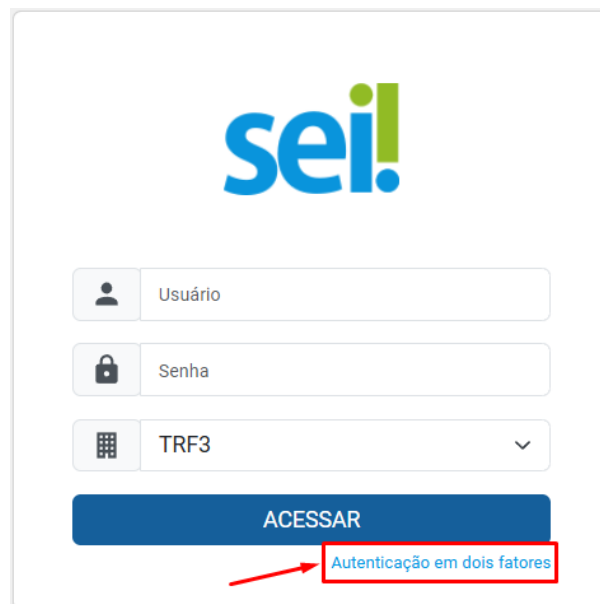


Autenticação em 2 Fatores

A autenticação em 2 fatores, ou 2FA, fornece segurança adicional, pois junta algo que você sabe (a sua senha) com algo que você possui (o seu smartphone). Somente com a combinação dos dois será possível efetuar o login. Após validar a senha, será preciso informar um código de 6 dígitos, que será gerado pelo aplicativo no smartphone.

1. Gerando um Código para Ativação

Na tela de login do sistema, após informar seu usuário, senha e o órgão, clique no link “Autenticação em dois fatores”:



A tela de login do sistema SEI! apresenta o logo "sei!" no topo. Abaixo dele, há três campos de entrada: "Usuário" (com ícone de pessoa), "Senha" (com ícone de cadeado) e "TRF3" (com ícone de teclado numérico e uma seta para baixo). Abaixo dos campos, há um botão azul "ACESSAR". À direita do botão, há um link "Autenticação em dois fatores" destacado por um retângulo vermelho, com uma seta vermelha apontando para ele.

Clique no botão “Prosseguir” na tela de apresentação da Autenticação em 2 Fatores:



A tela de apresentação da Autenticação em 2 Fatores apresenta o logo "sei!" no topo. Abaixo dele, há um texto explicativo: "A autenticação em 2 fatores é um recurso para adicionar maior segurança no seu acesso ao sistema. Ao ativá-la, qualquer tentativa de login, em dispositivos não liberados, irá requerer também um código numérico gerado por um aplicativo." Abaixo do texto, há um link "aqui" para as instruções. Abaixo do link, há dois botões: "Prosseguir" (destacado por um retângulo vermelho) e "Cancelar".

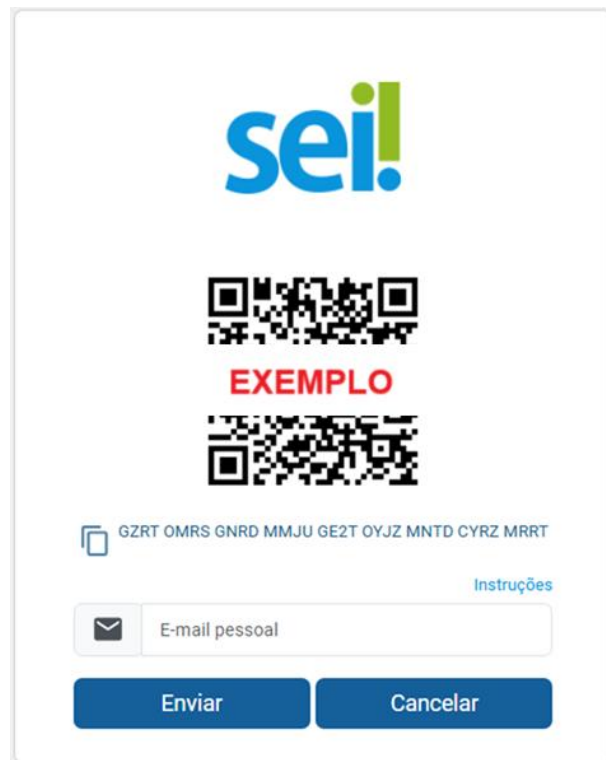
A mensagem abaixo será exibida e se você nunca fez este procedimento apenas ignore-a:



A mensagem de atenção é exibida em uma caixa de diálogo com o título "sei.trf3.jus.br diz". O texto principal diz: "ATENÇÃO: Se a sua conta 'SEI/TRF3' já estiver registrada no aplicativo certifique-se de excluí-la antes da leitura do código QR." Abaixo do texto, há um botão "OK".

2. Instalação do Aplicativo de Autenticação

Será gerado um código QR como este:



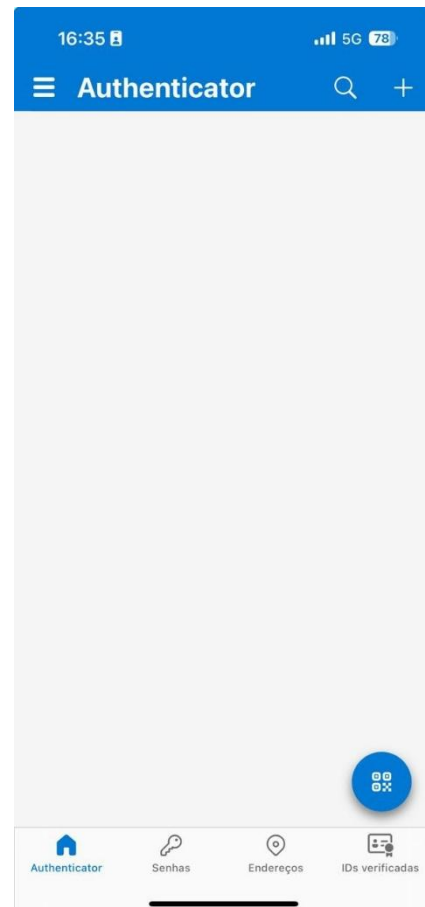
Para lê-lo, é necessário instalar em seu smartphone um aplicativo de autenticação em duas etapas, como o Microsoft Authenticator, Google Authenticator, FreeOTP, Authy, entre outros. Os exemplos a seguir demonstram o uso do Microsoft Authenticator, recomendado para uso na Justiça Federal da 3ª Região. Você pode baixá-lo na Apple Store ou Google Play.



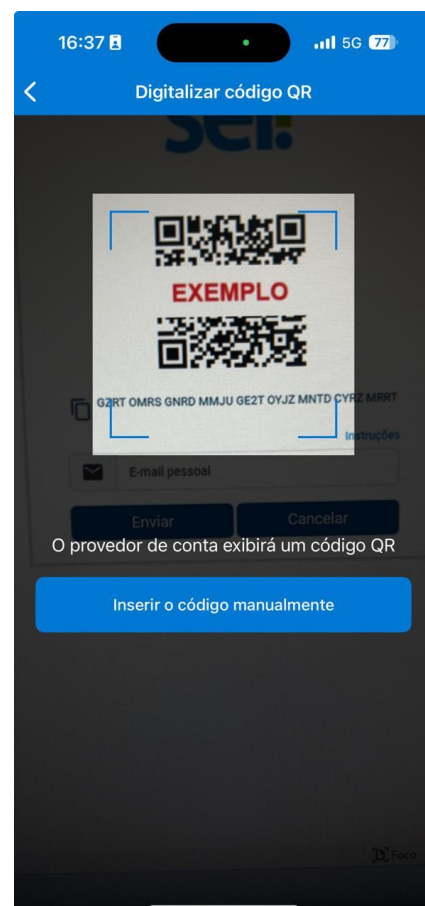
3. Leitura do Código

Abra o aplicativo Microsoft Authenticator em seu smartphone:

Encontre a opção para leitura de código. Pode ser necessário permitir que o aplicativo tenha acesso a câmera do smartphone:



Aponte a câmera para o código QR que está sendo exibido na tela e adicione a conta no aplicativo.



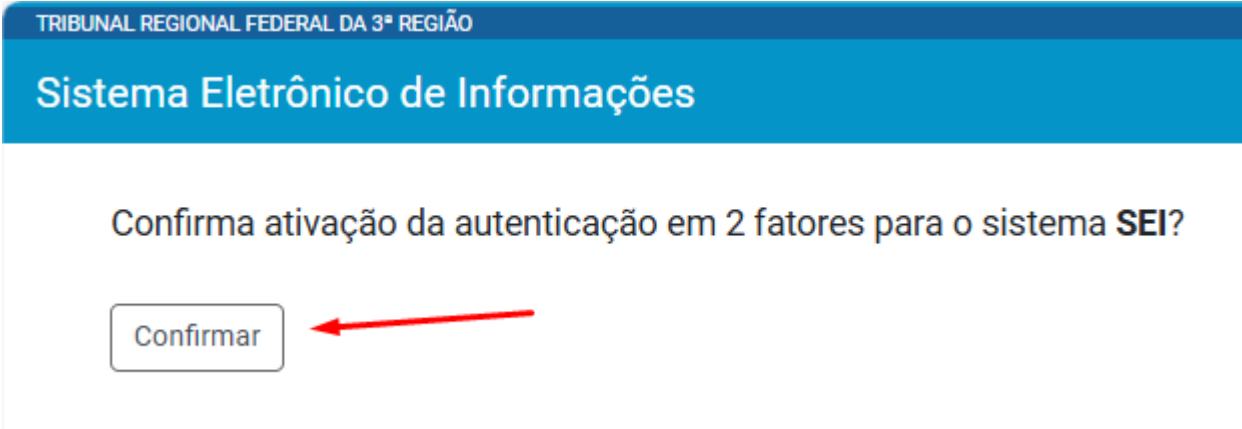
4. Finalização do Cadastro

Informe um endereço de e-mail que **não seja associado com a instituição**. Por exemplo, pode ser do gmail, hotmail, yahoo etc. É imprescindível que a senha de acesso ao e-mail seja diferente da senha de acesso ao sistema:



The image shows a web interface for SEI! (Sistema Eletrônico de Informações). At the top is the SEI! logo. Below it are two QR codes, with the word "EXEMPLO" in red text between them. Under the QR codes is a small icon of a document and a string of alphanumeric characters: "GZRT OMRS GNRD MMJU GE2T OYJZ MNTD CYRZ MRRT". To the right of this string is a link labeled "Instruções". Below this is an email input field with an envelope icon on the left and the placeholder text "seu_email@seu_provedor". At the bottom are two blue buttons: "Enviar" and "Cancelar".

Clique em "Enviar" para que um link de ativação seja enviado para o endereço de e-mail fornecido. Somente após receber o e-mail e clicar no link e confirmar a ativação da autenticação em 2 fatores é que o mecanismo de autenticação em 2 fatores estará ativado.



The image shows a confirmation screen for the SEI! system. At the top is a blue header bar with the text "TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO" in white. Below the header is a blue bar with the text "Sistema Eletrônico de Informações" in white. The main content area has a light gray background. It contains the text "Confirma ativação da autenticação em 2 fatores para o sistema SEI?". Below this text is a button labeled "Confirmar". A red arrow points to the "Confirmar" button.

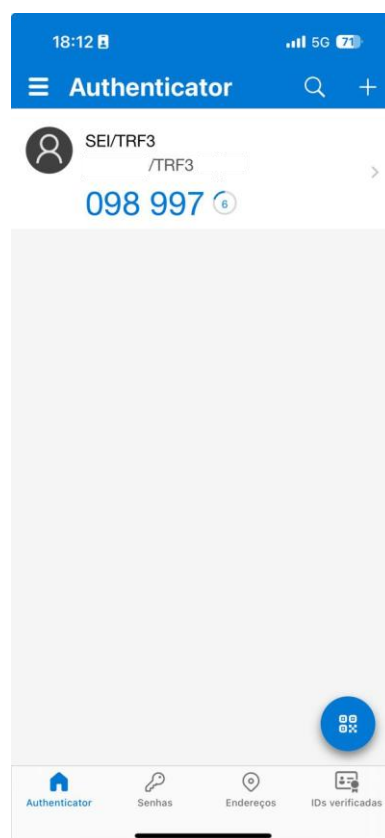
5. Login com a Autenticação em 2 Fatores

Se a autenticação em 2 fatores estiver ativada, então, após informar o usuário e senha, será exibida outra tela solicitando o código numérico.



A tela de autenticação em 2 fatores do SEI. No topo, há o logotipo "sei!" em azul e verde. Abaixo, o texto "Informe o código de 6 números gerado pelo aplicativo de autenticação em 2 fatores:". Segue um campo de entrada com o ícone de uma fechadura e o rótulo "Código de Acesso". Abaixo deste campo, há uma opção desativada com o texto "Não usar 2FA neste dispositivo e navegador". Na base da tela, há um link "Instruções" e dois botões azuis: "Validar" e "Desativar 2FA".

Abra o aplicativo de autenticação no seu smartphone e veja o código gerado. Informe o valor no campo Código de Acesso e clique botão “Validar”:



De agora em diante, sempre que fizer login, será preciso consultar o seu smartphone, porque o código muda a cada 30 segundos. O sistema aceitará qualquer um dos códigos gerados nos últimos 90 segundos por isso é importante que o seu smartphone esteja com o horário correto.

5.1. Liberando dispositivos usado com frequência

Para dispositivos usados com frequência, pode ser conveniente liberá-los da validação a cada login. Para isso, na tela onde é solicitado o código numérico, marque a opção "Não usar 2FA neste dispositivo e navegador". Essa sinalização precisará ser realizada para cada navegador utilizado. O código poderá ser solicitado novamente se for feita a limpeza dos cookies do navegador ou se a liberação perder a validade de acordo com o período estabelecido pela instituição.



A interface de login do SEI! apresenta o logotipo no topo. Abaixo, há uma instrução: "Informe o código de 6 números gerado pelo aplicativo de autenticação em 2 fatores:". Segue um campo de entrada com um ícone de cadeado e o rótulo "Código de Acesso". Abaixo deste campo, há uma opção desativada com o texto "Não usar 2FA neste dispositivo e navegador". Uma seta vermelha aponta para esta opção. Abaixo da opção, há um link "Instruções" e dois botões azuis: "Validar" e "Desativar 2FA".

Para cancelar as liberações, em todos os dispositivos, acesse o link "Autenticação em 2 fatores" disponível na tela inicial de login e clique no botão "Cancelar Dispositivos Liberados":

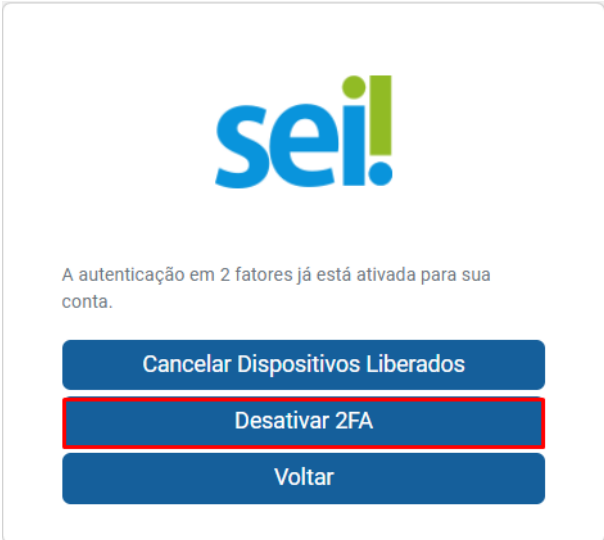


A interface de login do SEI! apresenta o logotipo no topo. Abaixo, há uma mensagem: "A autenticação em 2 fatores já está ativada para sua conta.". Seguem três botões azuis empilhados: "Cancelar Dispositivos Liberados" (destacado com um retângulo vermelho), "Desativar 2FA" e "Voltar".

6. Desativando a Autenticação em 2 Fatores

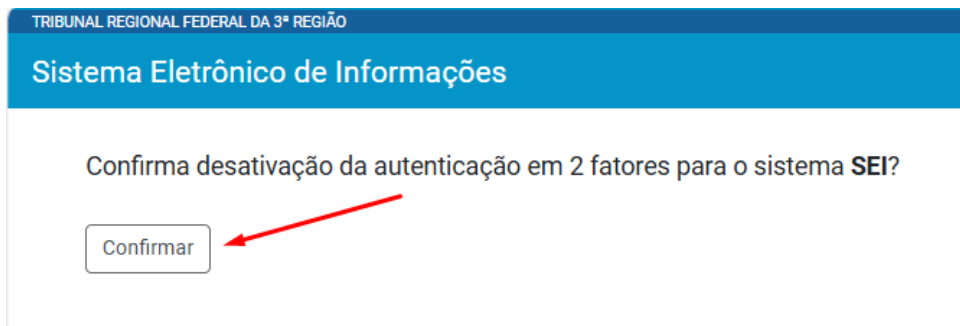
Se não conseguir validar o código por algum motivo (perda do aparelho, defeito, roubo, erro no aplicativo etc.), é possível requisitar a desativação da autenticação em 2 fatores na mesma tela onde é solicitado o código numérico, ou então por meio do link "Autenticação em 2 fatores" disponível na tela inicial de login.

Clique no botão "Desativar 2FA" para que um e-mail com o link de desativação seja enviado para o endereço e-mail que foi fornecido no momento da leitura do código QR



A tela exibe o logo do SEI (Sistema Eletrônico de Informações) no topo. Abaixo, há uma mensagem informando que a autenticação em 2 fatores já está ativada para a conta. No rodapé, há três botões: "Cancelar Dispositivos Liberados", "Desativar 2FA" (destacado com uma borda vermelha) e "Voltar".

Somente após receber o e-mail e clicar no link e confirmar a desativação da autenticação em 2 fatores é que o mecanismo de autenticação em 2 fatores estará desativado.

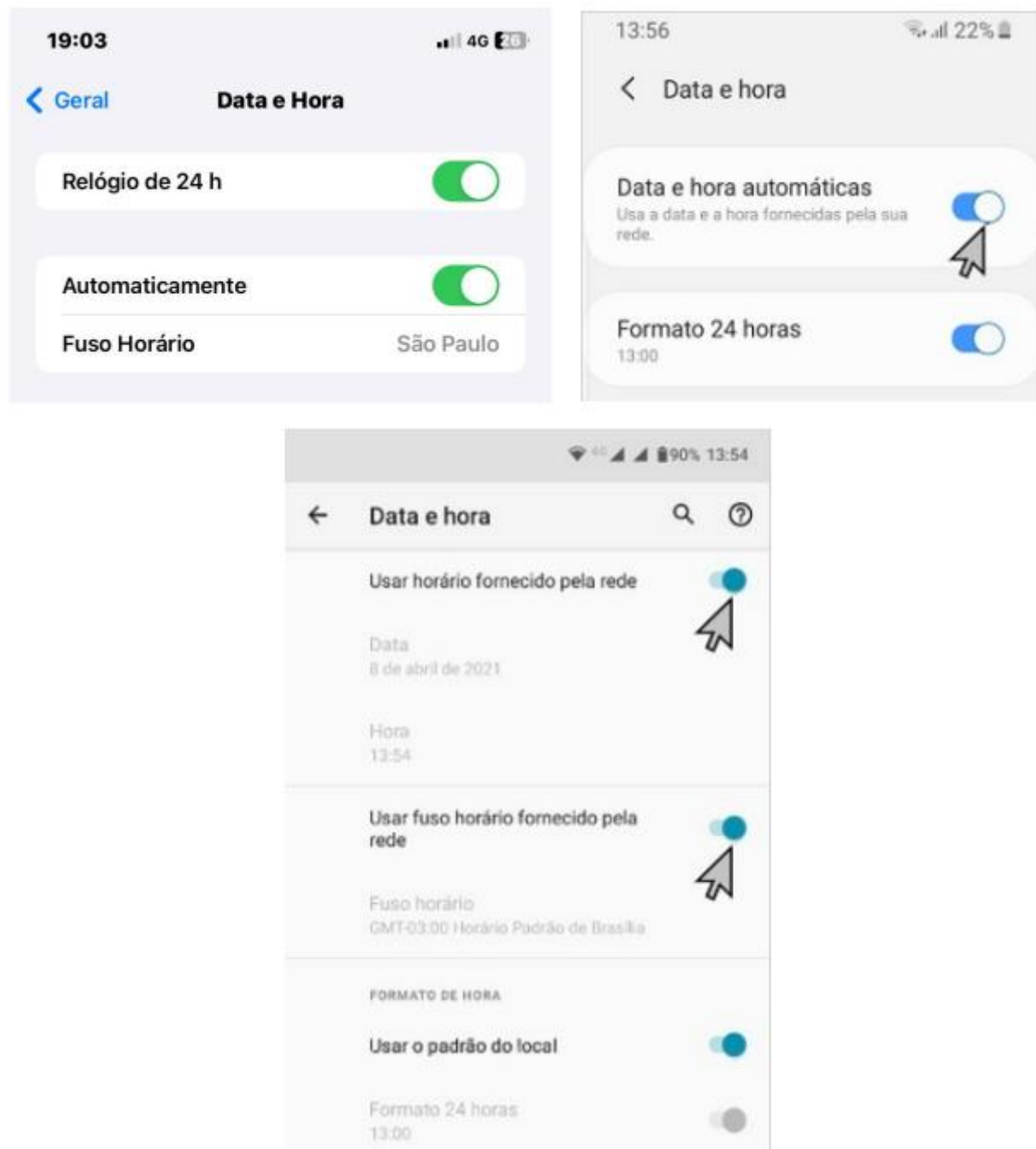


A tela exibe o cabeçalho do SEI (Sistema Eletrônico de Informações) e a mensagem "Confirma desativação da autenticação em 2 fatores para o sistema SEI?". Abaixo, há um botão "Confirmar" com uma seta vermelha apontando para ele.

7. Solução de problemas

7.1 Problemas para validação do código pelo Sei!

Caso esteja recebendo a mensagem "Código de autenticação inválido" ou "Código de autenticação não reconhecido", é possível que o horário no seu smartphone esteja desatualizado. Verifique se o aparelho está configurado para obter a hora automaticamente pela rede. Abaixo estão exemplos de como fazer isso em diferentes sistemas.



7.2 Como remover um código depois da desativação do 2FA no Sei! ou se necessário

A mensagem **“Código de autenticação inválido”** ou **“Código de autenticação não reconhecido”** também pode aparecer quando se tenta reutilizar um código antigo cadastrado no aplicativo de autenticação do smartphone.

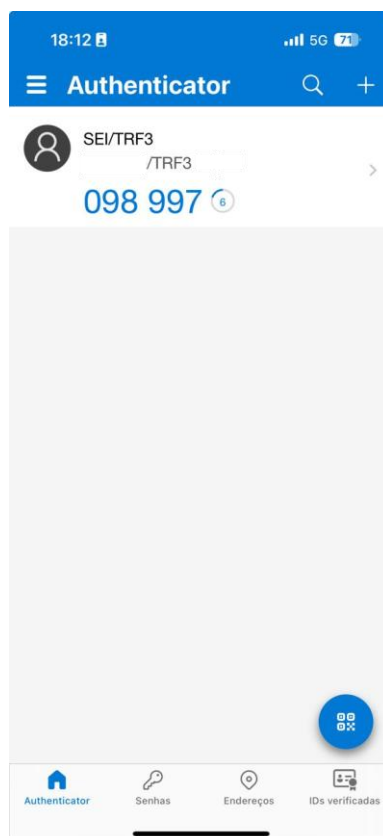
Se o 2FA for desativado no sistema por qualquer motivo, **não será possível reutilizar o código anteriormente registrado em seu smartphone.**

Para cadastrar um novo código, é necessário **remover o código antigo no aplicativo de autenticação** e, em seguida, **gerar e cadastrar um novo código no sistema**, evitando assim erros de validação.

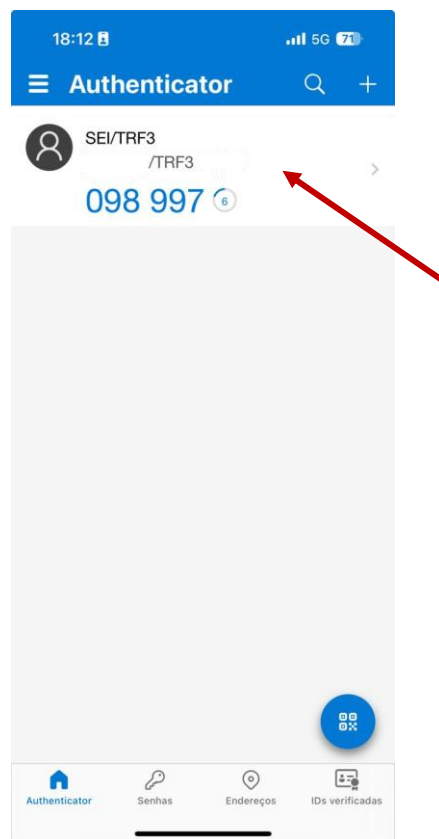
Abra o aplicativo Microsoft Authenticator em seu smartphone:



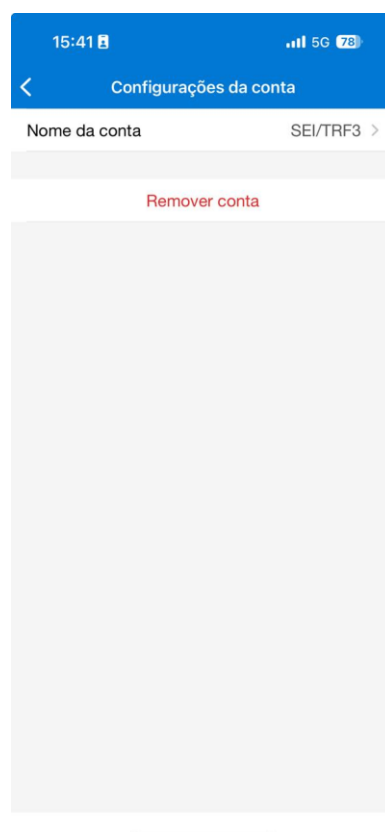
Na tela inicial, será exibida a lista de contas já cadastradas



Localize a conta do sistema Sei! (ela deve estar identificada pelo nome que foi configurado quando você adicionou o 2FA) e toque sobre essa conta



Toque no botão Remover conta



Confirme a remoção quando o aplicativo solicitar

