SEI - Autenticação em 2 Fatores

Ações

Categoria: Software Externo Aplicativo

Assunto

SEI - Autenticação em 2 Fatores

Conteúdo

Este procedimento orienta como configurar a autenticação em 2 fatores para o SEI.

Aplica-se para:

- SEI

Informações

A autenticação em 2 fatores, ou 2FA, fornece segurança adicional.

Após validar a senha no SEI, será preciso informar um código de 6 dígitos, que será gerado pelo aplicativo de autenticação no seu smartphone.

Procedimento

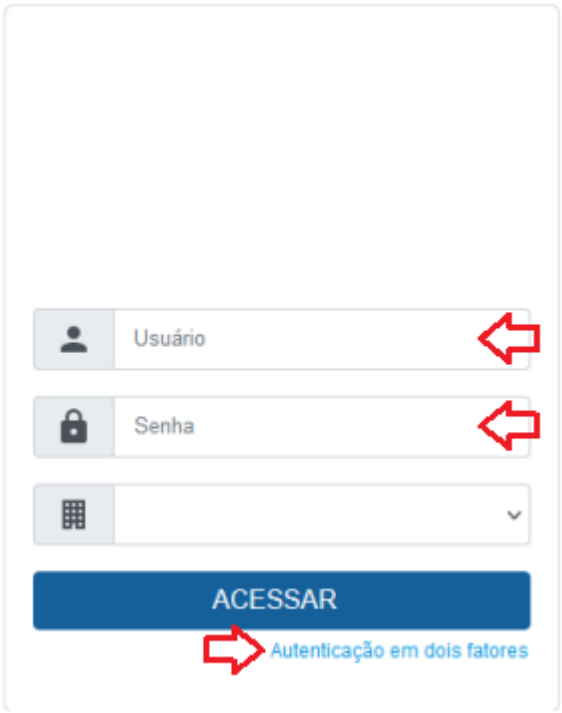
Procedimento a ser executado pela Central de Serviços:

1. Acessar o link: **https://sei.trf2.jus.br**

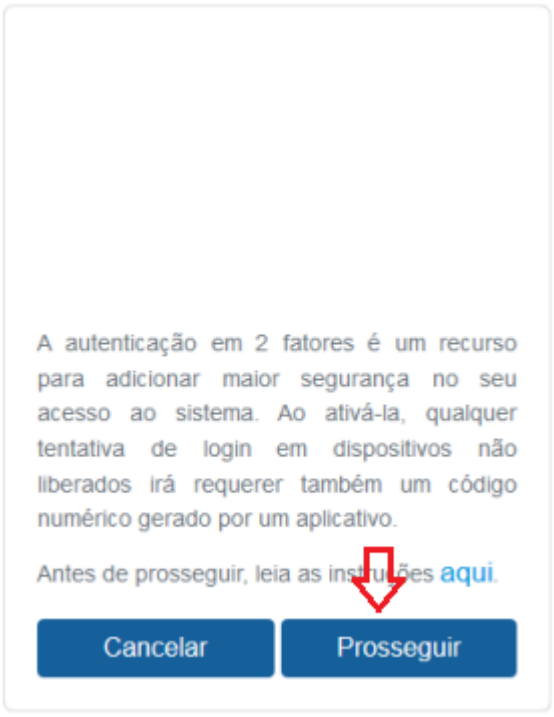
2. Informar o "Usuário" (sigla).

3. Informar a "Senha" (senha de rede).

4. Clicar no link "Autenticação em dois fatores".



5. Clicar em "Prosseguir".



Obs: Será exibida a mensagem abaixo, caso nunca tenha realizado o procedimento, ignore-a.

6. Clicar em "Ok".



7. Realizar a leitura do QrCode.



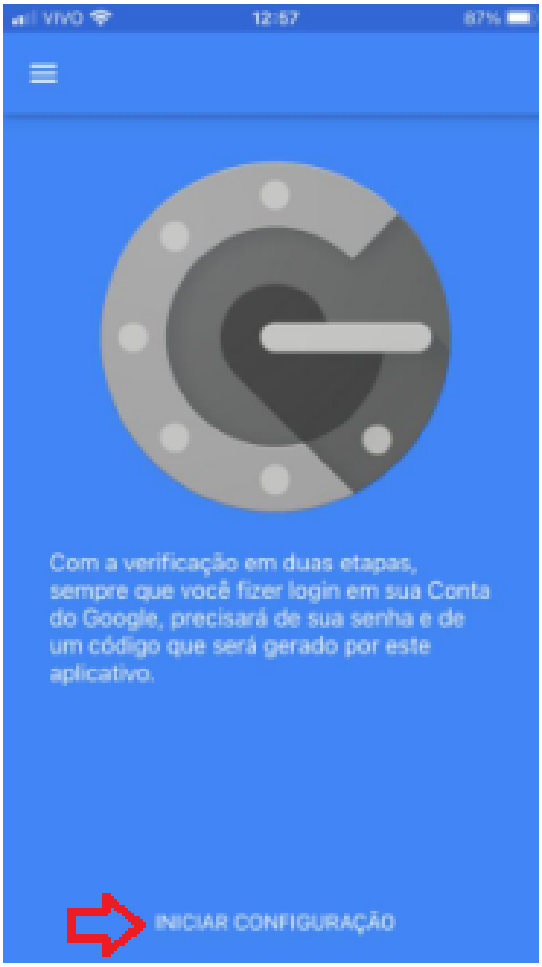
OBS: Caso não tenha um aplicativo de autenticação em 2 fatores, acessar a galeria de aplicativos do seu smartphone e realizar a instalação como o Google Authenticator, Microsoft Authenticator, FreeOTP, Authy, etc.

Recomendação: Instalar o aplicativo de autenticação **Google Authenticator.**

8. Abrir o Google Authenticator.



9. Clicar em "Iniciar configuração".

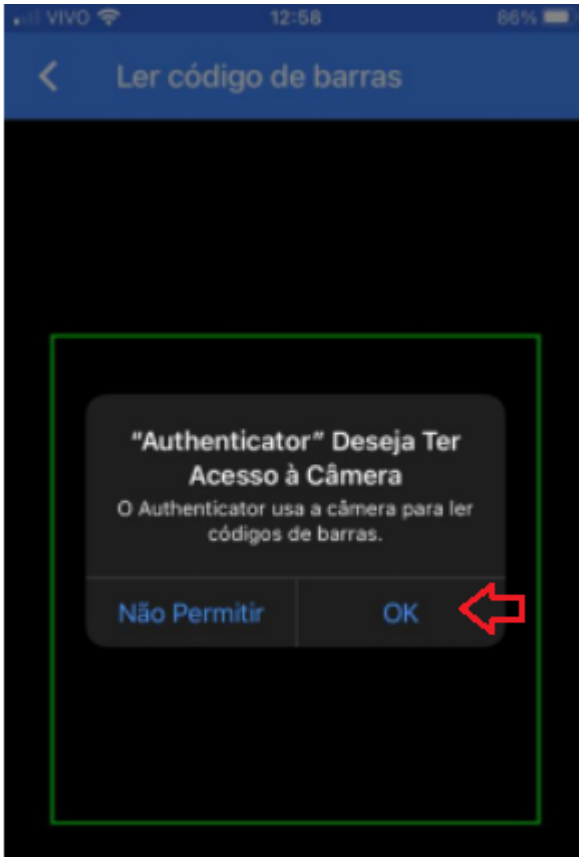


10. Clicar em "Ler código de barras".



OBS: O aplicativo pode pedir permissão para acessar a câmera do smartphone.

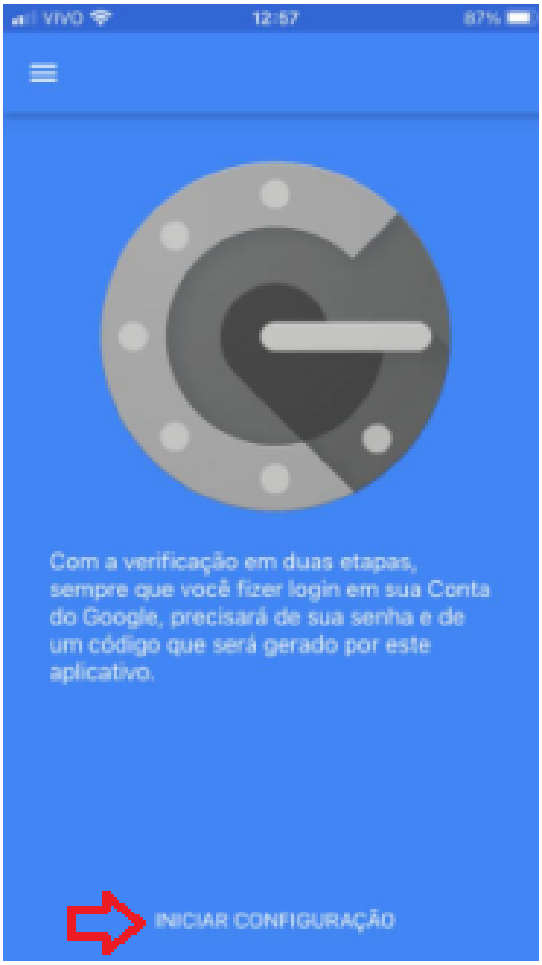
11. Clicar em "Ok".



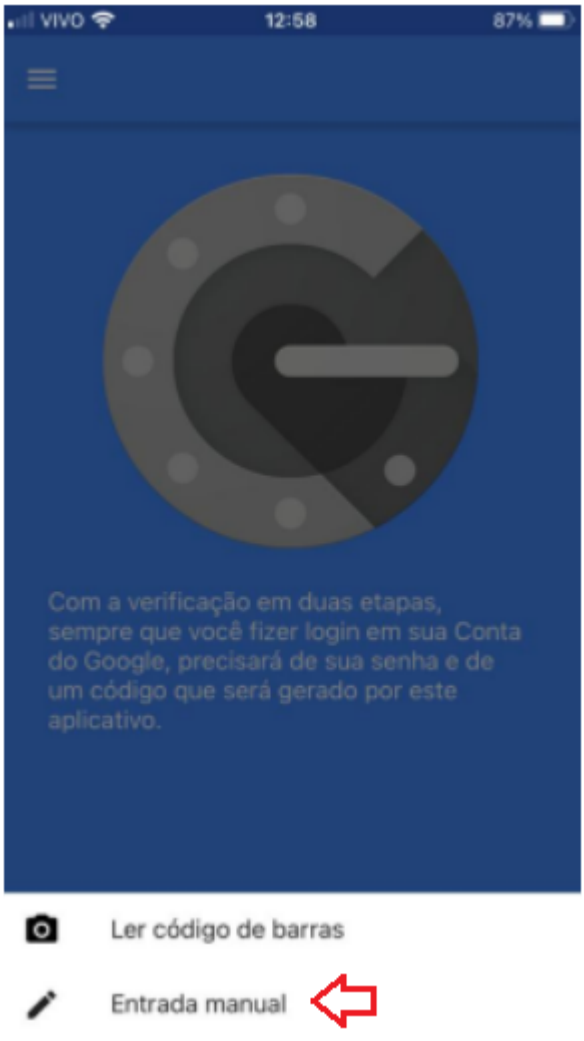
12. Apontar a câmera do smartphone para o código QRCode na tela e adicionar a conta no aplicativo.

OBS: Caso não consiga realizar a leitura do código QrCode, realizar a configuração de forma manual.

13. Clicar em "Iniciar configuração".



14. Clicar em "Entrada manual".

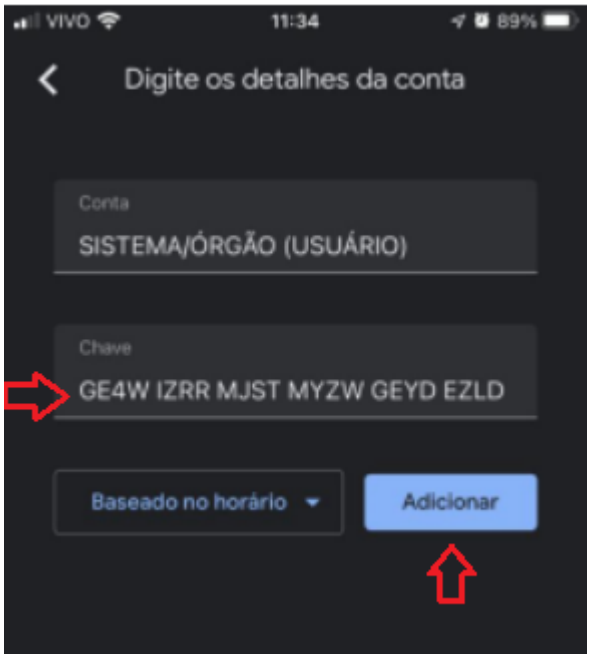


15. Clicar no código alfanumérico exibido abaixo do código QR e copiá-lo.



16. Colar no aplicativo de autenticação.

17. Clicar em "Adicionar".



18. Informar um endereço de email que não seja associado com a instituição.

OBS: A senha do email deve ser diferente da senha de acesso ao sistema.

19. Clicar em "Enviar".

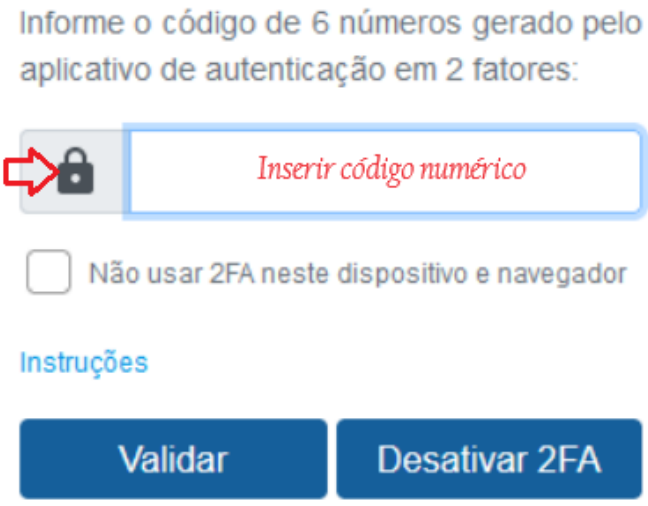


OBS: Somente após receber o e-mail e clicar no link, o mecanismo de autenticação em 2 fatores estará ativado.

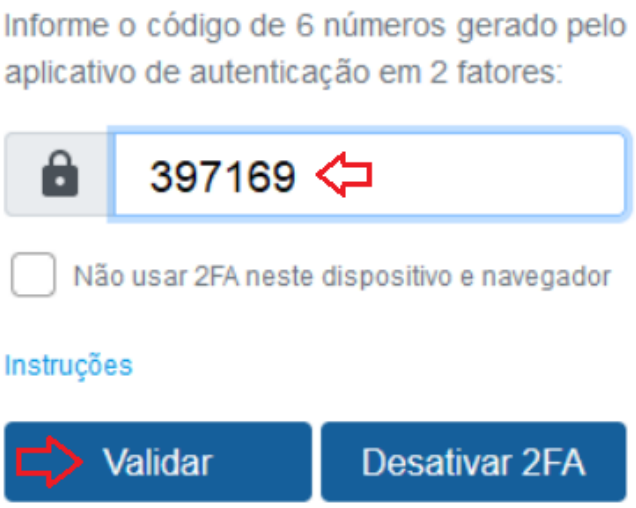
20. Informar usuário e senha.

21. Informar o código numérico.

22. Abrir o aplicativo de autenticação no seu smartphone e ver o código gerado.







OBS: De agora em diante, sempre que fizer login, será preciso consultar o seu smartphone, porque o código muda a cada 30 segundos.

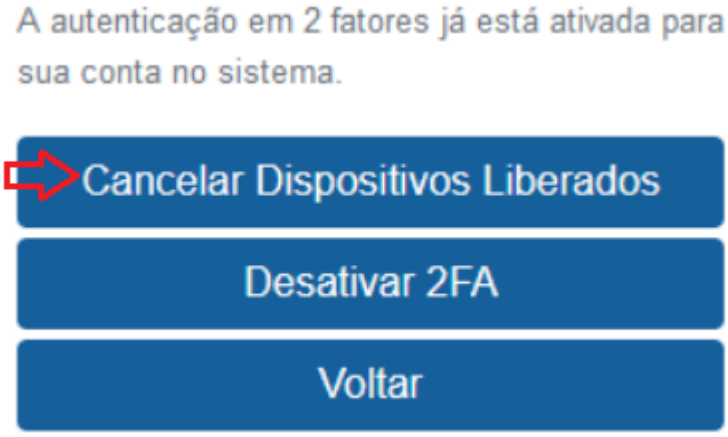
Liberando Dispositivos

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.

Cancelando Dispositivos Liberados

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".



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 que foi fornecido no momento da leitura do código QR. Somente após receber o e-mail e clicar no link é que o mecanismo de autenticação em 2 fatores será desativado.

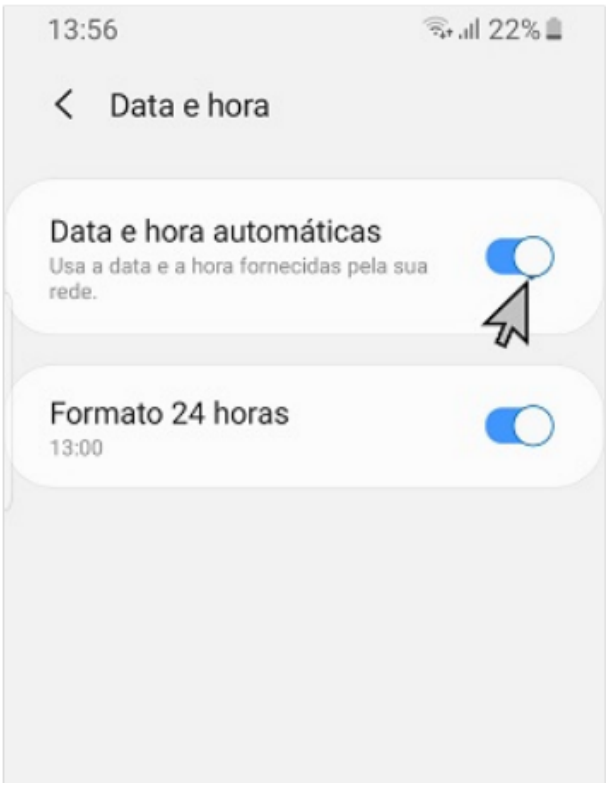
Solução de problemas

Caso esteja recebendo a mensagem "Código inválido." ou "Código não reconhecido.", é possível que o horário no seu smartphone esteja desatualizado.

1. Verificar se o aparelho está configurado para obter a hora automaticamente pela rede.

Seguir exemplos de como fazer isso em diferentes sistemas.



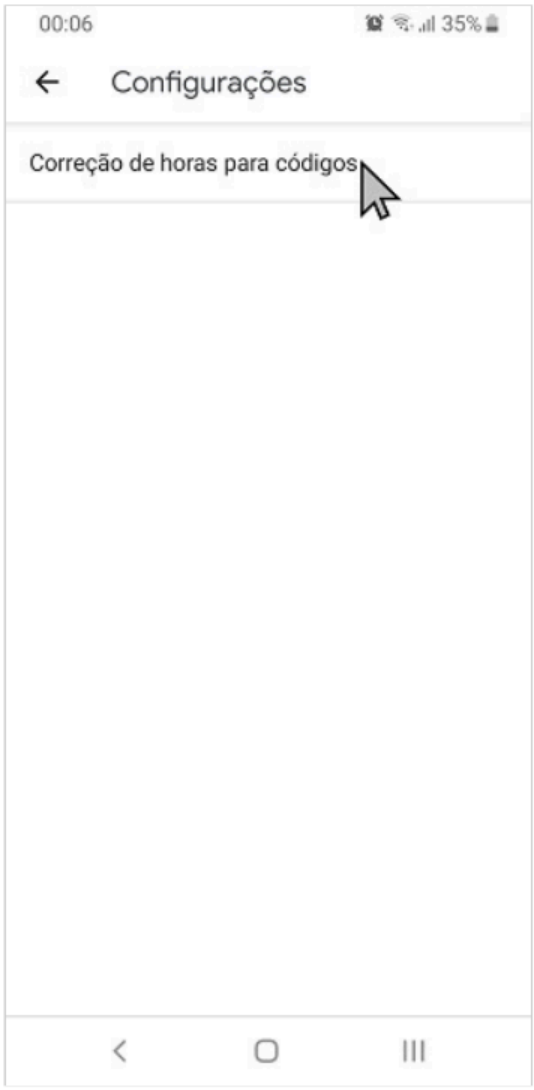


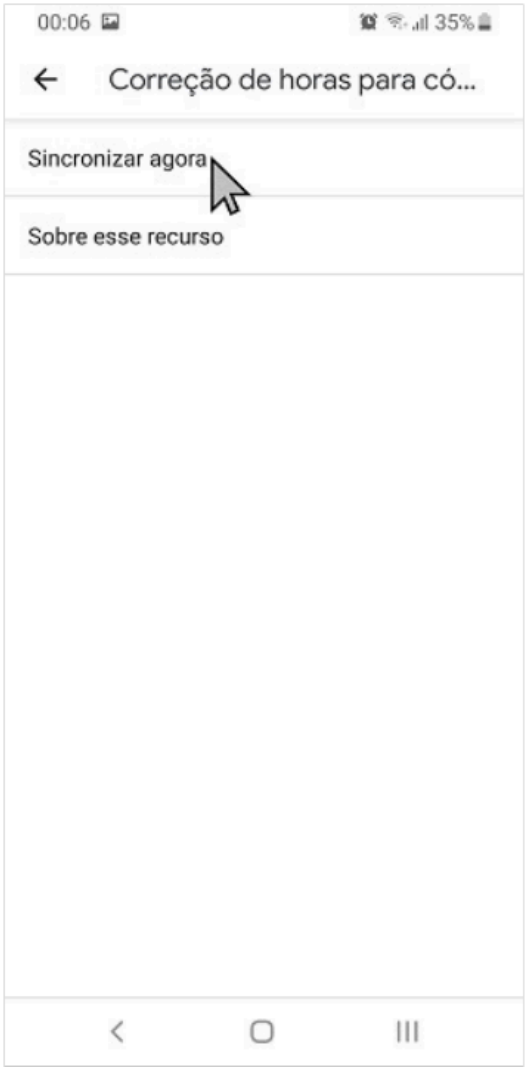




OBS: Apenas em dispositivos Android, é necessário seguir os passos abaixo para sincronizar o horário no Google Authenticator.


00:06
35%
Google Authenticator
Configurações
Sistema/Órgão (Sigla)
464 614


00:06
35%
Configurações
Correção de horas para códigos



Procedimento a ser executado pelo Suporte Local:

1. Não se aplica.

Procedimento a ser executado por outros Grupos Solucionadores:

1. Realiza reset de senha.

Palavras para pesquisa:

#SEI #Autenticação #2FA #fatores

Referências:
COSTA, F. - Stefanini **[N1] SEI - Autenticação em 2 Fatores**. Rio de Janeiro: BASE2R, 2024.

Autor: Fernanda Gonçalves da Costa
Criado em 29-07-2024 12:15
Última atualização em 30-10-2024 13:02

309 vistas
Este item não é parte da FAQ