INSTALANDO E CONFIGURANDO A

AUTENTICAÇÃO EM DUAS ETAPAS

PARA ACESSO AOS SISTEMAS

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO
TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL

AUTENTICAÇÃO EM DUAS ETAPAS VS DUPLO FATOR

FONTE: SENHASEGURA.COM[1]

COMO ACESSAR O CONTRACHEQUE NA PÁGINA DO TRE

Nos últimos anos, questões relacionadas à autenticação de usuários estão cada vez mais em evidência, considerando que esta é a razão ou o meio de prevenção de um dos maiores medos de qualquer organização: o vazamento de dados de clientes, fornecedores e colaboradores. Nesse contexto, senhas não são mais suficientes para proteger um sistema. Múltiplos fatores de autenticação, apesar de ser um conceito utilizado há algum tempo como solução à questão da proteção às senhas, ainda traz dúvidas para muitos usuários que precisam de proteção para credenciais em diversos sistemas.

A fim de garantir que quem está querendo acessar o sistema é de fato o usuário, é possível exigir a inserção de dois ou mais códigos de autenticação, além da senha. O objetivo é assegurar a legitimidade do acesso e evitar fraudes, uma vez que senhas podem ser obtidas de forma indevida, a impressão digital pode ser copiada através de um vidro ou o token pode ser roubado. Essa medida dificulta ações de atacantes que possam comprometer mais de um fator de autenticação, ao mesmo tempo.

---

[1] https://senhasegura.com/blog/diferenca-entre-two-factor-authentication-e-two-step-verification/

FATORES DE AUTENTICAÇÃO

Fatores de autenticação são categorias usadas para verificar e validar a identidade da solicitação do acesso, sendo divididos em três tipos:

- Fator de conhecimento: algo que o usuário tenha conhecimento.
- Fator de possessão: algo que o usuário possua.
- Fator de herança: algo que o usuário seja.

Estes fatores consideram dois tipos de processos para validar a identidade do usuário: a autenticação em duas etapas e a autenticação com duplo ou múltiplos fatores, os quais, muitas vezes, são confundidos como sendo o mesmo processo, porém possuem abordagem e níveis de segurança diferentes.

AUTENTICAÇÃO EM DUAS ETAPAS

O processo de autenticação em duas etapas (2FA) é muito simples: no momento da autenticação, quando as credenciais são solicitadas e o usuário insere sua senha, um código é enviado por SMS, e-mail ou ligação telefônica para um dispositivo pré-cadastrado para verificação da solicitação do acesso. Como a validade deste código é curta, caso o usuário não o utilize de imediato, será necessário gerar outro código para realizar a sua autenticação e obter o acesso, em outro momento.

O processo através de SMS ou ligação telefônica requer o cadastro de um número de telefone para receber o código, o que torna este tipo de autenticação vulnerável a ataques como o SIM-Swap (golpe que transfere a linha do chip da vítima para outro chip, em posse de um atacante malicioso).

Além do SMS, e-mail e ligação telefônica, os códigos para validação de usuário também podem ser gerados por aplicativos de autenticação, como o **Google Authenticator**. Para realizar esta autenticação, o usuário precisa inserir a sua senha e o código gerado através do aplicativo.

Este tipo de autenticação utiliza apenas um tipo de fator: de conhecimento. Muitas pessoas entendem que se trata de mais de um fator porque requer tanto a senha para acesso quanto o código de verificação, contudo é um tipo formado por dois pedaços de uma mesma informação baseada no conhecimento do usuário, que só ele sabe.

A autenticação em duas etapas é definida por etapas seguidas do mesmo fator de autenticação, ou seja, para se autenticar, o usuário deve inserir duas informações que somente ele sabe ou algo que ele possui.

Esse será o método utilizado para acessar os sistemas da página da internet do TRE, conforme veremos nas instruções mais adiante, nesse documento.

AUTENTICAÇÃO EM DOIS FATORES (2FA) OU MÚLTIPLO FATOR DE AUTENTICAÇÃO (2FV)

Este processo de autenticação é considerado o mais seguro, já que exige que o usuário insira no mínimo dois tipos de fatores de autenticação diferentes, como algo que ele tenha conhecimento e algo que ele tenha herdado.

- Algo que o usuário tenha conhecimento: senhas, PIN e códigos.
- Algo que o usuário possua: *smartcards*, USB Token, chave.
- Algo que o usuário tenha herdado: impressões digitais ou características físicas, como a íris.

A autenticação para acessar um *datacenter*, por exemplo, pode exigir que o usuário aproxime seu *smartcard* do visor da fechadura (ou mesmo sua digital em um leitor biométrico) e, em seguida, insira suas credenciais (usuário e senha). Ou seja, é mandatório realizar uma autenticação em dois fatores para entrar na sala.

A Autoridade de Bancos da Europa (EBA), em seu guia sobre pagamentos on-line, orienta que, no mínimo, um dos fatores não deve ser replicado, exceto o de herança, e que também não seja suscetível a roubos através da internet. Neste tipo de autenticação, cada pedaço de informação inserido é independente um do outro, porém as duas informações devem ser corretas para que o acesso seja liberado. Caso uma das informações inseridas esteja incorreta, somente esta deverá ser gerada novamente. Por conta disso, *tokens* baseados em tempo são muito usados, pois mudam constantemente em um intervalo de tempo, a cada cinco minutos, por exemplo.

É uma grande preocupação quando um desses fatores, principalmente e de possessão, é perdido ou por algum motivo destruído. Neste caso, o usuário não perde o acesso, pois quando o processo é implementado, uma chave mestra ou senha mestra é requisitada para a recuperação da conta. A maior preocupação é quando esta chave ou senha mestra é perdida ou roubada, pois pode comprometer a segurança e a recuperação da conta.

Senhas robustas são difíceis de se lembrar. Por este motivo, inserir mais de um fator de autenticação é um bom controle de segurança, ainda que possa tornar o processo de autenticação um pouco demorado, caso o usuário não tenha familiaridade com os fatores de autenticação ou com o processo. Existem ferramentas que, além de tornar o processo mais usual, gerenciam esses fatores e preenchem automaticamente senhas e informações de autenticação complexas.

Utilizar um único fator de autenticação não garante que quem está querendo acessar o sistema é, de fato, o respectivo usuário. Então, tentar tornar o processo de autenticação mais seguro e difícil de ser explorado por atacantes é um desafio para as organizações, independentemente do porte e segmentos em que atuam. Entre autenticação em duas etapas (2FA) e múltiplos fatores de autenticação (2FV), cabe a cada organização entender o que é mais adequado e seguro em relação às suas necessidades.

O comitê de segurança de TI do TRE entende que, pela natureza do acesso aos sistemas na página da internet e pela dificuldade em prover outros meios de autenticação para todos os usuários, a autenticação em duas etapas é suficiente para prover a segurança necessária para acesso ao sistemas. Por simplicidade, poderemos nos referir a esse processo como duplo fator (2FA), embora esteja esclarecido que trata-se, na verdade, de autenticação em duas etapas.

PRÉ-REQUISITOS

Você deve ter instalado em seu smartphone um aplicativo para gerenciamento de *tokens* e senhas. Sugerimos a utilização do **Google Authenticator** que pode ser obtido nas seguintes lojas de aplicativos:

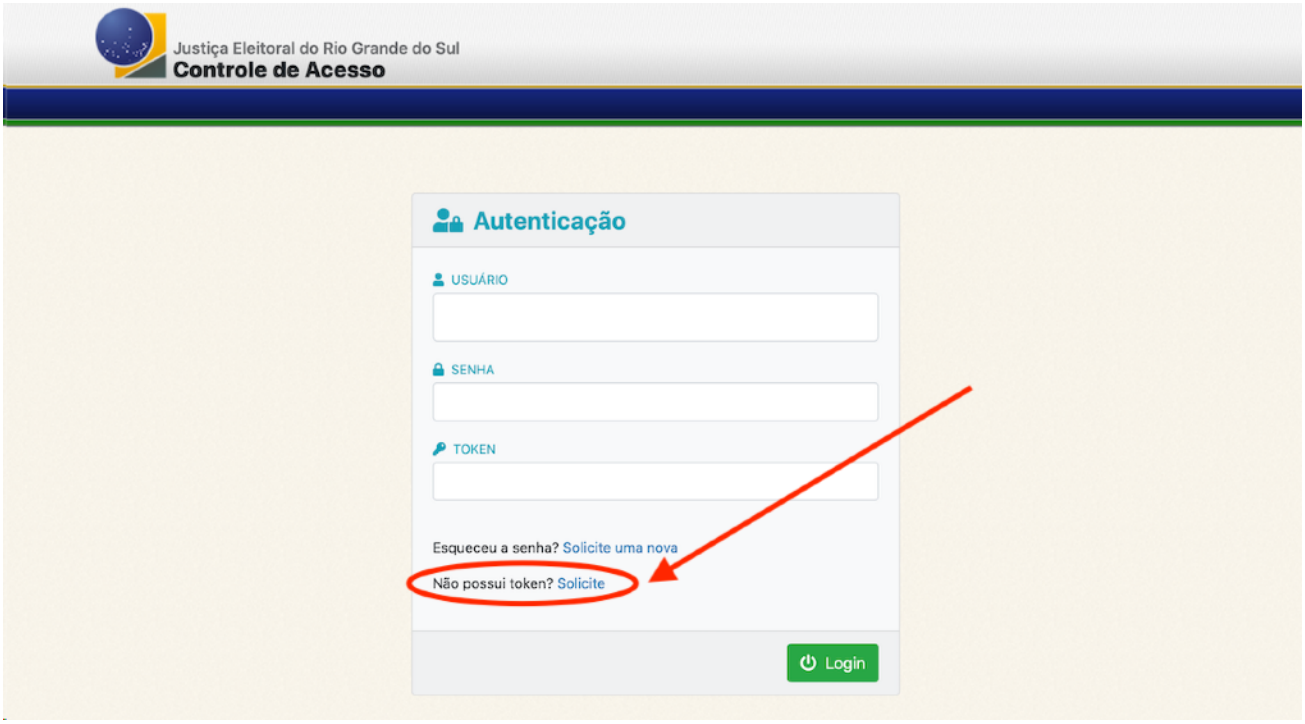
Google Play Store:
https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2

Apple App Store:
https://apps.apple.com/br/app/google-authenticator/id388497605

Se você ainda não tem o aplicativo, acesse o link correspondente ao sistema operacional do seu *smartphone* e instale-o antes de prosseguir.

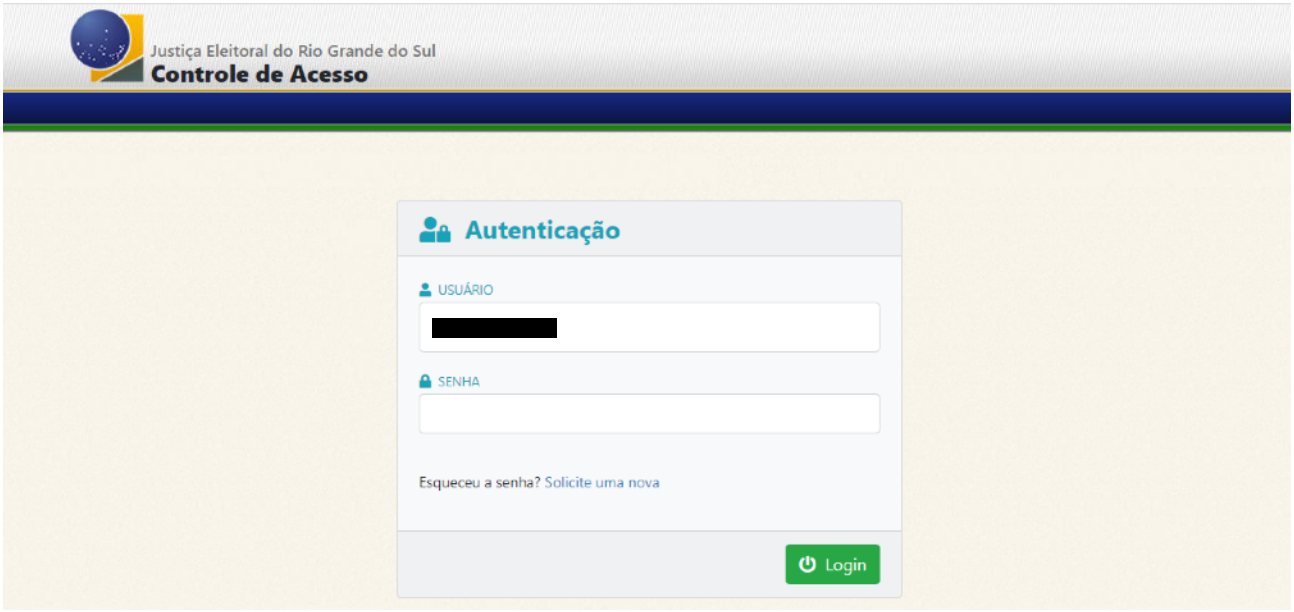
PROCEDIMENTOS

1. Se você estiver acessando um sistema que já exige o 2FA na página de internet do TRE e for solicitado um token, mas você ainda não possui o duplo fator de autenticação (2FA) configurado, é possível acessar o link de configuração diretamente pela página de login do sistema:

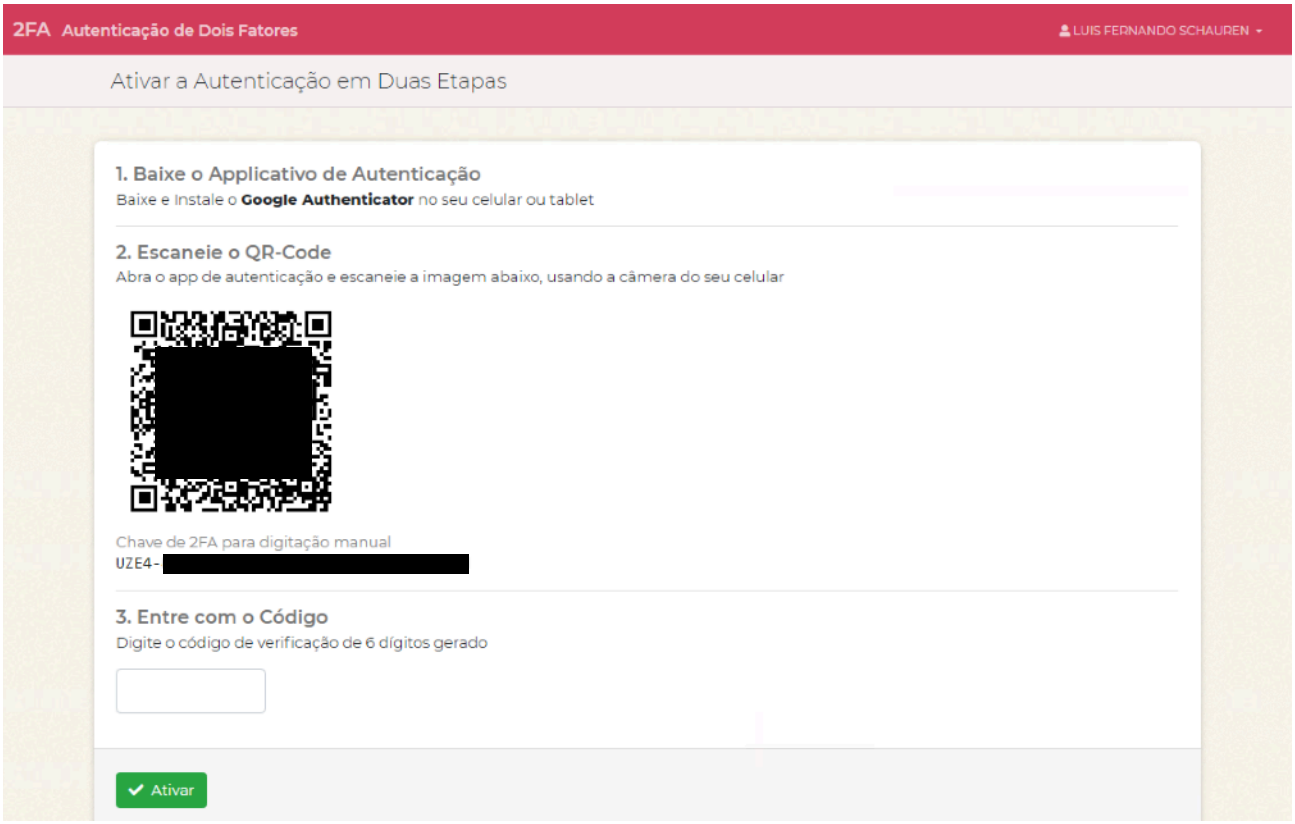


2. Se o sistema que você está acessando ainda não tem o 2FA configurado, então você poderá fazer essa configuração previamente, acessando diretamente, no navegador Google Chrome, o seguinte endereço: https://otp-seed.farm.tre-rs.jus.br/

3. Na tela de login, entre com seu usuário de e-mail (sem @tre-rs.jus.br) e senha:

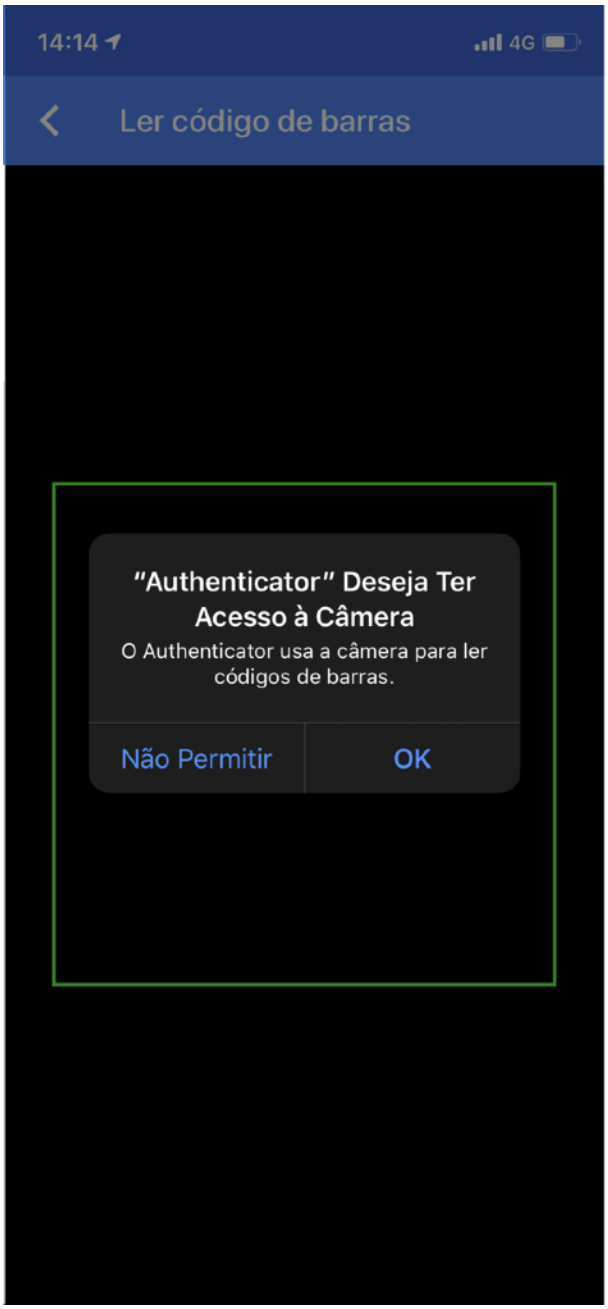


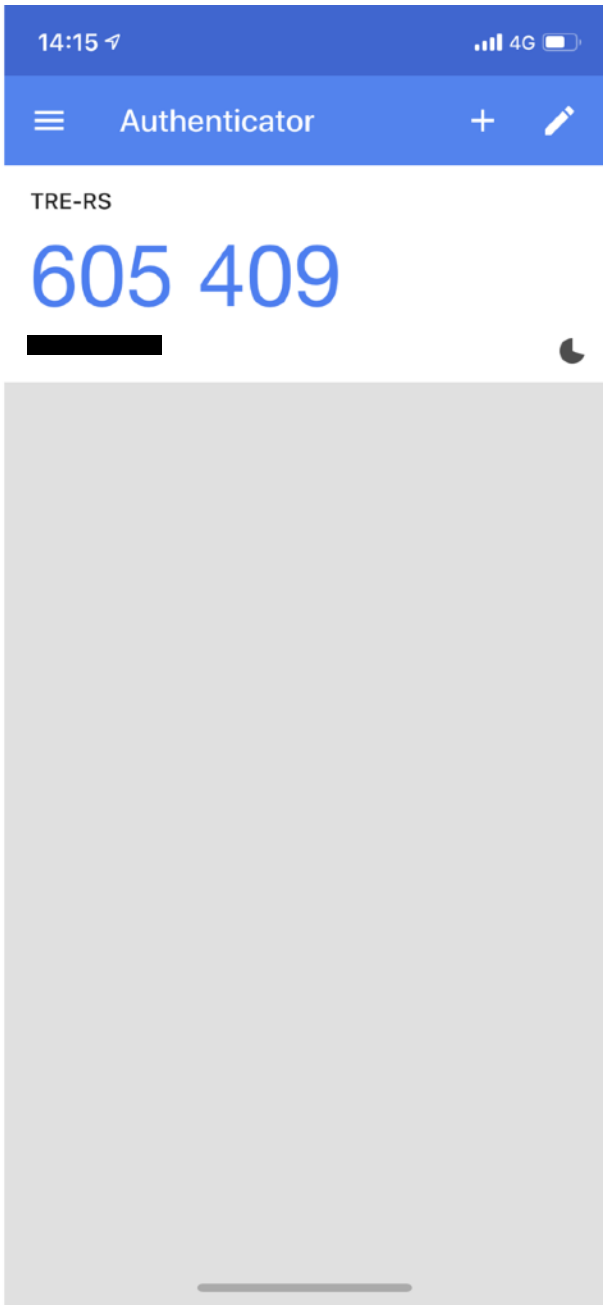
4. Agora será exibido uma tela com um **QR-Code** (um código de barras bidimensional), que deverá ser lido com o aplicativo **Google Authenticator**, fazendo uso da câmera do seu smartphone.



5. Abra o aplicativo **Google Authenticator** e clique em **Iniciar Configuração**, se isso ainda não foi feito, e depois clique em **Ler código de barras**.

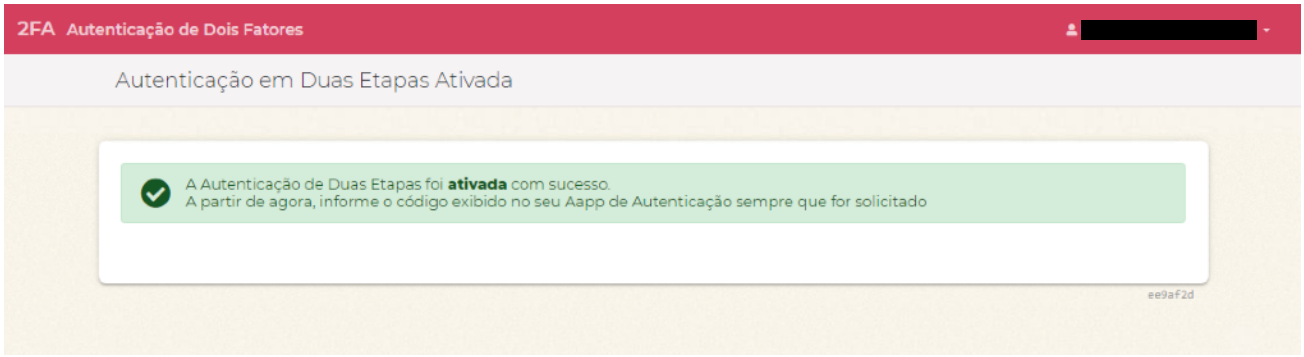
6. Pode ser que o aplicativo **Google Authenticator** solicite acesso à câmera do seu smartphone. Permita o acesso, se for o caso, e depois tente enquadrar o **QR-Code** exibido na tela do microcomputador dentro do quadro verde do aplicativo Google Authenticator.
   Uma vez lido o QR-Code, será gerado um código numérico de 6 dígitos, que tem duração de apenas 30 segundos - observe que o código vai mudando e que existe um timer que informa o tempo de validade restante para esse código.





7. Digite, no sistema de configuração da autenticação em 2 fatores (2FA), o código que está sendo exibido e clique em **Ativar** na parte inferior da tela, observando o tempo de validade desse código - talvez seja necessário digitar um novo código se o timer expirou. A dica é aguardar a geração de um novo código de seis dígitos e usá-lo no início do seu tempo de vida.

8. Se você digitou o código correto e clicou em **Ativar** dentro do tempo de validade desse código, será exibida a mensagem abaixo, confirmando o sucesso na ativação da **Autenticação em Duas Etapas**.



9. Pronto! A partir de agora, sempre que for solicitado um token, além da senha para autenticação, acesse o aplicativo Google Authenticator para gerar o código de 6 dígitos.