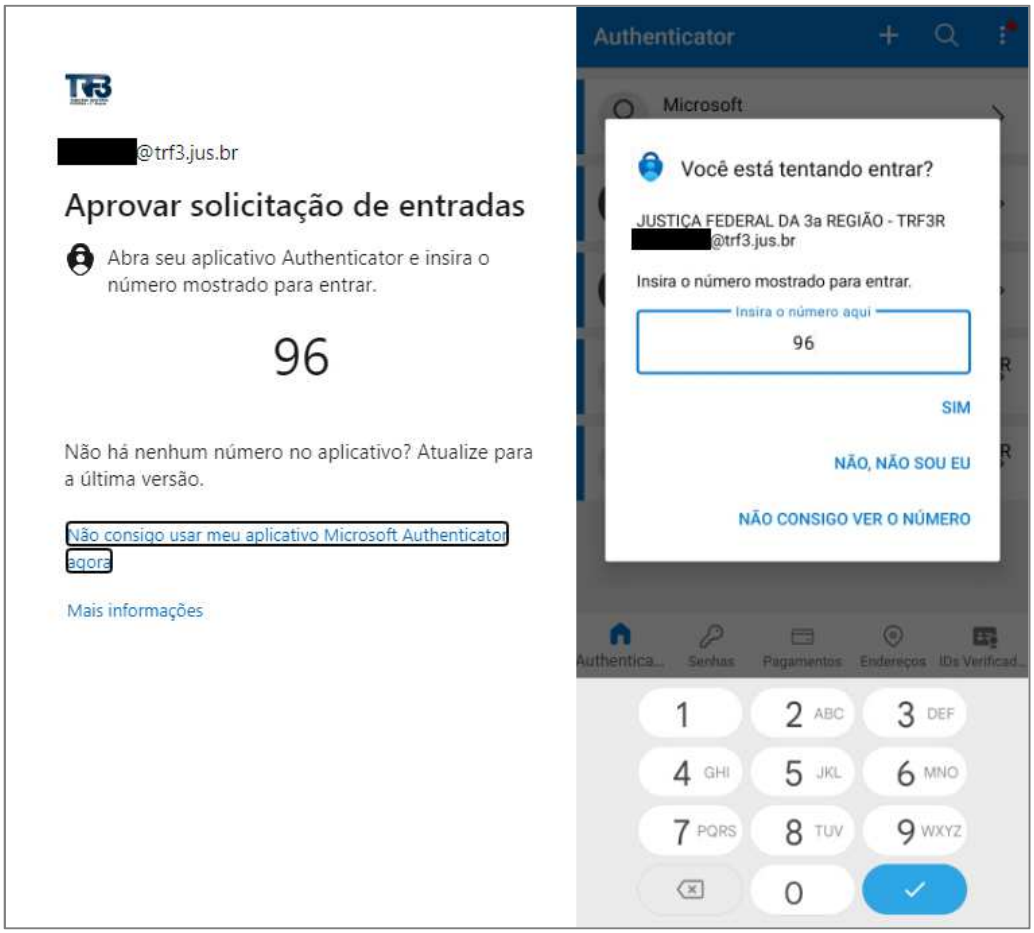



6. Basta digitar o número exibido na tela no aplicativo Microsoft Authenticator. Caso o número tenha sido digitado corretamente, uma tela de finalização da configuração será exibida e pode ser fechada.



7. Nas próximas vezes que for solicitado o fator de autenticação por aplicativo, a seguinte tela com um código de dois dígitos será exibida no computador. Enquanto isso, no smartphone aparecerá uma notificação solicitando o número informado na tela do computador. Após digitar o número corretamente, o *login* será validado.



JUSTIÇA FEDERAL

Tribunal Regional Federal da 3ª Região