

Manual do Usuário

AUTENTICAÇÃO MULTIFATOR (MFA)

SEI – Processo Administrativo Eletrônico

SUMÁRIO

1.	Introdução	3
2.	Autenticação Multifator	4
2.1	Cadastro	4
2.2	Instalação do Aplicativo de Autenticação	6
2.3	Leitura do QR Code	6
2.4	Configuração Manual do Código	8
2.5	Finalização do Cadastro	10
2.5.1	Validando o Link Recebido	11
3.	Login com a Autenticação de Dois Fatores	13

AUTENTICAÇÃO MULTIFATOR (MFA)

1. Introdução

Esta Dica de Sistema tem como objetivo orientar de forma simples o passo a passo para realizar o procedimento da **Autenticação Multifator (MFA)**, via Microsoft Authenticator, para acesso no sistema **SEI – Processos Administrativo Eletrônico**.

Esta melhoria impacta diretamente na segurança e garante a autenticidade dos usuários internos para acessarem os sistemas do **Tribunal de Justiça**, garantindo um ambiente mais seguro.

2. Autenticação Multifator

2.1 Cadastro

Para realizar a **Autenticação Multifator**, na área de login do sistema **SEI**, informe o **Usuário** e **Senha** de acesso, e logo após clique na opção **Autenticação em dois fatores**.



A imagem mostra a interface de login do sistema SEI. No topo, há o logotipo "sei!" em azul e verde. Abaixo, há dois campos de entrada: "Usuário" (com ícone de pessoa) e "Senha" (com ícone de cadeado). Ambos os campos são destacados por uma borda laranja. Abaixo dos campos, há um botão azul com o texto "ACESSAR". À direita do botão, há um link azul com o texto "Autenticação em dois fatores", também destacado por uma borda laranja.

Figura 1 - Tela de usuário e senha.

A tela é habilitada trazendo informações para configurar o recurso de segurança. Clique na opção **Prosseguir** para continuar com a configuração ou **Cancelar** para encerrar procedimento.



A imagem mostra a tela de configuração da autenticação. No topo, há o logotipo "sei!" em azul e verde. Abaixo, 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." Segue o texto: "Antes de prosseguir, leia as instruções [aqui](#)." No rodapé, há dois botões azuis: "Prosseguir" e "Cancelar", ambos destacados por uma borda laranja.

Figura 2 - Tela de Configuração da Autenticação.

Após clicar em **Prosseguir**, o sistema exibe uma mensagem, e, caso não tenha feito o procedimento mencionado, basta ignorá-la clicando em **Ok**.

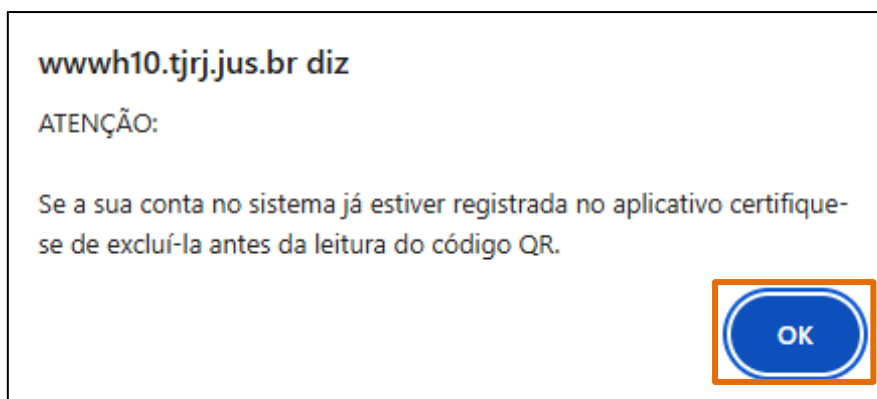


Figura 3 - Mensagem de Atenção.

Em seguida, o sistema gera e exibe um **QR Code** para leitura via aplicativo **Microsoft Authenticator**, usando seu smartphone.



Figura 4 - Tela do QR Code.

2.2 Instalação do Aplicativo de Autenticação

Para prosseguir com a configuração e com a leitura do **QR Code**, caso não tenha instalado, será necessário instalar em seu smartphone o aplicativo **Microsoft Authenticator** para autenticação em duas etapas, através da loja de aplicativo **Apple Store** ou **Google Play**.



Figura 5 - Plataformas para Download do App.

2.3 Leitura do QR Code

Após efetuar o download, abra o aplicativo e encontre a opção para leitura do QR Code.

Clique no botão + e, em seguida, selecione o tipo **Conta Corporativa** ou clique no **botão azul** para ler o **QR Code**.

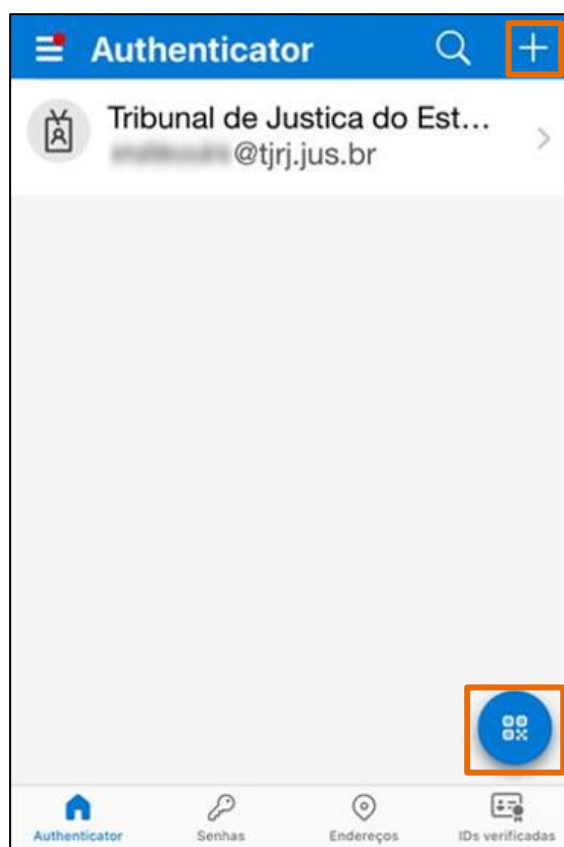


Figura 6 -Tela inicial do Microsoft Authenticator.

Aponte a câmera do celular para o **QR Code** exibido na tela do computador para que o sistema faça a leitura e adicione automaticamente a conta ao aplicativo.

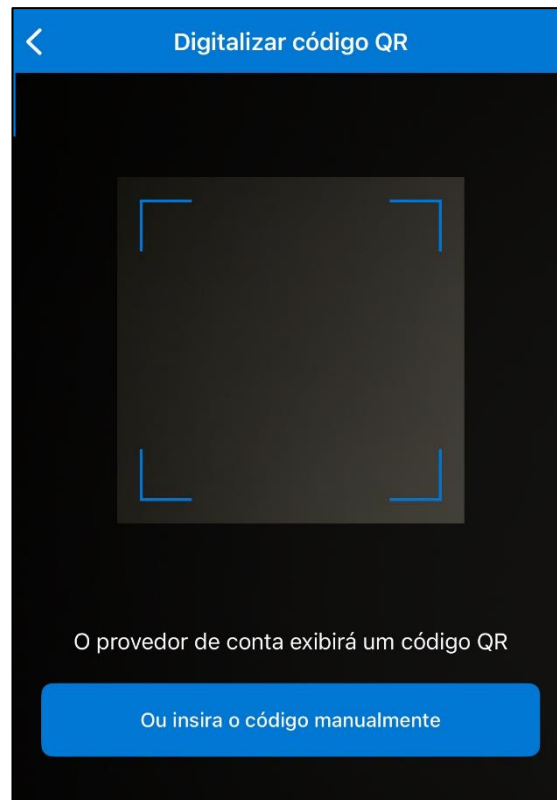


Figura 7 - Tela para leitura de QR Code.

A conta **SEI** adicionada é exibida na Tela inicial do seu aplicativo.

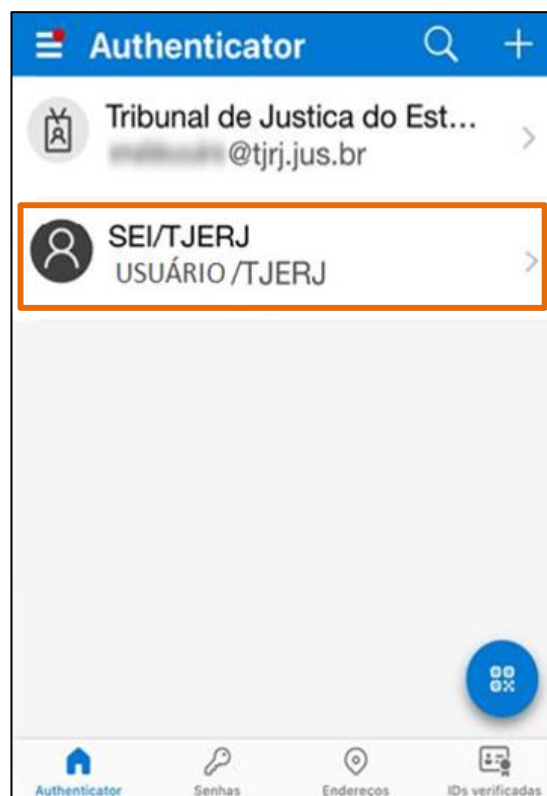


Figura 8 - Tela inicial do Microsoft Authenticator – Conta adicionada.

2.4 Configuração Manual do Código

Caso não esteja conseguindo efetuar a leitura do QR Code no aplicativo **Microsoft Authenticator**, na tela **Digitalizar QR Code**, clique no botão **Ou insira o código manualmente**.



Figura 9 - Inserir o código manualmente.

A tela **Adicionar conta** é exibida, selecione o tipo de conta **Outro (Google, Facebook, etc.)**.

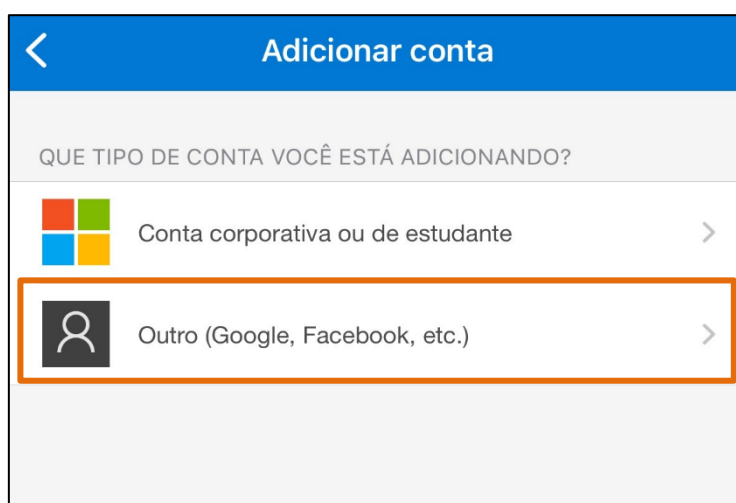


Figura 10 - Adicionar conta.

Na tela **Adicionar conta** do aplicativo, o sistema habilita os campos **Nome da conta** e **Chave secreta** para preenchimento.

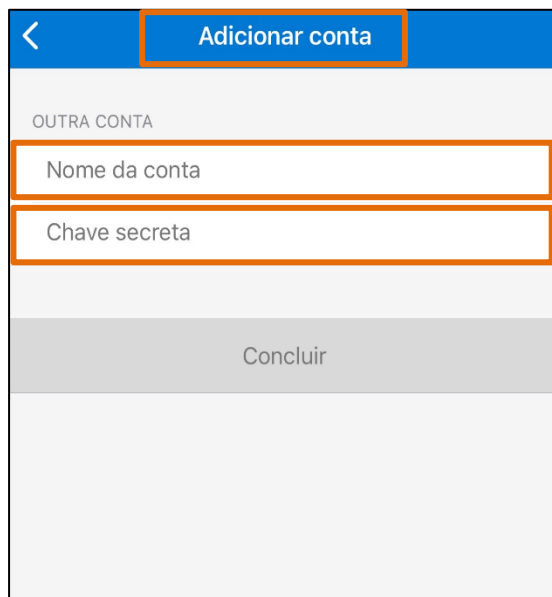


Figura 11 - Adicionar conta - Campos Nome da conta e Chave secreta.

Preencha o campo **Nome da conta** utilizando o modelo **SISTEMA/ÓRGÃO (USUÁRIO)**.

Para o preenchimento do campo **Chave secreta**, vá à tela do sistema **SEI**, clique sobre o **código alfanumérico** que é exibido abaixo do **Código QR Code** para copiá-lo, ou, digite manualmente o código se estiver pelo computador. Em seguida, cole-o no campo **Chave secreta** do aplicativo de autenticação e clique em **Concluir**.

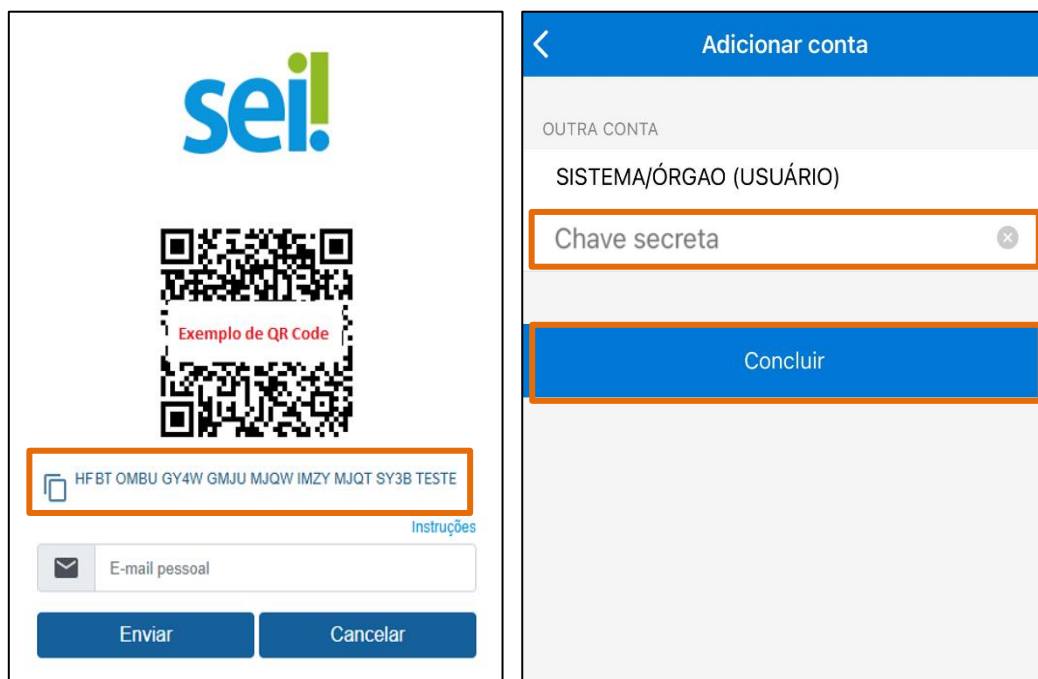


Figura 12 - Inserção de Chave secreta.

2.5 Finalização do Cadastro

Para finalizar o cadastro, informe um endereço de **e-mail pessoal**, não sendo permitido a utilização do e-mail associado com a instituição. Exemplos de e-mails que podem ser utilizados são os do **Gmail, Hotmail, Yahoo, entre outros**.

⚠️ ATENÇÃO: É imprescindível que a **Senha de Acesso** ao e-mail, seja diferente da **senha de acesso ao sistema**.

Informe o **e-mail** e clique em **Enviar**.



Figura 13 - Tela do QR Code.

O sistema exibe uma mensagem informando o envio de e-mail com o link de ativação para o endereço de e-mail fornecido, com validade de **60 minutos**, para habilitar a **Autenticação de dois fatores**.

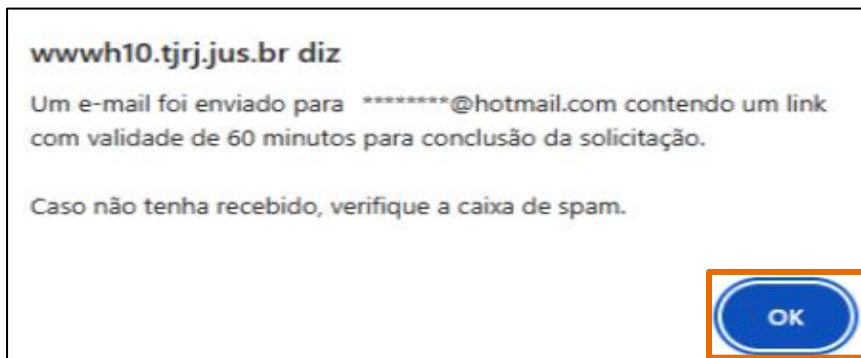


Figura 14 - Mensagem informando o envio de e-mail.

2.5.1 Validando o Link Recebido

Acesse o e-mail cadastrado anteriormente e verifique o recebimento do e-mail encaminhado pelo **SEI/TJERJ**, em seguida, clique no **link**.

 **OBSERVAÇÃO:** Caso não encontre o e-mail em sua **Caixa de Entrada**, verifique a **Caixa de Spam** e **Lixo eletrônico**.

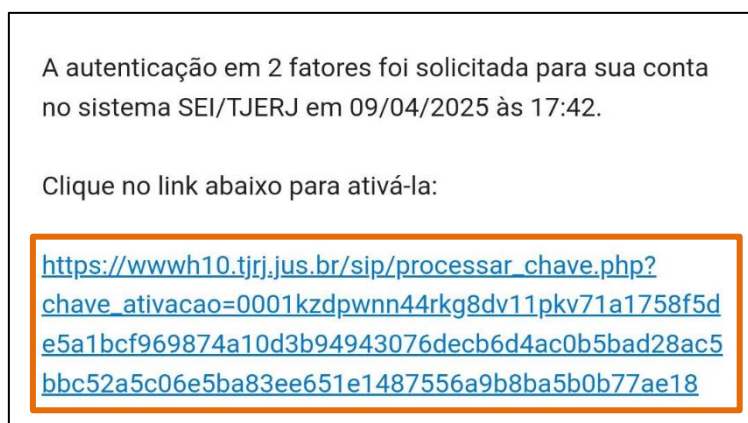


Figura 15 - Exemplo do e-mail contendo o link de ativação.

Em seu navegador é exibida uma guia, solicitando a confirmação da ativação da autenticação em dois fatores no sistema **SEI**. Clique em **Confirmar** para prosseguir.

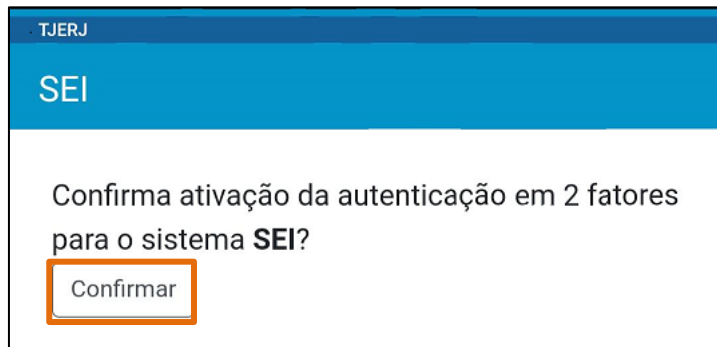


Figura 16 - Guia aberta no navegador para confirmação.

Após confirmação, o sistema exibe a mensagem informativa, confirmando a ativação.

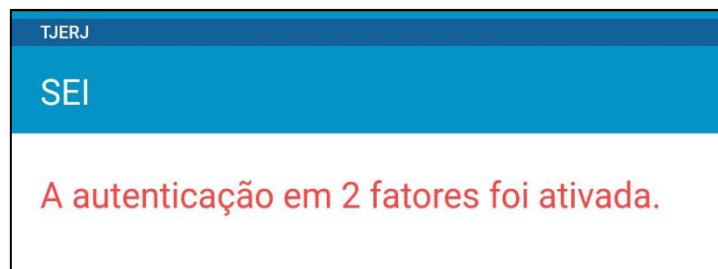


Figura 17 - Autenticação em dois fatores ativada.

3. Login com a Autenticação de Dois Fatores

Após a ativação da **Autenticação de Dois Fatores**, acesse o **sistema SEI** utilizando o **login** e a **senha** de acesso ao sistema. A tela é atualizada solicitando o **Código de Acesso**, uma sequência numérica é gerada no aplicativo autenticador.



The screenshot shows the SEI login interface. At the top is the 'sei!' logo. Below it, a message asks the user to enter a 6-digit code generated by the authenticator app. A text input field with a lock icon and the label 'Código de Acesso' is highlighted with an orange border. Below the input field is a checkbox labeled 'Não usar o 2FA neste dispositivo e navegador'. There is a link for 'Instruções' and two buttons at the bottom: 'Desativar 2FA' and 'Validar'.

Figura 18 - Tela de inserção de Código de acesso.

No **Aplicativo**, selecione o **perfil SEI** criado anteriormente após a leitura do QR Code.

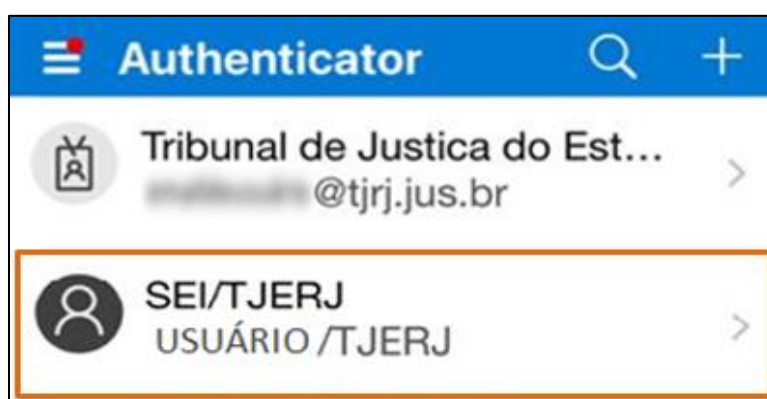


Figura 19 - Selecionar perfil criado no aplicativo.

Ao abri-lo, o aplicativo exibe o **código** com duração temporária para verificação em dois fatores.




Figura 20 - Tela do app Authenticator.

No computador, insira o **código** do aplicativo no campo **Código de Acesso** e clique em **Validar**.



Figura 21 - Tela de inserção de código de acesso.

 **OBSERVAÇÃO:** Vale destacar que, ao efetuar o login, é necessário inserir o **código** gerado no aplicativo do smartphone e o código muda a cada **trinta segundos**.

O sistema aceita qualquer um dos **códigos gerados nos últimos noventa segundos**, desde que o smartphone esteja com a hora correta.

DÚVIDAS?

Entre em contato com o nosso Atendimento:



SGTEC.ATENDIMENTO@TJRJ.JUS.BR



ATENDIMENTO POR TELEFONE (21) 3133-9100