SOE
Organização
E-mail
Documento
Certificado
Entrar
Dificuldades no acesso?
SOE
PROCERGS - Controle de Acesso e Segurança
Versão: 1.1.0 - 05/08/2020 00:23:00

Versão 07

SOE – Controle de acesso e segurança

O SOE tem como principal objetivo permitir o controle de acesso a aplicações disponibilizadas no ambiente Web pela PROCERGS.
O controle de acesso está baseado na criação de usuários e na definição de suas permissões em cada sistema.

2FA – Uma nova funcionalidade do SOE

O SOE está disponibilizando uma camada extra de segurança, o segundo fator de autenticação, também conhecido como 2FA.
Essa nova funcionalidade está disponível somente para sistemas que usam a nova interface de autenticação do SOE.

2FA - Segundo Fator de Autenticação

O que é 2FA ?

Autenticação por dois fatores adiciona uma camada extra de segurança quando você se autentica em um sistema usando o SOE.
Além de fornecer usuário e senha para acessar sua conta, é preciso inserir uma nova informação para confirmar que é você, de fato, que está se autenticando.

Por que usar o 2FA ?

Se você usar o 2FA, mesmo que uma pessoa tenha conhecimento da sua senha, ela não será capaz de acessar sua conta em um sistema que exige o 2FA. Isso porque o acesso completo depende de informação que só você tem.

Quando usar?

O 2FA pode ser configurado para um sistema, ou seja, todos os usuários obrigatoriamente terão que usar o 2FA ao acessar a aplicação ou pode ser uma opção do usuário.

2FA - Segundo Fator de Autenticação

O que eu preciso para usar o 2FA ?

- Um smartphone.
- Um aplicativo para gerar os códigos de verificação do 2FA, instalado no smartphone. Existem vários aplicativos que geram esses códigos, como por exemplo o Google Authenticator, que está disponível nas lojas da Apple e do Android. Habilitar o uso do 2FA usando as interfaces do SOE.
- Um e-mail cadastrado no SOE que será usado, caso seja necessário para redefinir o 2FA.

Como habilitar o 2FA?

O 2FA pode ser habilitado:

- Após a autenticação com usuário e senha, para sistemas que exigem o 2FA.
- Na interface “Meus Dados” das aplicações, geralmente um ícone disponível no menu superior à direita.

2FA – Boas práticas

Boas práticas

- Você pode fazer backup do aplicativo de geração de código do 2FA para recuperar a associação com o SOE, caso seja feita uma reinstalação do aplicativo no seu smartphone.

- Configurar para usar o 2FA em todos os sistemas que se autenticam usando o SOE, para aumentar o nível de segurança dificultando o acesso caso alguém descubra a sua senha.

- Para o aplicativo gerador dos códigos do 2FA funcionar corretamente ele precisa estar com a data/hora sincronizada corretamente. Por isso, é aconselhável configurar no smartphone a sincronização automática da data/hora. Alguns aplicativos disponibilizam a opção para sincronizar a data/hora, por exemplo no Google Authenticator(smartphone com sistema operacional Android) e está disponível no menu Configurações/Correção de horas para códigos/Sincronizar agora.

- Um usuário SOE(organização/matrícula) só pode ter uma habilitação com um aplicativo gerador de códigos do 2FA instalado no smartphone. *A habilitação válida será sempre a última realizada,* caso uma nova habilitação seja feita, é uma boa prática excluir as antigas do aplicativo 2FA.

Como faço para utilizar o 2FA ?

Vamos demonstrar o passo a passo como habilitar o uso do 2FA acessando uma aplicação *web* da PROCERGS. A aplicação precisa estar configurada para exigir o 2FA.

Antes de iniciar a habilitação, o aplicativo gerador de códigos de verificação do 2FA precisa estar instalado no seu smartphone.

Ao acessar você receberá a tela de autenticação do SOE.

1. Informe a sua identificação: usuário e senha. Alguns sistemas não apresentam todas as opções de identificação, por exemplo: um sistema pode ter apenas as abas de Documento e Certificado.

2. Após essas informações clique em **Entrar.**

Habilitando o 2FA

3. Será mostrado um aviso para utilizar o segundo fator de autenticação para poder completar a autenticação.

4. Essa interface vem preenchida com alguns dos seus dados que estão cadastrados no SOE.

5. Clique em **Habilitar**.

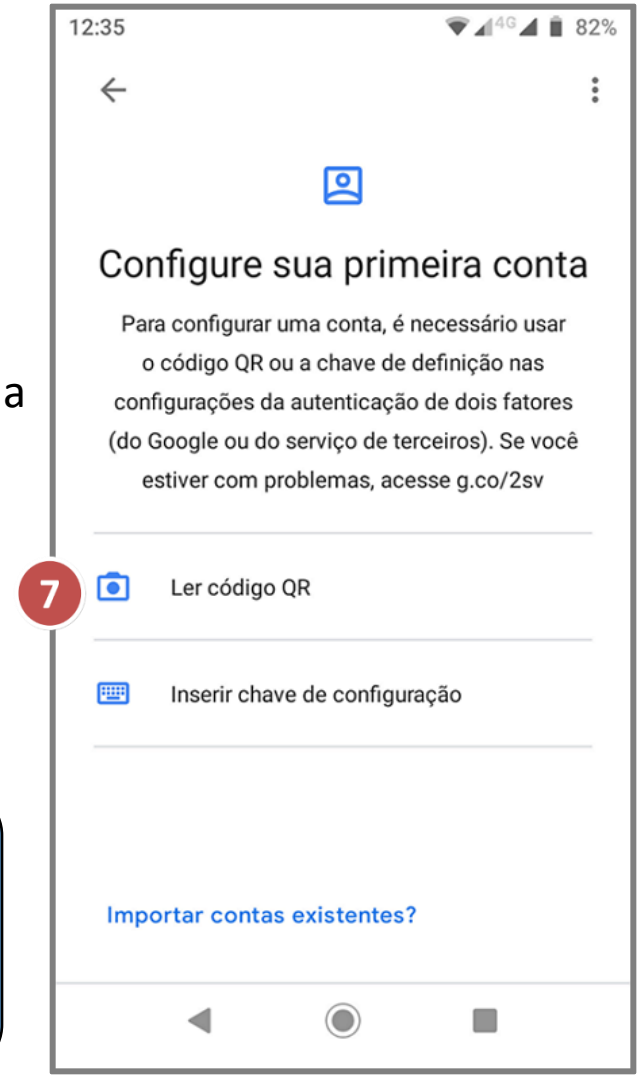
A habilitação associa o aplicativo 2FA instalado no smartphone com o seu usuário SOE(organização/matrícula) e os códigos gerados são usados em todos os sistemas que solicitarem o código de verificação do 2FA do SOE.
Nova habilitação é necessária se o usuário desinstalar o aplicativo do celular, trocar de celular ou desabilitar o 2FA do SOE.

Habilitando o 2FA

Neste momento você precisa estar com seu smartphone em mãos.

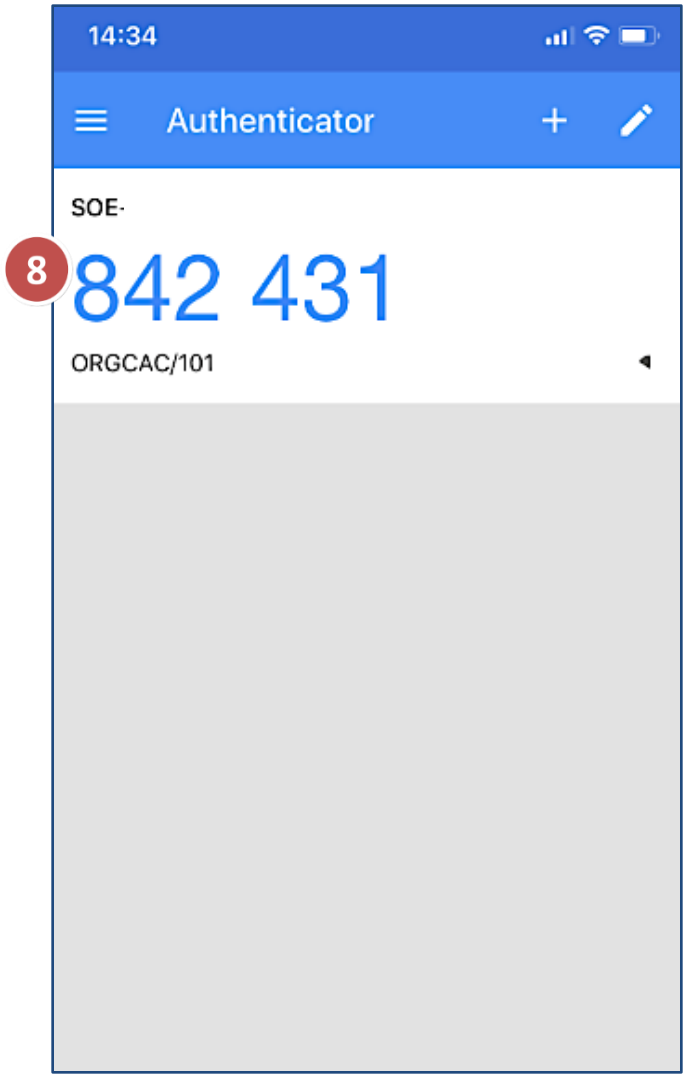
6. Leia o QRCode com o aplicativo gerador de código de verificação instalado no smartphone. Para isso, aponte a câmera fotográfica para a imagem QRCode que aparece na interface do SOE.

7. Na tela do aplicativo clique em **Ler código QR.**



A partir deste momento o aplicativo vai gerar os códigos de verificação do 2FA que são solicitados pelo SOE. Os códigos gerados pelo aplicativo mudam a cada 30 segundos

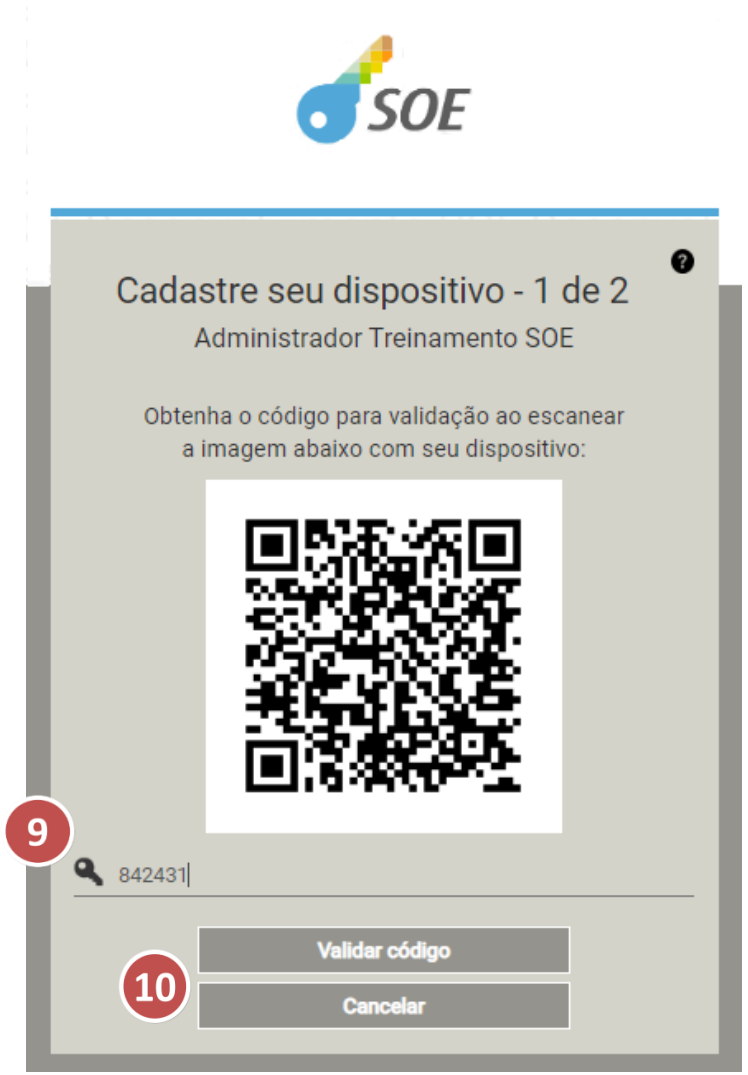
Habilitando o 2FA



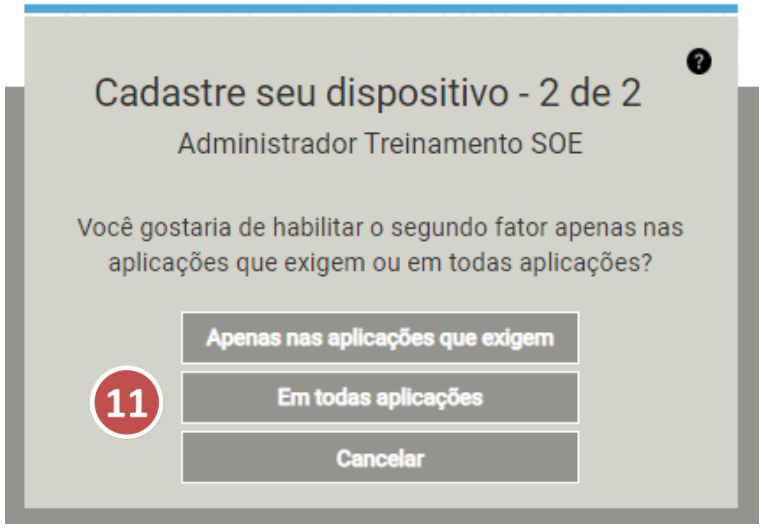
8. O aplicativo instalado no seu smartphone vai gerar um código de verificação do 2FA. A cada 30 segundos é gerado um novo código.

9. Na interface do SOE informe o código no campo onde tem a chave.

10. Clique em **Validar código**.



Habilitando o 2FA



11. Defina quando usar o 2FA: para aplicações que exigem ou para todas aplicações.

Pronto! Você habilitou o 2FA.

12. Clique em **Acessar aplicação** e você já estará acessando seu sistema.

A habilitação feita ao ler o QRCode pelo aplicativo do 2FA instalado no seu smartphone é feita só uma vez, ela é a ligação do usuário SOE(organização/matrícula) com a funcionalidade do 2FA do SOE.

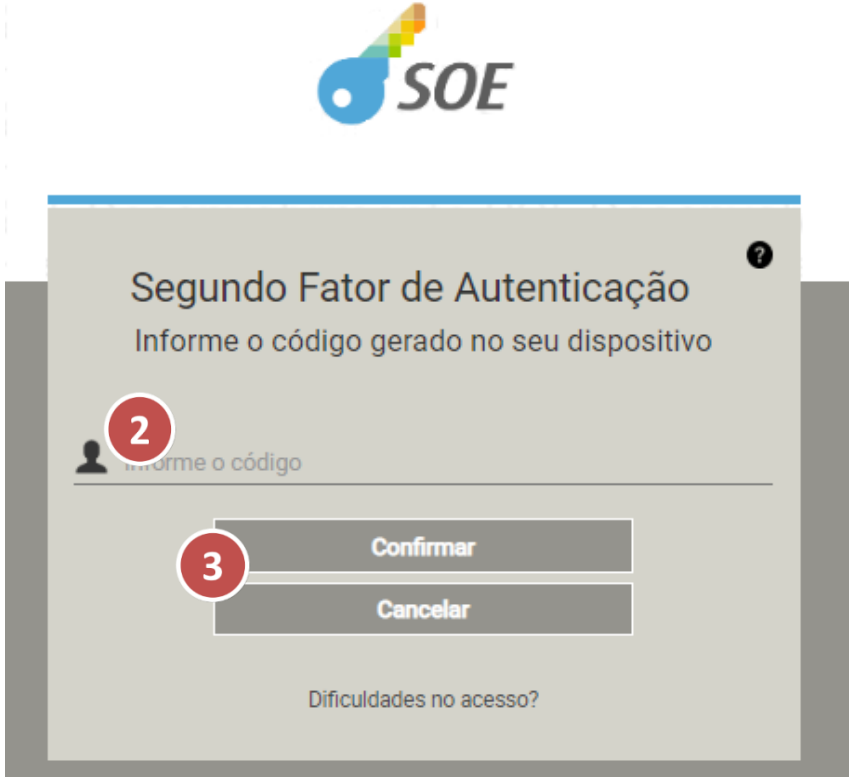
Acessando a aplicação com 2FA

Depois de ter habilitado o 2FA, para acessar o sistema nas próximas vezes:

1. Faça a autenticação com seu usuário e senha.

2. Informe o código de verificação mostrado no aplicativo de geração de código do seu smartphone.

3. Clique em **Confirmar**.



Configurando os seus dados

Você pode consultar e configurar os seus dados pela interface “Meus Dados” disponível nos sistemas.

A imagem ao lado é de um sistema após você ter feito a autenticação.

1. Clique na opção de **alteração de Senha** (ícone do cadeado) para abrir a interface “Meus Dados".

O ícone desta opção pode ser diferente nos sistemas ou não estar disponível.

Configurando os seus dados

A interface "Meus Dados" também está disponível no aplicativo SOE. Esta interface está disponível para todos os usuários cadastrados no SOE, mesmo os que não estão autorizados no sistema SOE.

Endereço do aplicativo do SOE: https://www.soe.rs.gov.br

Consultando os seus dados

1. Clique aqui para mostrar seus dados

2. Serão mostrados alguns dos seus dados cadastrados no SOE.

Alterando sua senha

1. Abre a interface de alteração da sua senha.

2. Informe sua senha atual, a nova senha e a confirmação da nova senha.

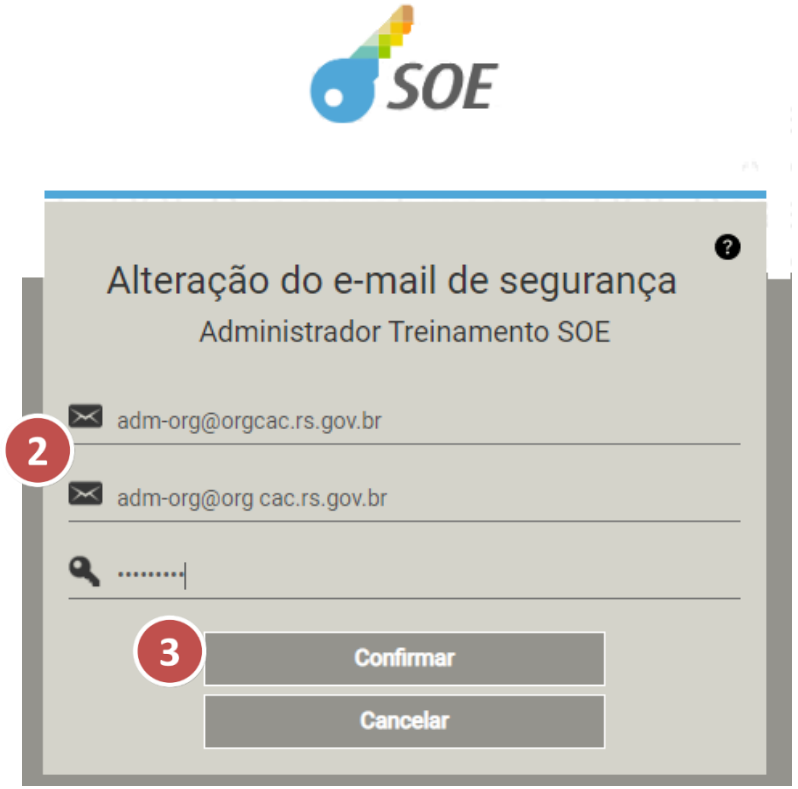
3. Clique no **Confirmar** para alterar a sua senha.

Alterando seu e-mail de segurança

1. Abre a interface para alterar o seu e-mail de segurança.

2. Informe seu e-mail e a confirmação do seu e-mail.

3. Clique no **Confirmar** para alterar o seu e-mail.



Habilitando o 2FA

1. Você também pode optar por habilitar o 2FA na interface "Meus dados" ao clicar no **Habilitar**.

O passo a passo é o mesmo mostrado anteriormente para habilitar quando um sistema exige o 2FA.

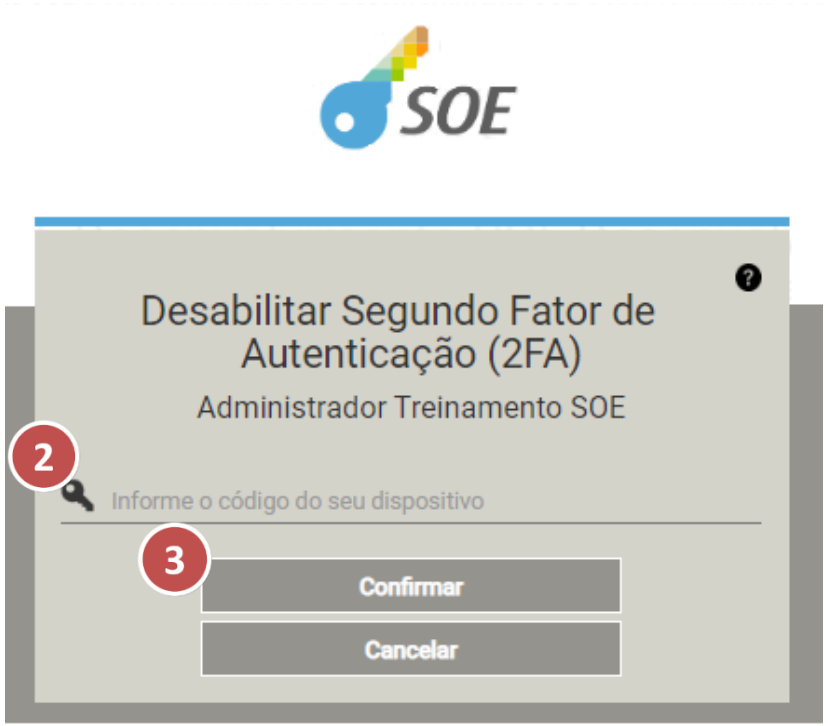
Desabilitando o 2FA

Na interface “Meus Dados” você pode desabilitar o 2FA.

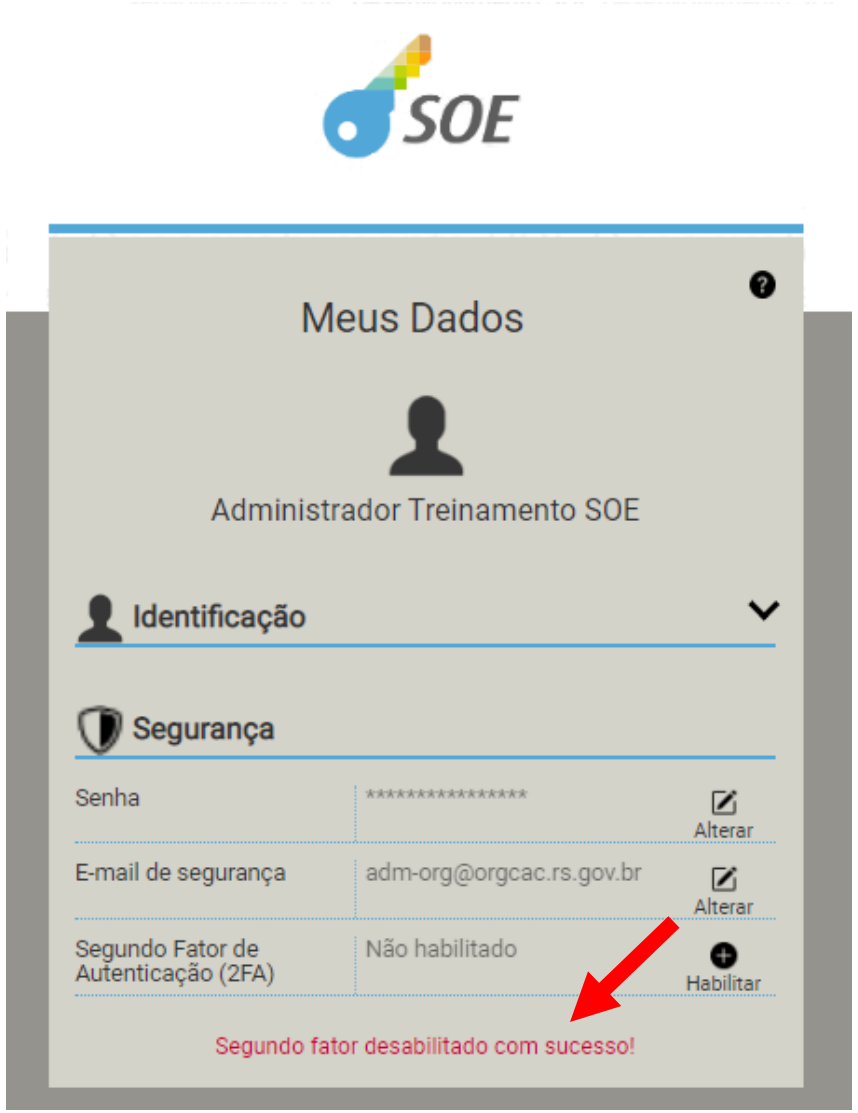
1. Para desabilitar clique em **Desabilitar**.

2. Digite o código de autenticação gerado por seu autenticador.

3. Clique em **Confirmar**.

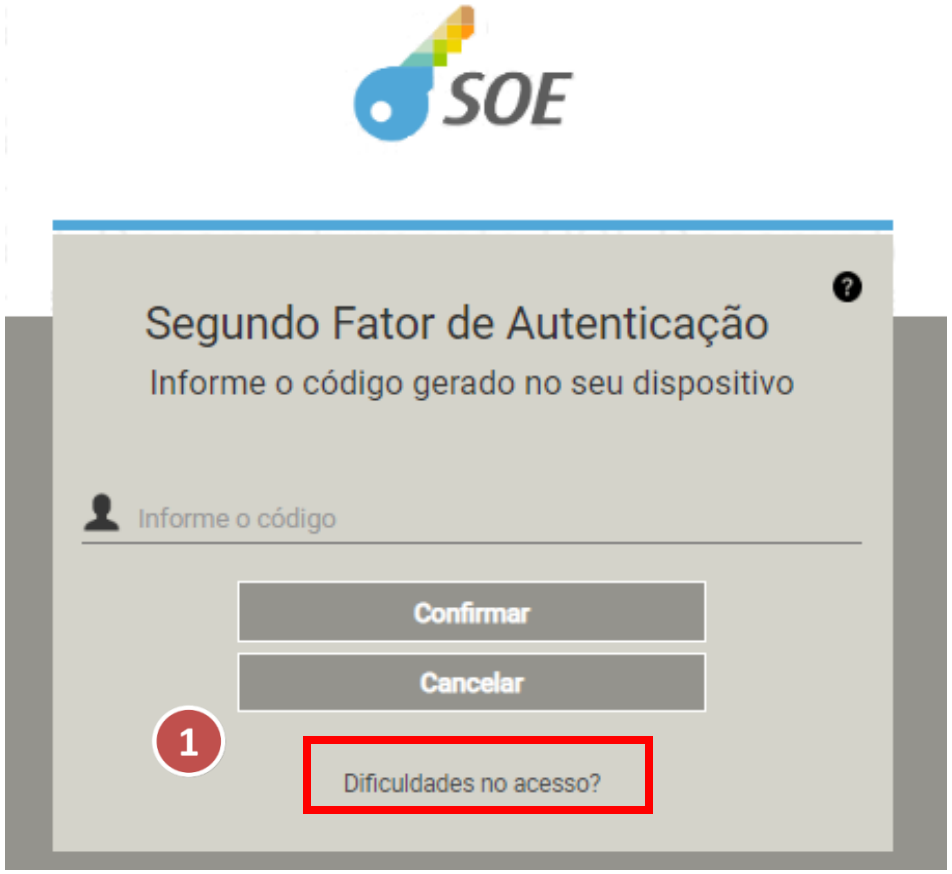


Desabilitando o 2FA



O 2FA está desabilitado. Caso um sistema exija o 2FA será necessário fazer a habilitação novamente.

O que fazer se perder ou trocar de celular?



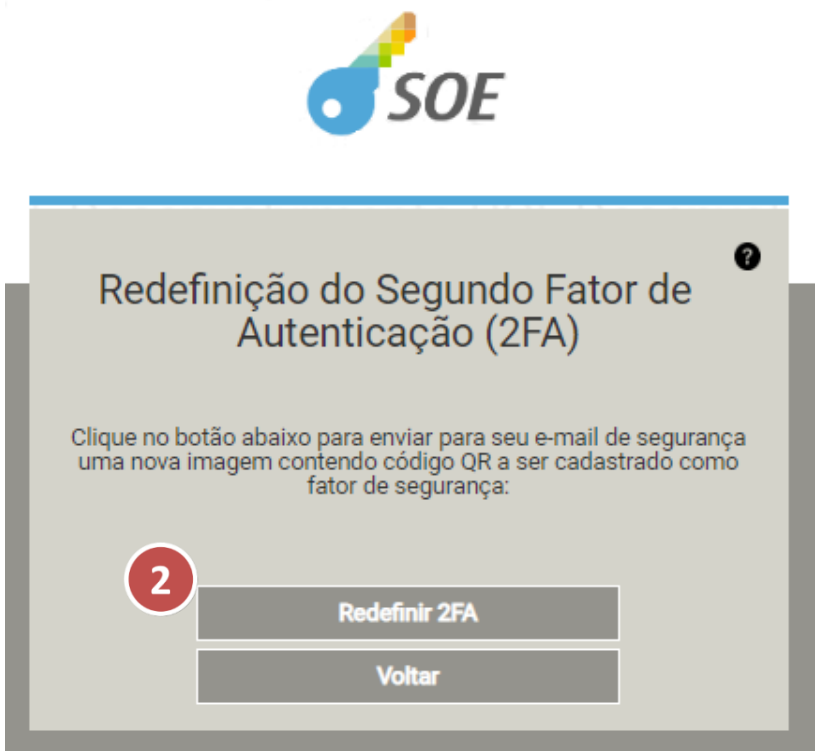
Se o aplicativo de geração de códigos para o 2FA tem backup, ao reinstalar o aplicativo no smartphone os dados do SOE serão recuperados.

Se o aplicativo do 2FA não tem backup, existe a opção de redefinir o 2FA.

Esta opção está disponível na tela de autenticação do SOE.

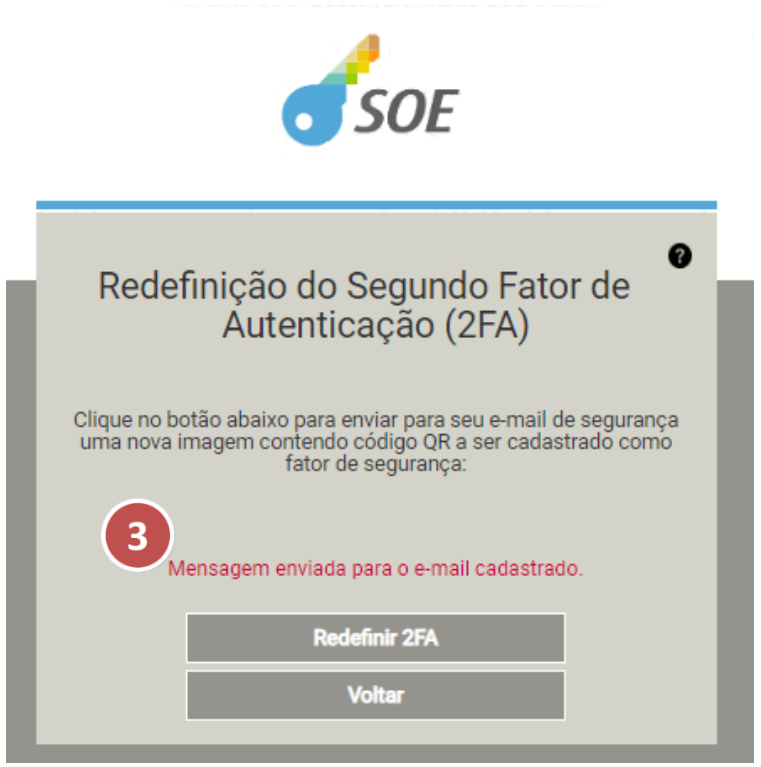
1. Após se autenticar com usuário e senha clique em **Dificuldades no acesso?**

O que fazer se perder ou trocar de celular?

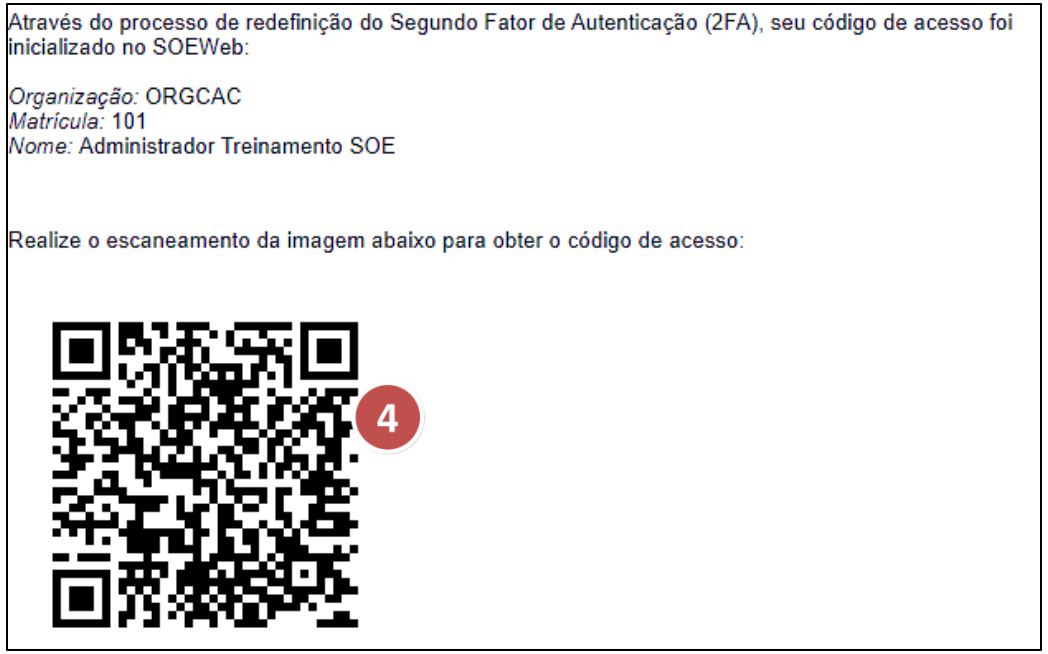


2. Clique em **Redefinir 2FA**.

3. Será enviado um novo QRCode, para o seu e-mail do SOE, para associar novamente o aplicativo do 2FA com o seu usuário do SOE.



O que fazer se perder ou trocar de celular?

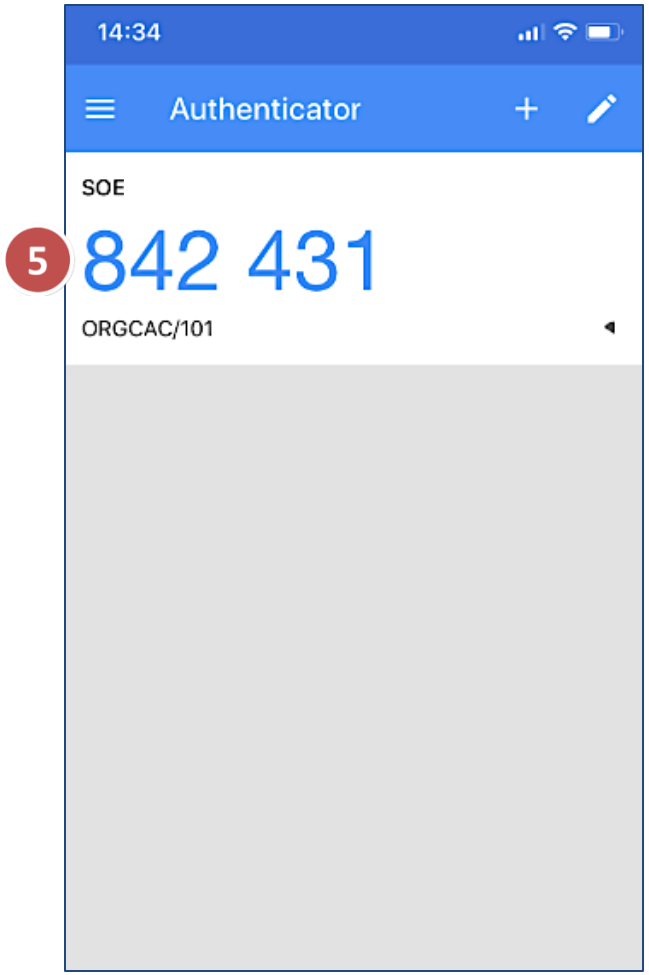

Através do processo de redefinição do Segundo Fator de Autenticação (2FA), seu código de acesso foi inicializado no SOEWeb:

Organização: ORGCAC
Matrícula: 101
Nome: Administrador Treinamento SOE

Realize o escaneamento da imagem abaixo para obter o código de acesso:

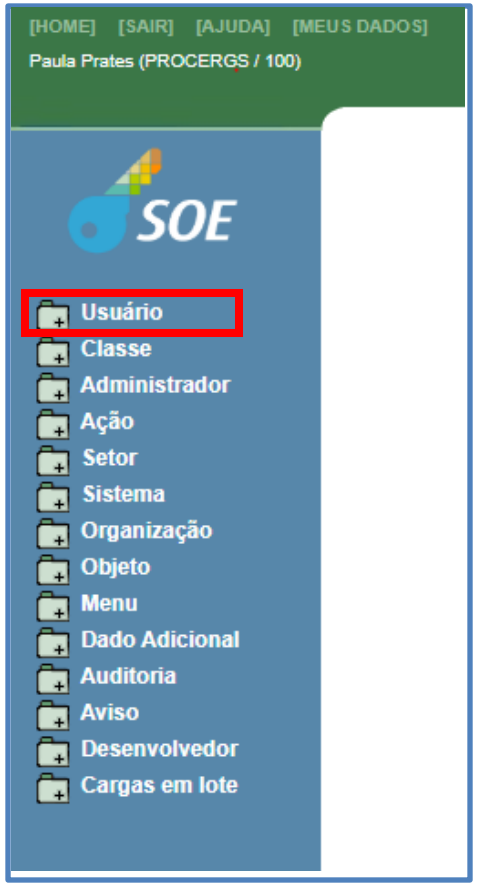
4. Com a mensagem recebida por e-mail leia o QRCode com o aplicativo de geração de código do 2FA, instalado no seu celular, para fazer uma nova associação com o SOE.

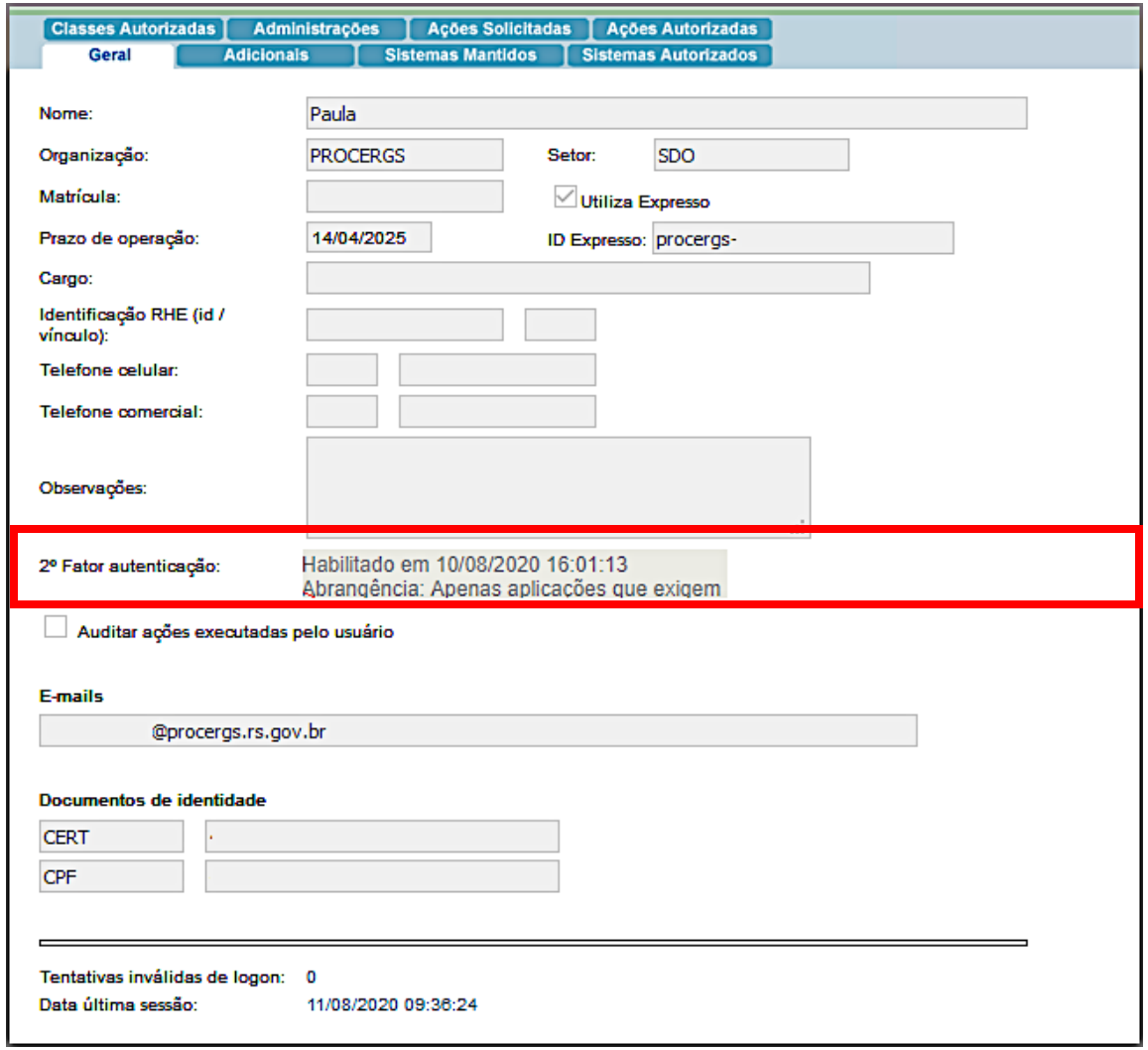
5. Agora você está novamente habilitado!



Como saber se um usuário está usando o 2FA?

No aplicativo SOE, ao consultar um usuário, os administradores podem visualizar se foi habilitado o 2º Fator de Autenticação e qual o tipo de abrangência escolhido.





Mais informações sobre o 2FA

No aplicativo do SOE também tem o menu 2FA com as seguintes opções:

- Totais por org: mostra os totais por organização de usuários com o 2FA habilitado. É possível pesquisar usuários que usam um sistema ou que estão ligados em uma determinada classe ou ação.
- Lista usuários: lista os usuários de uma organização com o 2FA habilitado. Além da organização, pode ser informado como critério o tipo de abrangência do 2FA ou se ele usa o sistema.
- Desabilitar: está funcionalidade permite que um administrador da organização desabilite o 2FA de um usuário. Além do administrador da organização, usuários autorizados nas ações SOE-USUARIO2FA-DESABILITARORG e SOE-USUARIO2FA-DESABILITARSETOR também podem desabilitar o 2FA para usuários da sua organização ou setor.
- Auditoria: permite consultar as ações relacionadas ao 2FA que foram executadas por um usuário ou pelo responsável pela desabilitação do 2FA de um usuário.