



Organização

E-mail

Documento

Certificado



Entrar

[Esqueci minha senha](#)

Versão 11– atualizado em 24/11/2025

SOE – Controle de acesso e segurança

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



Organização E-mail Documento Certificado


[Esqueci minha senha](#)


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.



Organização E-mail Documento Certificado

 orgcac

 101



Entrar

[Esqueci minha senha](#)

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 ou Microsoft Authenticator, que está disponível nas lojas da Apple e do Android.
- Habilitar o uso do 2FA usando as interfaces do SOE.
- Um e-mail de segurança cadastrado no SOE que será usado, caso seja necessário, para configurar o 2FA.
- O e-mail pode ser cadastrado:
 - Na habilitação do 2FA.
 - Na interface *Meus Dados* das aplicações, geralmente um ícone disponível no menu superior à direita.

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 para habilitar o uso do 2FA acessando uma aplicação *web* da PROCERGS. A **aplicação** precisa estar configurada para **exigir o 2FA**. Também é possível habilitar o 2FA pela interface *Meus Dados*.



Organização E-mail Documento Certificado

orgcac

1 101

.....

2 Entrar

Esqueci minha senha

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

Ao acessar o sistema, você receberá a tela de autenticação do SOE.

1. Informe a sua identificação: usuário e senha. Eventualmente, alguns sistemas não apresentam todas as opções de identificação, podendo ter, por exemplo, apenas as abas de Documento e Certificado.

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

Como faço para utilizar o 2FA ?

SOE

Meus Dados

Administrador Treinamento SOE

Identificação

Segurança

Senha: *****

E-mail de segurança: Não cadastrado

Segundo Fator de Autenticação (2FA): Não habilitado **4**

3 O acesso à esta aplicação requer a habilitação do Segundo Fator de Autenticação (2FA). Clique em Habilitar.

Cancelar

3. Será solicitada a habilitação do 2FA.

4. Clique em **Habilitar**.

Nas próximas páginas tem a explicação de como habilitar o 2FA.

Habilitando o 2FA



Cadastre seu dispositivo - 1 de 2

Administrador Treinamento

Use um **aplicativo autenticador** (como Google Authenticator ou Microsoft Authenticator), instalado no seu **smartphone**, para escanear a imagem abaixo. Em seguida, digite o código exibido no aplicativo.



1

Caso não possa escanear a imagem QR acima, clique na chave de configuração abaixo ou copie seu valor e a utilize em seu aplicativo de leitura de autenticação:

[HCNS26FGX2XA](#)

Informe o código para validação

Validar código

Cancelar

Neste momento você precisa estar com seu smartphone em mãos.

1. 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.


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

Se não for possível ler o código QR, copie a chave de configuração que aparece abaixo do código QR e insira no aplicativo.

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.

12:35 4G 82%

←



Configure sua primeira conta

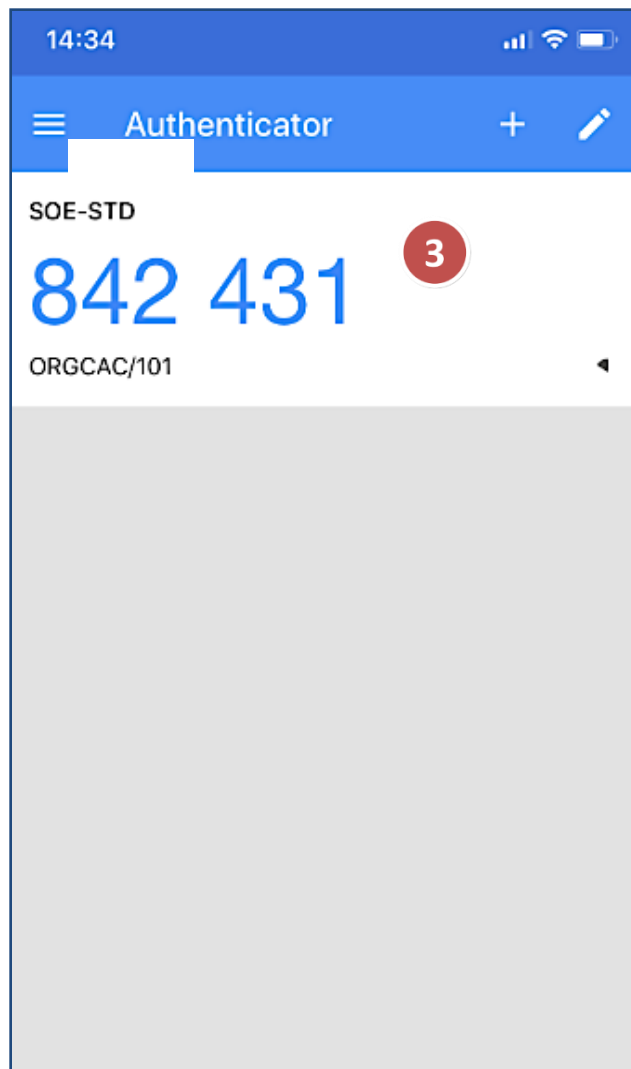
Para configurar uma conta, é necessário usar o código QR ou a chave de definição nas configurações da autenticação de dois fatores (do Google ou do serviço de terceiros). Se você estiver com problemas, acesse g.co/2sv

Ler código QR 2

Inserir chave de configuração

[Importar contas existentes?](#)

Habilitando o 2FA



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

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

5. Clique em **Validar código**.



Habilitando o 2FA



Cadastre seu dispositivo - 2 de 2
Administrador Treinamento SOE

Você gostaria de habilitar o segundo fator apenas nas aplicações que o exigem ou em todas as aplicações?

6

Apenas nas aplicações que o exigem

Em todas as aplicações

Cancelar

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

Pronto! Você habilitou o 2FA.

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

Se o usuário não possuir e-mail de segurança cadastrado, aparece mensagem informando da necessidade para recuperação da senha e redefinição do 2FA. O e-mail de segurança pode ser cadastrado aqui, clicando em Incluir ou, posteriormente, pela interface do Meus Dados.

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.



Meus Dados

Administrador Treinamento SOE

Identificação

Segurança

Senha	*****	Alterar
E-mail de segurança	Não cadastrado	Incluir
Segundo Fator de Autenticação (2FA)	Habilitado	Desabilitar
- Tipo de Abrangência	Apenas nas aplicações que exigem	Alterar

Segundo fator habilitado com sucesso!

Para recuperação da senha e redefinição do 2FA, é necessário ter o e-mail de segurança cadastrado.

Acessar aplicação

7

Acessando a aplicação com 2FA



Organização E-mail Documento Certificado

orgcac

101

.....

1

Entrar

Esqueci minha senha

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

- 1.** Faça a autenticação com seu usuário e senha.
- 2.** Será solicitado o código de verificação do 2FA.



Segundo Fator de Autenticação ?

Informe o código gerado no seu dispositivo

Informe o código **2**

Confiar neste dispositivo?

Confirmar

Cancelar

Confiando no dispositivo

A screenshot of the SOE authentication interface. At the top, it says 'Segundo Fator de Autenticação' and 'Informe o código gerado no seu dispositivo'. Below this, there is a user icon and the number '123456'. A red circle with the number '1' is placed over the user information. Below the user information, there is a checkbox labeled 'Confiar neste dispositivo?' with a red circle containing the number '2' next to it. At the bottom, there are two buttons: 'Confirmar' and 'Cancelar', with a red circle containing the number '3' next to the 'Confirmar' button.

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

2. Ao marcar a opção de *Confiar neste dispositivo*, o código do 2FA não será solicitado no próximo logon. Por segurança, sua organização define um tempo de confiança, após o qual o código será solicitado novamente.

Se não marcar em confiar, o código sempre será solicitado no logon.

3. Clique em **Confirmar**.

Não é recomendado usar esta funcionalidade em dispositivos que são compartilhados com outros usuários.

Deixando de confiar no dispositivo



Na interface *Meus Dados* você pode deixar de confiar no dispositivo.

1. Clicar no botão **Deixar de confiar neste dispositivo**. Assim, o código do 2FA será solicitado no próximo logon.

Outras maneiras de deixar de confiar no dispositivo são limpando o cache do navegador ou se outro usuário usar o 2FA no mesmo dispositivo.

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.

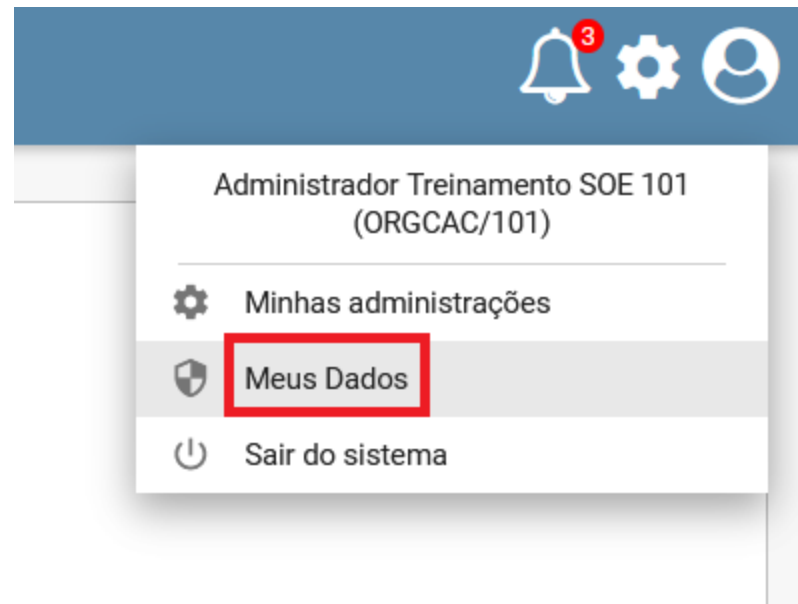
1. Clique na opção de **alteração de Senha** (ícone do cadeado) para abrir a interface *Meus Dados*.

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.

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



Consultando os seus dados



Meus Dados



Administrador Treinamento SOE

Identificação

Segurança

Senha	*****	Alterar
E-mail de segurança	suzanak@procergs.rs.gov.br	Alterar
Segundo Fator de Autenticação (2FA)	Habilitado	Desabilitar
- Tipo de Abrangência	Apenas nas aplicações que exigem	Alterar

Fechar

1. Clique aqui para mostrar seus dados

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



Meus Dados



Administrador Treinamento SOE

Identificação

Organização	ORGCAC
Setor	CAC
Matrícula	103
Prazo de Operação	22/02/2022
E-mails corporativos	
Documentos	

Segurança

Senha	*****	Alterar
E-mail de segurança	suzanak@procergs.rs.gov.br	Alterar
Segundo Fator de Autenticação (2FA)	Habilitado	Desabilitar
- Tipo de Abrangência	Apenas nas aplicações que exigem	Alterar

Fechar

Alterando sua senha



Meus Dados



Administrador Treinamento SOE

Identificação

Segurança

Senha	*****	Alterar
E-mail de segurança	suzanak@procergs.rs.gov.br	Alterar
Segundo Fator de Autenticação (2FA)	Habilitado	Desabilitar
- Tipo de Abrangência	Apenas nas aplicações que exigem	Alterar

Fechar

1. Abra 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.



Alteração de senha

Administrador Treinamento SOE

Senha atual

Nova senha

Confirmação nova senha

Confirmar

Cancelar

Alterando/cadastrando seu e-mail de segurança



Meus Dados

Administrador Treinamento SOE

Identificação

Segurança

Senha	*****	Alterar
E-mail de segurança	suzanak@procergs.rs.gov.br	Alterar
Segundo Fator de Autenticação (2FA)	Habilitado	Desabilitar
- Tipo de Abrangência	Apenas nas aplicações que exigem	Alterar

Fechar

1

1. Abra a interface para alterar ou
2. Incluir seu e-mail de segurança.



Meus Dados

Administrador Treinamento SOE

Identificação

Segurança

Senha	*****	Alterar
E-mail de segurança	Não cadastrado	Incluir
Segundo Fator de Autenticação (2FA)	Habilitado	Desabilitar
- Tipo de Abrangência	Apenas nas aplicações que exigem	Alterar

Notamos que você não possui um e-mail de segurança cadastrado. Ele é utilizado caso você precise recuperar sua conta.

Fechar

2

Alterando/cadastrando seu e-mail de segurança



Alteração do e-mail de segurança - 1 de 2
Administrador Treinamento SOE

E-mail atual: Não cadastrado

1 Informe o novo e-mail de segurança

2 Confirme o novo e-mail de segurança

Senha

3 Confirmar

Cancelar

- Para cadastrar ou alterar o e-mail de segurança:
1. Informe e confirme o seu e-mail de segurança.
 2. Informe a sua senha do SOE.
 3. Clique em **Confirmar**.

4. Você receberá um código de validação no e-mail de segurança que está sendo cadastrado.

De: sistema-soe@procergs.rs.gov.br
Para: adm-org@procergs.rs.gov.br
Data: 16/11/2020 15:51 (agora)
Assunto: SOEWeb - Troca de e-mail de segurança - Confirmação - Desenvolvimento STD


Administrador, percebemos que você solicitou uma troca de e-mail no SOEWeb.

4 Esse é o seu código de confirmação:
04042203

Caso você não tenha solicitado essa troca, entre em contato com o Administrador da sua organização.

**** Mensagem enviada pelo sistema. Favor não responder. ****

Alterando/cadastrando seu e-mail de segurança



Alteração do e-mail de segurança - 2 de 2
Administrador Treinamento SOE

Para finalizar a troca do e-mail de segurança, preencha o campo abaixo com o código de confirmação recebido no novo e-mail:

5 04042203

Foi enviado um código de confirmação para o novo e-mail.

6 Confirmar código

Reenviar código

Cancelar

5. Informe o código recebido por e-mail.

6. Clique em **Confirmar código**.

7. Seu e-mail foi cadastrado/alterado com sucesso.



Meus Dados

Administrador Treinamento SOE

Identificação

Segurança

Senha	*****	Alterar
E-mail de segurança	suzanak@procergs.rs.gov.br	Alterar
Segundo Fator de Autenticação (2FA)	Habilitado	Desabilitar
- Tipo de Abrangência	Apenas nas aplicações que exigem	Alterar

E-mail de segurança salvo com sucesso!

7

Fechar

Habilitando o 2FA



Meus Dados

Administrador Treinamento SOE

Identificação

Segurança

Senha	*****	Alterar
E-mail de segurança	suzanak@procergs.rs.gov.br	Alterar
Segundo Fator de Autenticação (2FA)	Não habilitado	Habilitar

Que tal aumentar sua segurança? O Segundo Fator de Autenticação (2FA) já pode ser habilitado.

Fechar

1

1. Você também pode optar por habilitar o 2FA na interface “Meus Dados” ao clicar no **Habilitar**.

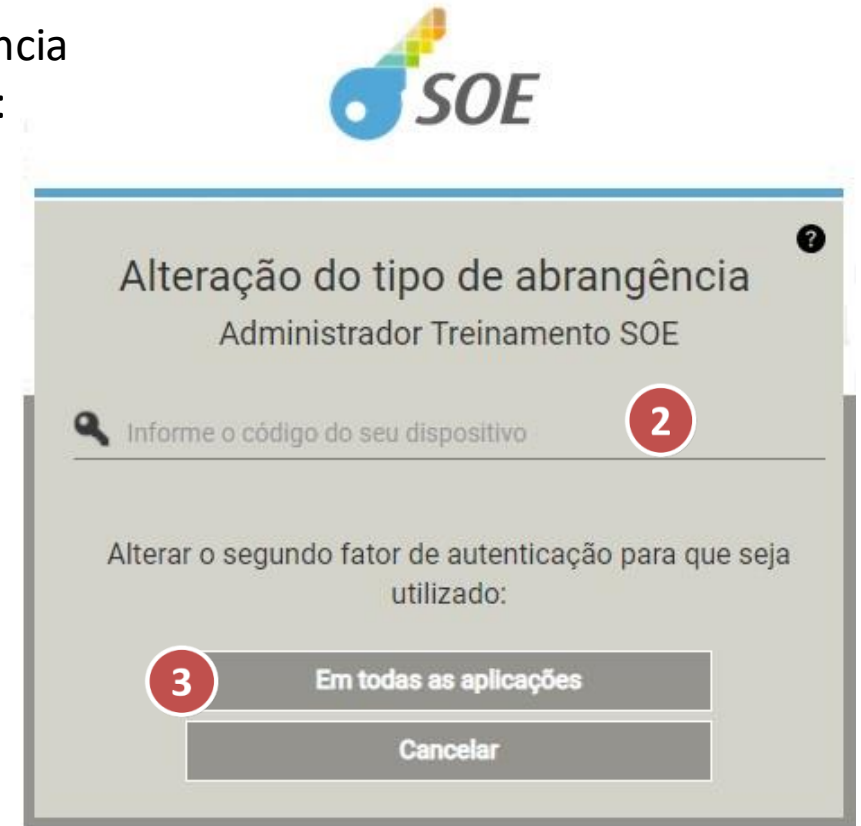
O passo a passo é o mesmo mostrado anteriormente para habilitar quando um sistema exige o 2FA.

Alterando a abrangência do 2FA



Você pode alterar o tipo de abrangência do 2FA pela interface “Meus Dados”:

1. Abre a interface de alteração do tipo de abrangência.
2. Informe o código de verificação mostrado no aplicativo de geração de código do seu smartphone.
3. Clique no botão que altera a abrangência.



Alterando a abrangência do 2FA



Meus Dados ?


Administrador Treinamento SOE

 Identificação ∨

 Segurança

Senha	*****	 Alterar
E-mail de segurança	suzanak@procergs.rs.gov.br	 Alterar
Segundo Fator de Autenticação (2FA)	Habilitado	 Desabilitar
- Tipo de Abrangência	Em todas as aplicações	 Alterar

Alteração de tipo de Abrangência realizada com sucesso!

Fechar

O tipo de abrangência está alterado. Conforme o tipo e a aplicação, o 2FA pode ser exigido na entrada da aplicação.

Desabilitando o 2FA

Meus Dados

Administrador Treinamento SOE

Identificação

Segurança

Senha	*****	Alterar
E-mail de segurança	suzanak@procergs.rs.gov.br	Alterar
Segundo Fator de Autenticação (2FA)	Habilitado	Desabilitar
- Tipo de Abrangência	Apenas nas aplicações que exigem	Alterar

Fechar

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**.

Desabilitar Segundo Fator de Autenticação (2FA)


Administrador Treinamento SOE

Informe o código do seu dispositivo

Confirmar

Cancelar

Desabilitando o 2FA



Meus Dados

Administrador Treinamento SOE

Identificação

Segurança

Senha	*****	Alterar
E-mail de segurança	suzanak@procergs.rs.gov.br	Alterar
Segundo Fator de Autenticação (2FA)	Não habilitado	Habilitar

Segundo fator desabilitado com sucesso!

Fechar

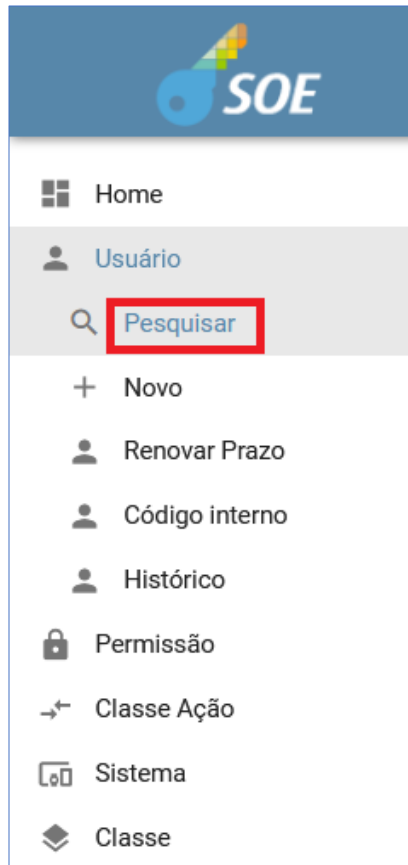
O 2FA está desabilitado. Caso um sistema exija o 2FA será necessário fazer a habilitação novamente.

O que fazer se perder ou trocar de celular?

- 1.** Solicite a **desabilitação** do seu 2FA para o **administrador da sua organização**.
- 2.** Após a desabilitação, habilite novamente o 2FA. O passo a passo é o mesmo mostrado anteriormente para habilitar quando um sistema exige o 2FA ou pela interface Meus Dados.

Como saber se um usuário está usando o 2FA?

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



A screenshot of the user profile page for 'Usuário Administrador Treinamento SOE'. The page shows various fields for user information, including Name, Organization, Matricula, Prazo de operação, and 2º Fator autenticação. The '2º Fator autenticação' field is highlighted with a red box, showing the date '11/02/2025 15:59:39' and the type 'Apenas aplicações que exigem'. There is also a checkbox for 'Auditar ações executadas pelo usuário' which is checked.

Usuário Administrador Treinamento SOE			
✓ Salvar ✕ Excluir 🔑 Inicializar senha 📅 Renovar prazo 📄 Copiar perfil ✕ Fechar ⌵ Outras informações			
Geral Dados de controle			
Nome *	Administrador Treinamento SOE		
Organização	ORGCAC	Setor *	CAC
Matricula *	101	Cargo	
Prazo de operação	01/02/2027	ID LDAP	orgcac-10111
Identificação RHE (id/vínculo)			
Telefone celular			
Telefone comercial			
Observações	640 caracteres restantes		
2º Fator autenticação	11/02/2025 15:59:39	Apenas aplicações que exigem	
<input checked="" type="checkbox"/> Auditar ações executadas pelo usuário			

Como configurar o tempo de confiança no dispositivo?

No aplicativo SOE, na edição da organização, os administradores podem definir por quanto tempo um dispositivo será considerado confiável, sem exigir nova autenticação via 2FA.

Prazo máximo de validade para usuários	720	dias
Prazo máximo de validade para senha	365	dias
Prazo de expiração por inatividade	90	dias
Quantidade de senhas não reutilizáveis	5	
Nro dias para mensagem expiração prazo	7	dias
Prazo de confiança do dispositivo(2FA) ?	14	dias

Ajuda

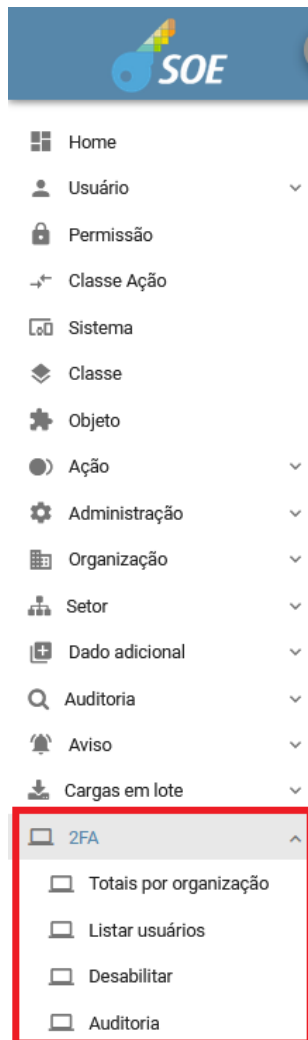
Selecione por quanto tempo um dispositivo será considerado confiável, sem exigir nova autenticação via 2FA.

- **1 dia:** Recomendado para dispositivos compartilhados ou ambientes de alta segurança.
- **7 dia:** Indicado para uso pessoal com risco moderado.
- **14 dia:** Conveniente para dispositivos pessoais e protegidos.

Importante:

- Tempos maiores oferecem conveniência, mas aumentam o risco de acesso indevido. Avalie conforme o contexto de uso.
- Alterações no tempo de confiança só terão efeito após o vencimento da configuração atual.

Mais informações sobre o 2FA



No aplicativo do SOE também tem o menu 2FA, disponível para os administradores de organização, com as seguintes opções:

- **Totais por organização:** 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.
- **Listar 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 um sistema.
- **Desabilitar:** esta 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.