



MANUAL DO(A) USUÁRIO(A): ATIVAÇÃO DA AUTENTICAÇÃO EM DUAS ETAPAS (2FA)

Informações:

Versão:	3.4
Data de criação:	06/09/2023
Criada por:	Núcleo de Correio Eletrônico - Coordenadoria de Infraestrutura e Telecomunicações (CIT)
Aprovada por:	Claudio Henrique Carneiro Sampaio - Diretor da Diretoria de Informática e Automação (DIA)
Aprovada em:	30/01/2024

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações
06/09/2023	3.0	Jairo Ferreira Rocha Carlos José Lago Beckman	Confecção de novo manual.
11/09/2023	3.0	Hallyson Carlos R. Nascimento	Revisão final.
29/09/2023	3.1	Jairo Ferreira Rocha	Ajustes na capa do manual.
06/10/2023	3.2	Jairo Ferreira Rocha	Melhorias visuais e textuais
18/11/2023	3.3	Jairo Ferreira Rocha	Inclusão de dicas e adição da transferência da 2FA.
30/01/2024	3.4	Jairo Ferreira Rocha Hallyson Carlos R. Nascimento	Ajustes textuais e inclusão dos tópicos 4, 5 e 8.

SUMÁRIO

1. 2FA.....	4
1.1 O que é?.....	4
1.2 Como funciona?.....	4
1.3 Qual sua importância?.....	4
1.4 Onde utilizar?.....	5
1.5 Métodos.....	5
2. GMAIL - MENSAGEM DE TEXTO (SMS).....	6
2.1 Como ativar?.....	6
3. GMAIL - GOOGLE AUTHENTICATOR.....	10
3.1 Como instalar?.....	10
3.2 Como ativar?.....	10
3.3 Como transferir contas entre 02 dispositivos?.....	14
3.4 Removendo o método “Mensagem de Texto (SMS)”	16
4. GMAIL - TELEFONE DE RECUPERAÇÃO.....	19
4.1 Como cadastrar?.....	19
5. GMAIL - CÓDIGOS DE BACKUP.....	22
5.1 Como conseguir?.....	22
5.2 Como utilizar?.....	24
6. SENTINELA - GOOGLE AUTHENTICATOR.....	26
6.1 Como ativar?.....	26
7. SOLUÇÃO DE PROBLEMAS.....	29
7.1 Solução 01.....	29
7.2 Solução 02.....	29
7.3 Solução 03.....	29
8. FAQ.....	31
8.1 Dúvidas conceituais.....	31
8.2 Dúvidas do método “Verificação por SMS ou Chamada Telefônica”	32
8.3 Dúvidas do método “Google Authenticator”	33
8.4 Dúvidas do método “Solicitações do Google”	34

1. 2FA

1.1 O que é?

A autenticação em duas etapas, verificação em duas etapas ou autenticação de dois fatores é uma camada extra de proteção que pode ser ativada em contas online. Também conhecido pela sigla 2FA, originária do inglês **"two-factor authentication"**, o recurso insere uma segunda verificação de identidade do(a) usuário(a) no momento do login, evitando o acesso às contas mesmo quando a senha é vazada.

A funcionalidade está presente atualmente em aplicativos e serviços online. Cada plataforma oferece diferentes métodos de verificação, que podem compreender códigos SMS, dispositivos de token, biometria e códigos, por exemplo.

1.2 Como funciona?

De forma simplificada, a autenticação em duas etapas adiciona uma camada extra de segurança quando o(a) usuário(a) acessa algum tipo de aplicativo ou serviço online. Mesmo que suas credenciais sejam roubadas, dificilmente uma pessoa não autorizada conseguirá entrar nos seus perfis, porque ela não terá informações do segundo fator.

Ao inserir nome e senha, por exemplo, há a primeira etapa da autenticação, e quando uma nova informação para confirmar a identidade é exigida, há a segunda fase, ou seja, autenticação em duas etapas.

Embora nem todo mundo conheça a expressão, é muito provável que a maioria já tenha passado por ela, seja inserindo a impressão digital em um caixa eletrônico após validar a senha ou inserindo um código de ativação recebido via SMS após validar e-mail e senha em um acesso.

Para não cair em golpes ou ter sua conta invadida, é importante nunca compartilhar os códigos recebidos ou gerados com terceiros.

1.3 Qual sua importância?

As senhas, quando não implementadas com outros fatores de autenticação, são consideradas métodos de segurança fracos. Ainda que sejam necessárias, ter apenas um código de texto é insuficiente para proteger as contas, considerando a sofisticação dos sistemas de roubo atuais.

Embora não possamos afirmar que seja à prova de falhas, a autenticação em duas etapas é extremamente importante para elevar o nível de segurança dos dados que trafegam em ambientes digitais, já que complica muito o trabalho de possíveis invasores.

1.4 Onde utilizar?

A autenticação em duas etapas está disponível para:

- Acesso a operações bancárias e compras on-line;
- E-mail (Gmail, Microsoft, Yahoo, Outlook, etc.);
- Contas de armazenamento na nuvem (Apple, Dropbox, Box, etc.);
- Contas nas redes sociais (Facebook, Instagram, LinkedIn, Twitter, etc.);
- Aplicativos de produtividade (Evernote, Trello, etc.);
- Gerenciadores de senhas (LastPass, etc.).

1.5 Métodos

Existem vários métodos de autenticação em duas etapas, logo abaixo seguem algumas delas:

- Código de verificação via SMS ou chamada telefônica;
- Código de verificação pelo aplicativo Google Authenticator: dispositivos móveis com Android ou dispositivos iOS (iPhone, iPod Touch ou iPad com iOS 5.0 ou posterior) utilizam o aplicativo para gerar o código de verificação;
- Solicitações do Google: Android atualizado ou iPhone (5S ou posterior) com o aplicativo do google instalado.

2. GMAIL - MENSAGEM DE TEXTO (SMS)

Esse é o método inicial apresentado para realizar a autenticação em duas etapas no ambiente corporativo do Tribunal de Justiça do Estado do Maranhão (TJMA). Esse método também é conhecido como “**Smartphones para verificação em duas etapas**”.

⚠ O método de autenticação recomendado pela Diretoria de Informática e Automação (DIA) é o **Google Authenticator**, um aplicativo de autenticação em duas etapas (2FA), detalhado no tópico 3 deste manual.

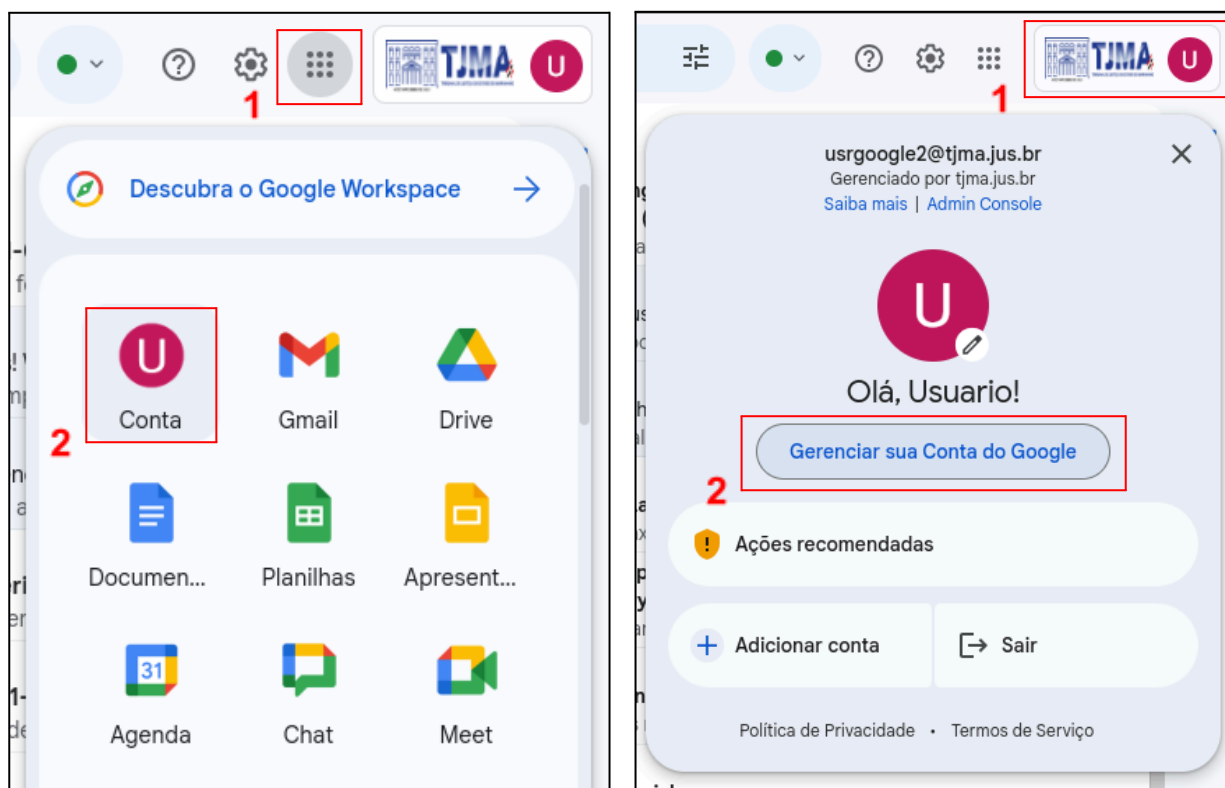
2.1 Como ativar?

2.1.1 Logue na sua conta de e-mail do domínio **tjma.jus.br** (conta corporativa) e informe sua senha.

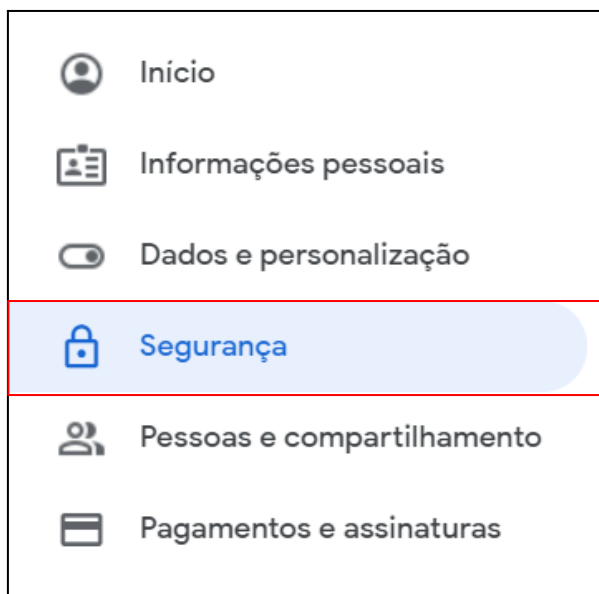
2.1.2 Existem 02 (duas) formas de chegar na opção “**Segurança**”:

a) No menu do aplicativo do Google “**Google Apps**” selecione “**Conta**”.

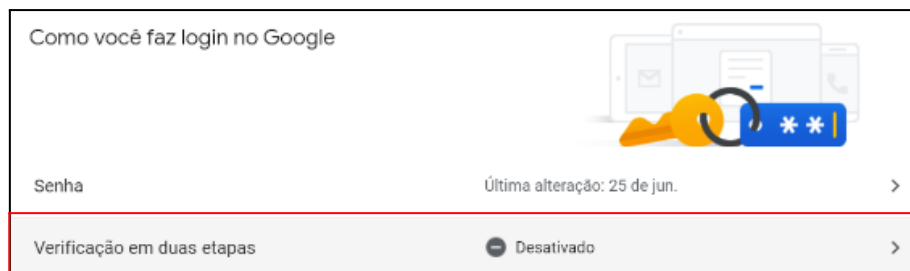
b) Em “**Conta do Google**” selecione “**Gerenciar sua Conta do Google**”.



2.1.3 Clique na opção “**Segurança**”.



2.1.4 Em **"Como você faz login no Google"** clique em **"Verificação em duas etapas"**.

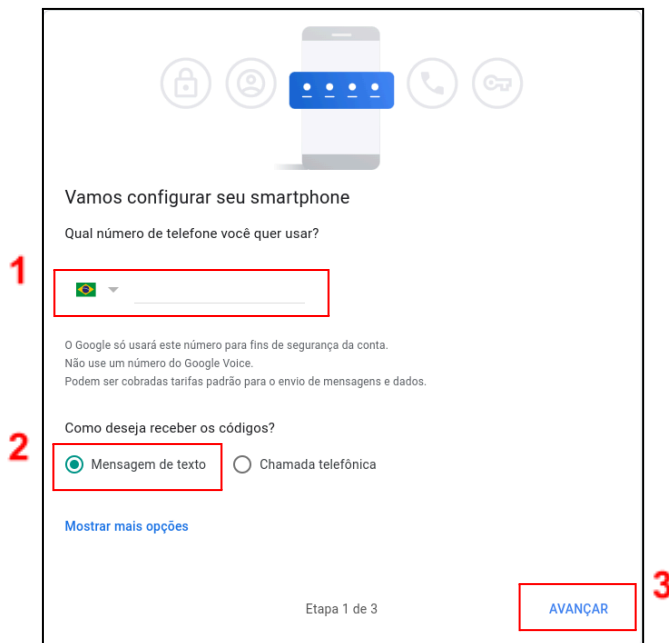


⚠ Insira novamente sua senha novamente, caso seja solicitado.

2.1.5 Na página **"Verificação em duas etapas"** clique em **"Começar"**.

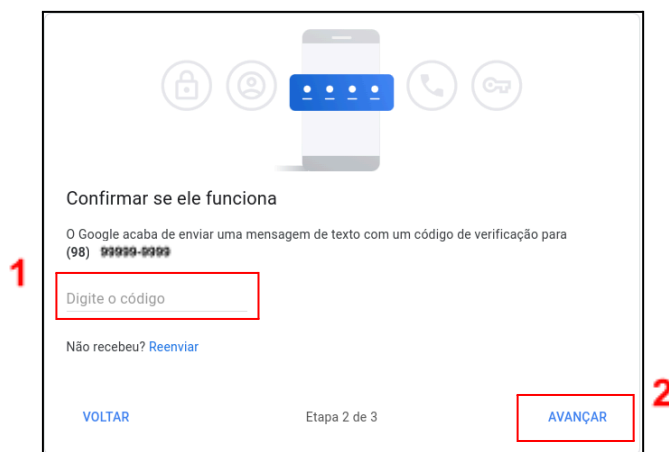


2.1.6 Etapa 1 de 3: Confirme se a bandeira do Brasil está selecionada, insira o número de seu dispositivo móvel (smartphone/celular) com o DDD, mantenha a opção **"Mensagem de texto"** marcada e clique em **"AVANÇAR"**.



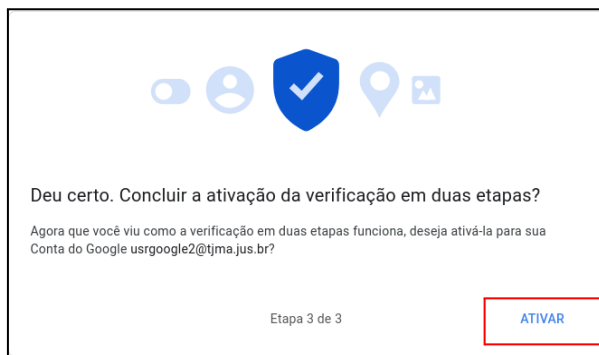
⚠ O Google usará o número do seu dispositivo móvel (smartphone/celular) para enviar códigos de verificação (SMS) para você. Não utilize o número do **"Google Voice"** ou de telefone fixo, pois podem ser cobradas tarifas de uso. Não marque a opção **"Chamada telefônica"**, pois essa não é uma opção coberta ou recomendada neste manual e pode ser considerada insegura.

2.1.7 Etapa 2 de 3: Digite o código de verificação (**informe apenas os números, sem a letra "G"**) que foi enviado para o número do smartphone/celular informado e clique em **"AVANÇAR"**.



⚠ Caso não receba o código, clique em **"Reenviar"**. Caso não o receba mais uma vez, clique em **"VOLTAR"** e confirme o número informado. Repita o processo.

2.1.8 Etapa 3 de 3: Clique em "ATIVAR".



2.1.9 Pronto, sua ativação foi finalizada.

2.1.10 Prossiga para a ativação do método padrão adotado pelo TJMA, conforme detalhado no tópico seguinte (3), "GMAIL - GOOGLE AUTHENTICATOR".

3. GMAIL - GOOGLE AUTHENTICATOR

Este é o método **padrão**, que utiliza aplicativo (App) chamado “**Google Authenticator**”, para realizar a autenticação em duas etapas no ambiente corporativo do TJMA.

⚠ Este método consiste em utilizar o aplicativo “**Google Authenticator**” para gerar códigos aleatórios e assim acessar o e-mail corporativo e o sistema “**SENTINELA**”.

3.1 Como instalar?

No dispositivo móvel, acesse a “**Google Play Store**” ou “**Apple's App Store**”, procure pelo aplicativo “**Google Authenticator**” e instale-o. Para utilizá-lo, é necessário ter Android 4.4 ou versão mais recente, ou iPhone 5S ou posterior, além de ter configurado o bloqueio de tela com PIN, senha, padrão (pattern) ou digital (fingerprint).

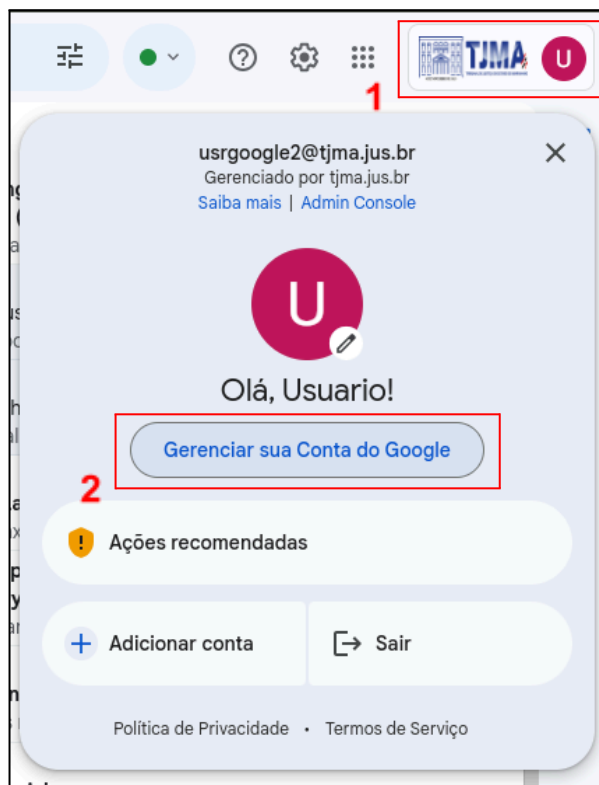
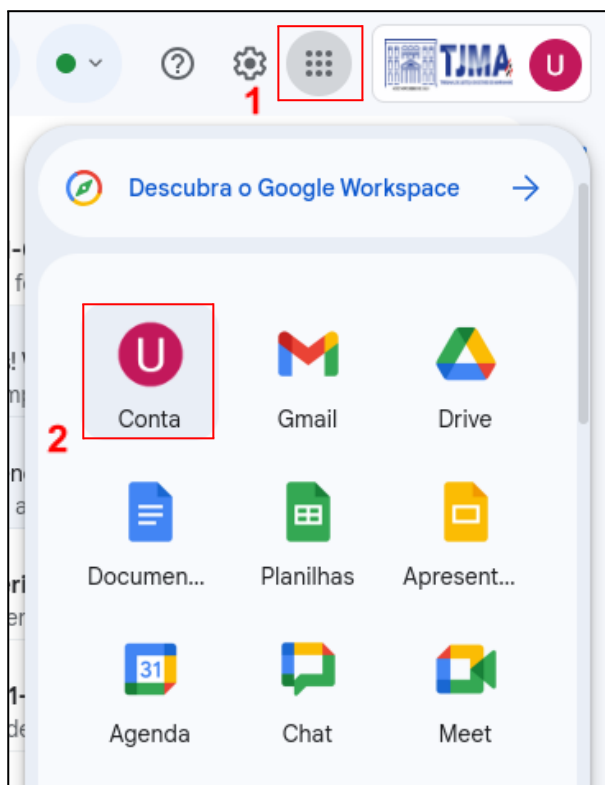
3.2 Como ativar?

3.2.1 Logue na sua conta de e-mail do domínio **tjma.jus.br** (conta corporativa) e informe sua senha.

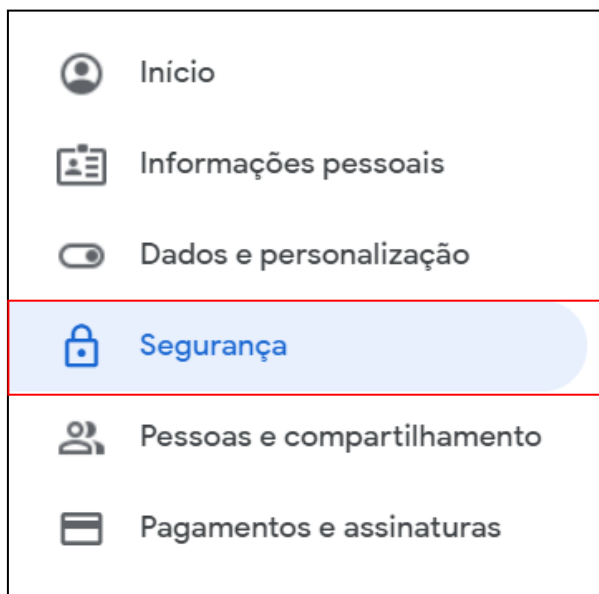
3.2.2 Existem 02 (duas) formas de chegar na opção “**Segurança**”:

a) No menu do aplicativo do Google “**Google Apps**” selecione “**Conta**”.

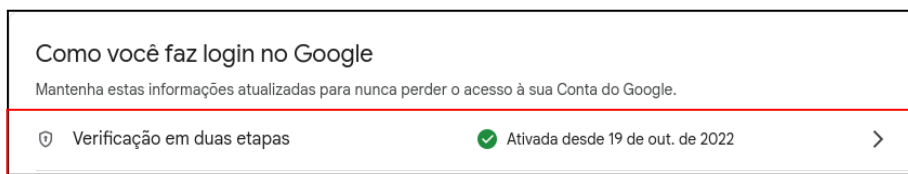
b) Em “**Conta do Google**” selecione “**Gerenciar sua Conta do Google**”.



3.2.3 Clique na opção "**Segurança**".

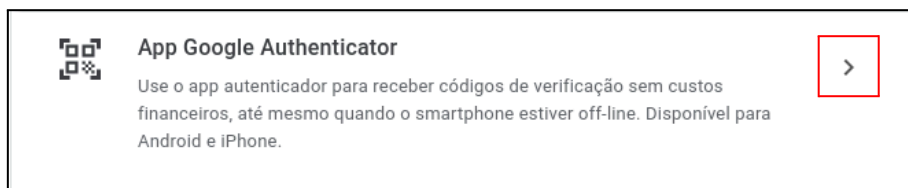


3.2.4 Em "**Como você faz login no Google**" clique em "**Verificação em duas etapas**".



 **Insira novamente sua senha novamente, caso seja solicitado.**

3.2.5 Em "**Verificação em duas etapas**", localize "**App Google Authenticator**" e clique na setinha ">". Se essa opção não estiver disponível, procure por "**Google Authenticator**".



Como você faz login no Google

Mantenha estas informações atualizadas para nunca perder o acesso à sua Conta do Google.

Verificação em duas etapas	Ativada desde 14:41	>
Senha	Última alteração: 26 de abr. de 2023	>
Smartphones para verificação em duas etapas		>
Telefone de recuperação	Adicione um número de celular	>
E-mail de recuperação	Adicionar um endereço de e-mail	>

Você pode adicionar mais opções de login

Chaves de acesso Chaves de segurança **Google Authenticator** Solicitação do Google

3.2.6 Clique em "**Configurar o autenticador**".

← App Google Authenticator

Em vez de esperar mensagens de texto, receba códigos de verificação de um app autenticador. Essa opção funciona mesmo quando o smartphone está off-line.

Primeiro, faça o download do Google Authenticator na [Google Play Store](#) ou na [App Store da Apple](#).

+ Configurar o autenticador


⚠ O passo seguinte deve ser realizado em sincronia com o smartphone/celular.

3.2.7 No dispositivo móvel (smartphone/celular) utilizando o aplicativo "**Google Authenticator**", toque em "+".

- Selecione "**Ler código QR/Scan a QR Code**".
- Após abrir a câmera, aponte para o "**QR Code**".
- Após a leitura do "**QR Code**" clique em "**Avançar**".

Configurar o app autenticador

- No app Google Authenticator, toque em +
- Selecione **Ler código QR**



Não consegue ler o código?

Cancelar Avançar

⚠ Caso não consiga ler o código, clique em **“Não consegue ler o código”** e siga as orientações informadas.

3.2.8 Digite o código de 6 dígitos mostrado no aplicativo **“Google Authenticator”** do dispositivo móvel (smartphone/celular).

a) Clique em **“Verificar”**.

Configurar o app autenticador

Digite o código de seis dígitos mostrado no app

1

Digite o código

Voltar

Cancelar Verificar 2

3.2.9 Pronto. A ativação foi finalizada.

3.2.10 Saia de sua conta para validação. Em **“Conta do Google”** selecione **“Sair”**.



3.2.11 Logue novamente na sua conta de e-mail do domínio **tjma.jus.br** (conta corporativa), informe sua senha e agora informe o código gerado no “**Google Authenticator**”.

⚠ Caso o código não seja solicitado, experimente realizar esse procedimento utilizando uma janela anônima ou privada, com o navegador de sua preferência.

⚠ Ao ativar este método e acessar sua conta de e-mail corporativo, você pode remover o método “**Mensagem de Texto (SMS)**”, conforme detalhado no item 3.4.

3.3 Como transferir contas entre 02 dispositivos?

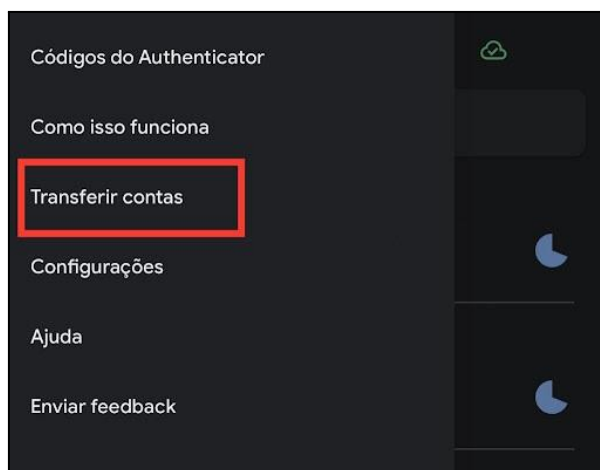
Este item descreve como transferir contas no aplicativo “**Google Authenticator**” entre 02 (dois) dispositivos móveis, principalmente em casos de troca de aparelho ou de compartilhamento de várias pessoas gerenciando uma mesma conta corporativa.

⚠ Este procedimento é destinado para conta corporativa que possua mais de um(a) servidor(a) gerenciando-a. A indicação do(a) servidor(a) e a transferência é feita sob a responsabilidade do(a):

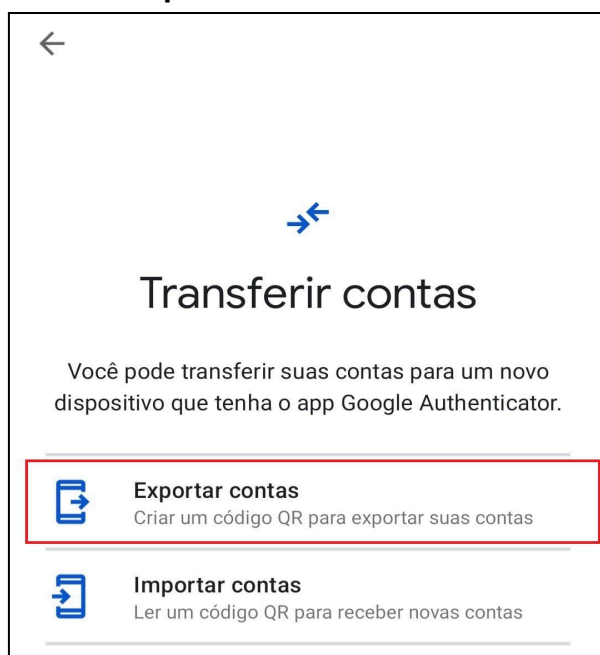
- secretário(a) judicial para a conta corporativa da unidade judicial;
- superior imediato(a): chefe, coordenador(a), diretor(a), supervisor(a), etc. para a conta corporativa da unidade administrativa.

3.3.1 No dispositivo móvel (smartphone/celular) do(a) secretário(a) judicial ou superior imediato(a):

a) Abra o aplicativo “**Google Authenticator**” e clique em “**Transferir contas/Transfer accounts**”.



b) Clique em “**Exportar contas/Export accounts**”.



c) Desmarque todas as opções, deixando selecionada apenas a opção desejada. Exemplo: “**Google: contacorporativa@tjma.jus.br**”. Clique em “**Próxima/Next**”.

d) O aplicativo “**Google Authenticator**” exibirá um “**QR Code**” na tela. Apresente o “**QR Code**” para o(a) servidor(a) indicado(a) fazer a leitura do mesmo.

3.3.2 No dispositivo móvel (smartphone/celular) do(a) servidor(a) indicado(a):

a) Abra o aplicativo “**Google Authenticator**” e clique em “**+**”.

b) Selecione “**Ler código QR/Scan a QR Code**”.

c) Após abrir a câmera, aponte para o “**QR Code**” gerado pelo(a) secretário(a) judicial ou superior imediato(a) e faça a leitura do mesmo.

3.3.3 Após o(a) servidor(a) indicado(a) realizar a leitura do “**QR Code**”, clique em “**Done/Concluir**”.

3.3.4 Valide se a conta foi transferida corretamente realizando um acesso.

3.4 Removendo o método “**Mensagem de Texto (SMS)**”

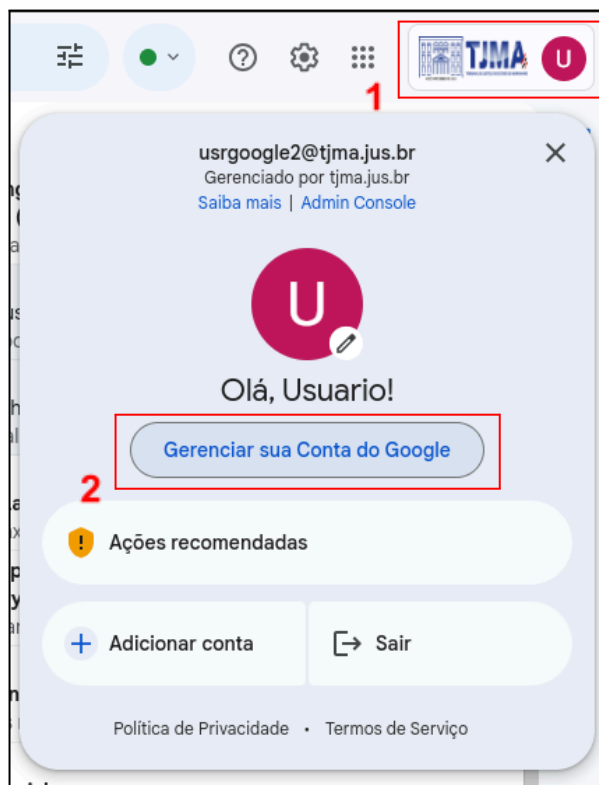
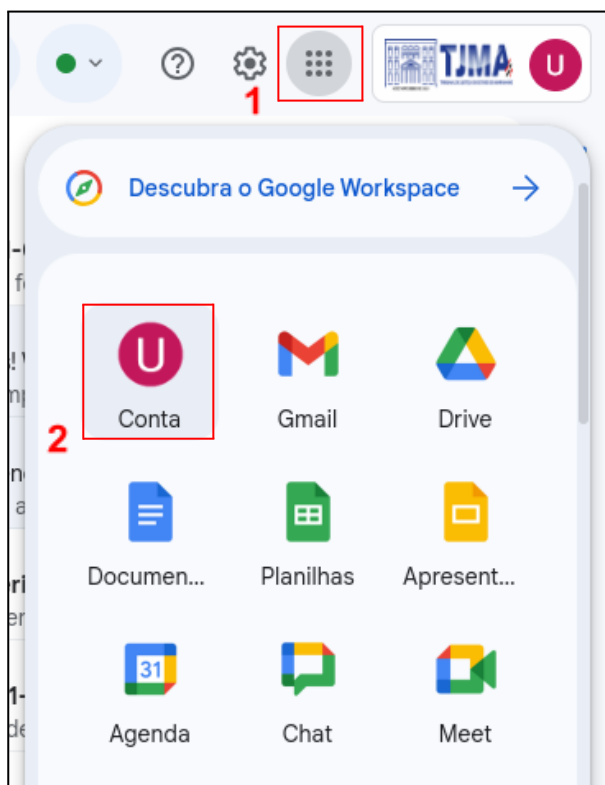
⚠ Este método também é conhecido como “**Smartphones para verificação em duas etapas**”.

3.4.1 Logue na sua conta de e-mail do domínio **tjma.jus.br** (conta corporativa) e informe sua senha.

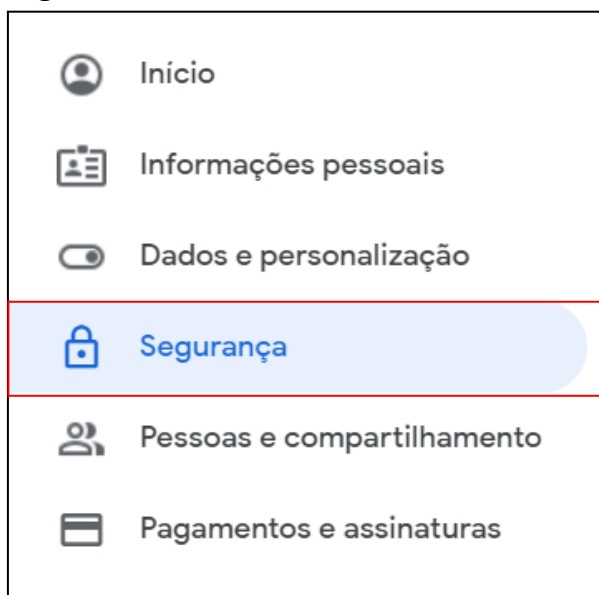
3.4.2 Existem 02 (duas) formas de chegar na opção “**Segurança**”:

a) No menu do aplicativo do Google “**Google Apps**” selecione “**Conta**”.

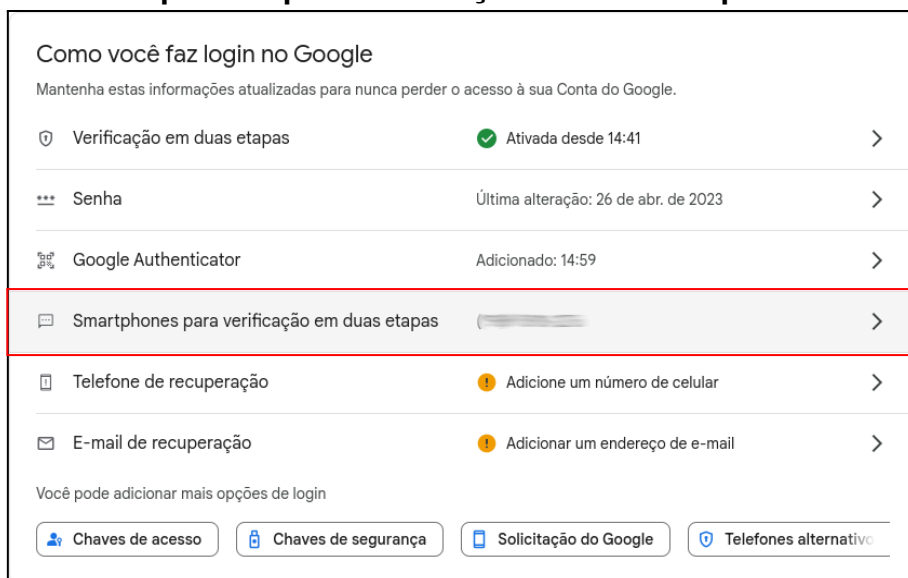
b) Em “**Conta do Google**” selecione “**Gerenciar sua Conta do Google**”.



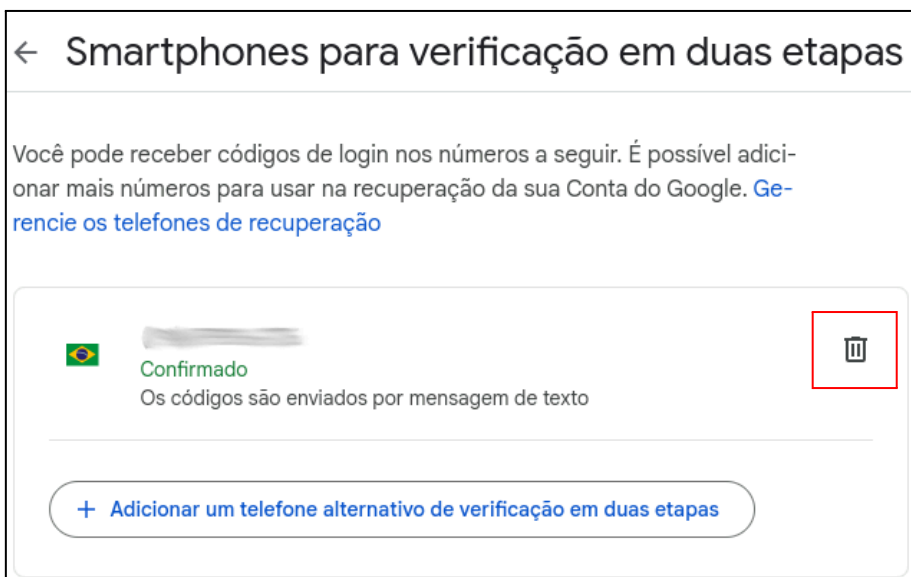
3.4.3 Acesse a opção "**Segurança**".



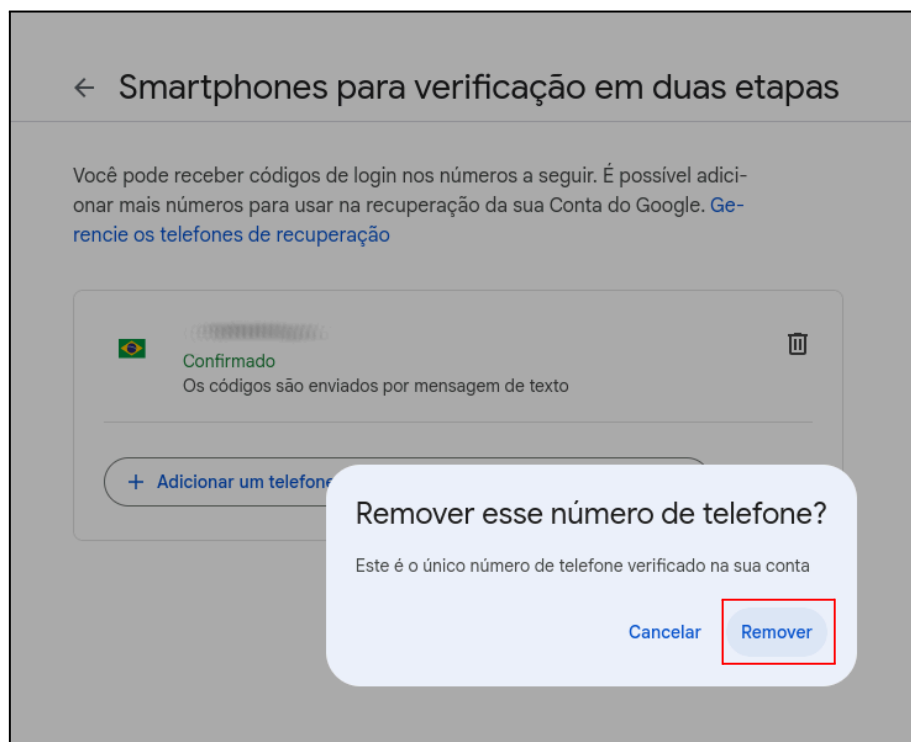
3.4.4 Clique em "**Smartphones para verificação em duas etapas**".



3.4.5 Clique na "**Lixeira**" para excluir o número cadastrado.



3.4.6 Clique em “**Remover**”.



3.4.7 Pronto, a remoção do número de telefone foi realizada.

⚠ A exclusão do número de telefone associado ao método “**Mensagem de Texto (SMS)**” ou “**Smartphones para verificação em duas etapas**” não deve ser confundida com o número registrado como “**Telefone de recuperação**”.

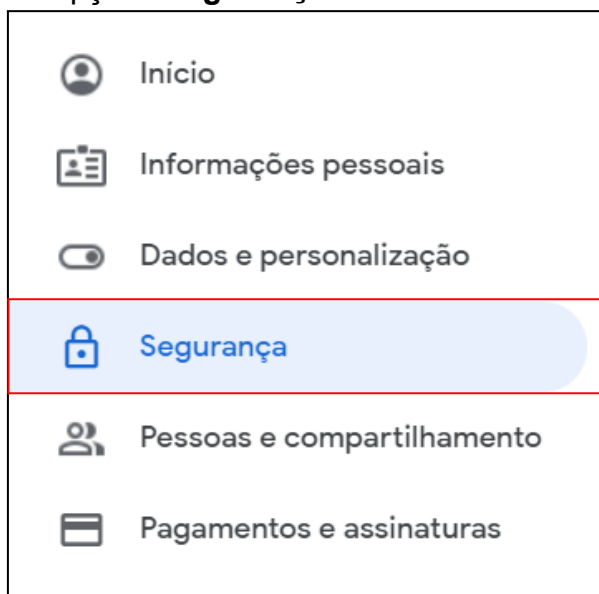
4. GMAIL - TELEFONE DE RECUPERAÇÃO

O número de telefone de recuperação será utilizado apenas para a Diretoria de Informática e Automação (DIA) entrar em contato com o(a) usuário(a), caso seja detectada alguma atividade suspeita na conta corporativa. Certifique-se de fornecer o número corretamente e mantê-lo atualizado, revisando-o periodicamente para garantir sua precisão.

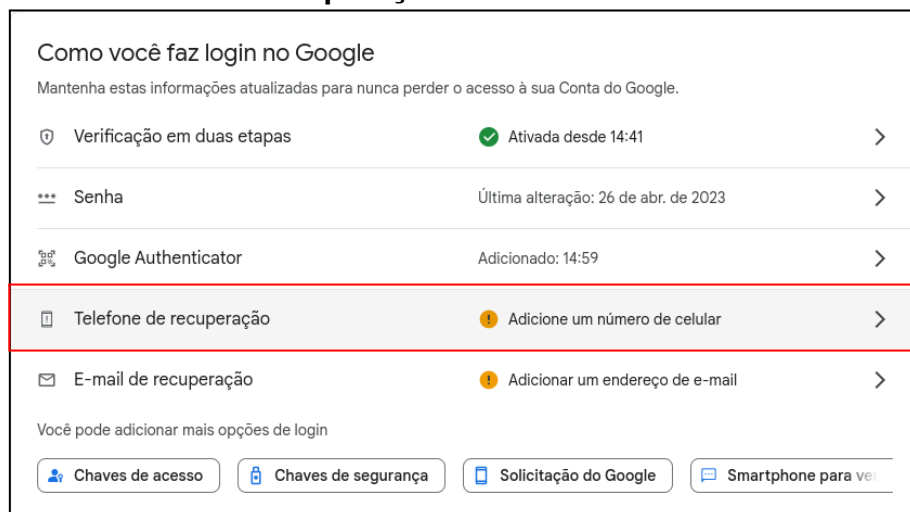
⚠ O número cadastrado do **“Telefone de recuperação”** não serve para receber mensagem de texto (SMS).

4.1 Como cadastrar?

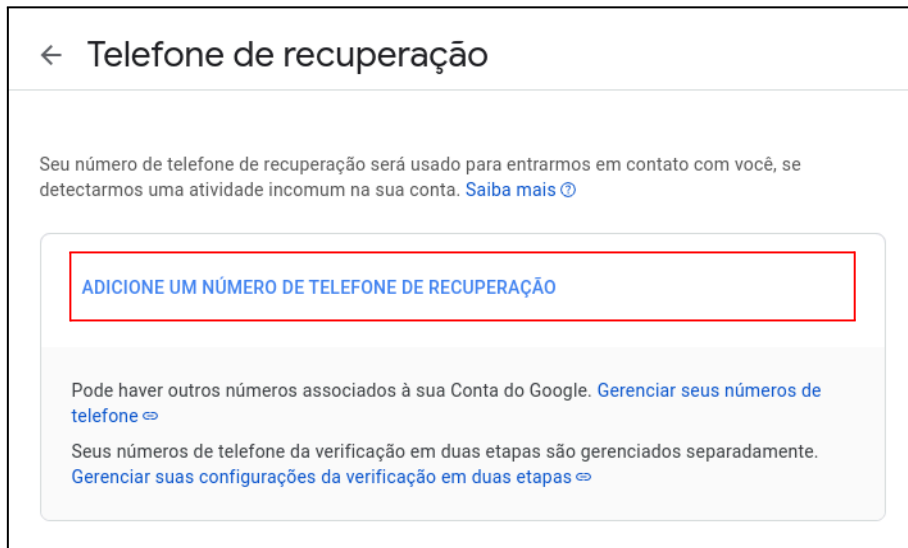
4.1.1 Acesse novamente a opção **“Segurança”**.



4.1.2 Clique em **“Telefone de recuperação”**.



4.1.3 Clique em **“ADICIONE UM NÚMERO DE TELEFONE DE RECUPERAÇÃO”**.



← Telefone de recuperação

Seu número de telefone de recuperação será usado para entrarmos em contato com você, se detectarmos uma atividade incomum na sua conta. [Saiba mais](#) ⓘ

ADICIONE UM NÚMERO DE TELEFONE DE RECUPERAÇÃO

Pode haver outros números associados à sua Conta do Google. [Gerenciar seus números de telefone](#) ⇌

Seus números de telefone da verificação em duas etapas são gerenciados separadamente. [Gerenciar suas configurações da verificação em duas etapas](#) ⇌

4.1.4 Adicione um número de telefone e clique em **“AVANÇAR”**.



← Telefone de recuperação


Seu número de telefone de recuperação será usado para entrarmos em contato com você, se detectarmos uma atividade incomum na sua conta. [Saiba mais](#) ⓘ

ADICIONE UM NÚMERO DE TELEFONE DE RECUPERAÇÃO

Pode haver outros números associados à sua Conta do Google. [Gerenciar seus números de telefone](#) ⇌

Seus números de telefone da verificação em duas etapas são gerenciados separadamente. [Gerenciar suas configurações da verificação em duas etapas](#) ⇌

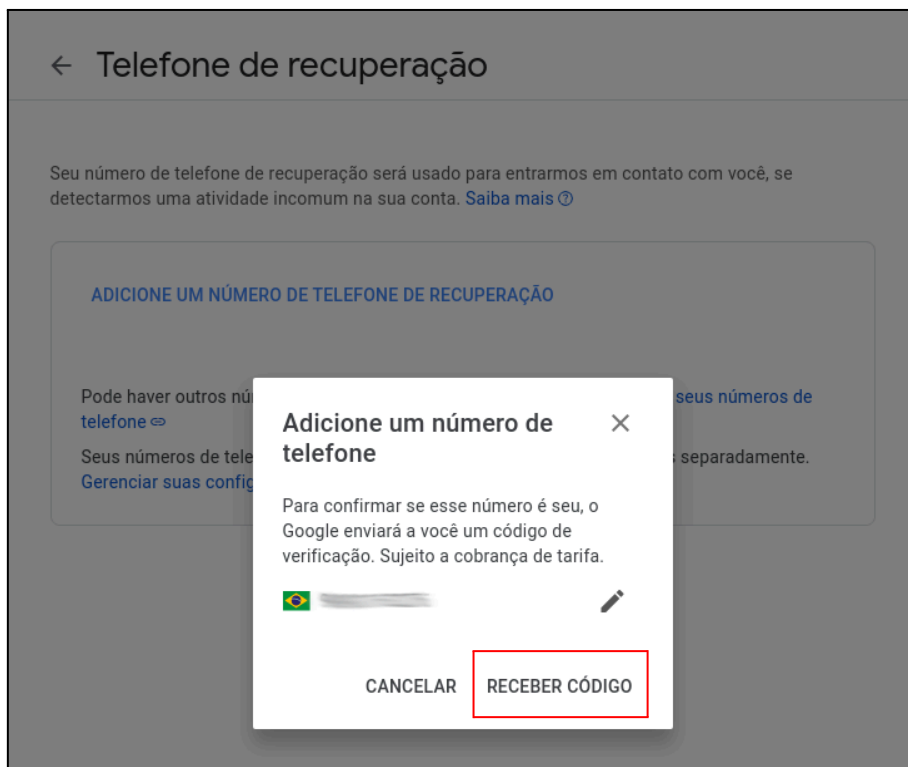
Adicione um número de telefone ×

 1

Seu número de telefone será usado para fins de segurança. Por exemplo, para ajudar você a recuperar sua conta, caso tenha esquecido sua senha.

CANCELAR 2 **AVANÇAR**

4.1.5 Clique em **“RECEBER CÓDIGO”**.



← Telefone de recuperação

Seu número de telefone de recuperação será usado para entrarmos em contato com você, se detectarmos uma atividade incomum na sua conta. [Saiba mais](#)


ADICIONE UM NÚMERO DE TELEFONE DE RECUPERAÇÃO

Pode haver outros números de telefone associados à sua conta. [Gerenciar suas configurações](#)

Seus números de telefone são gerenciados separadamente.

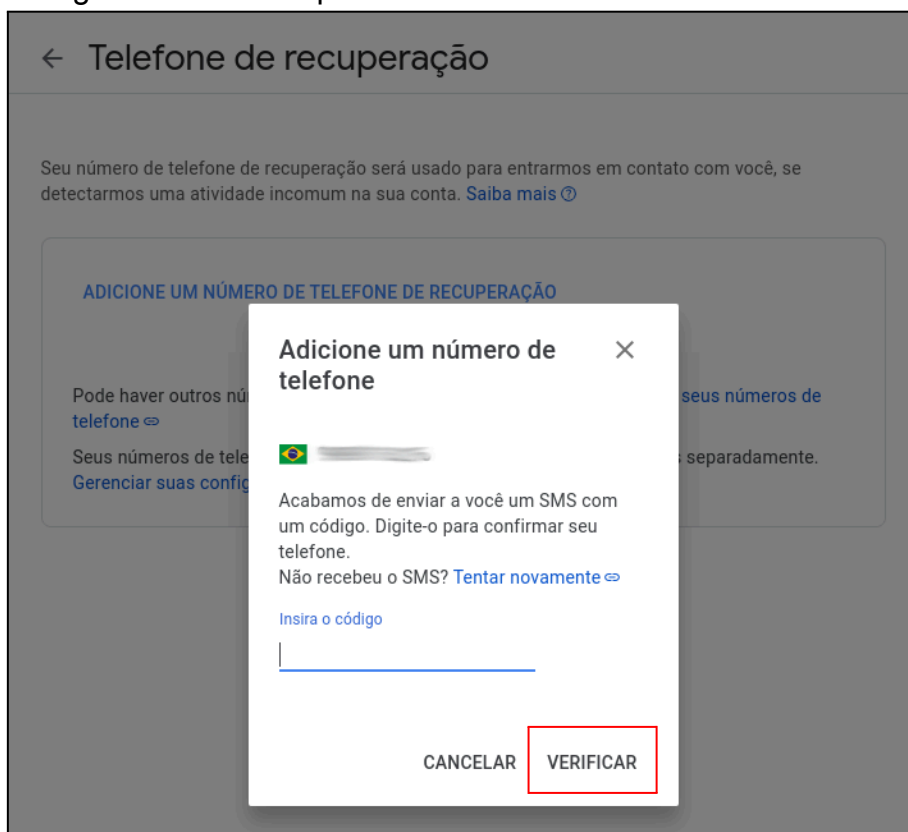
Adicione um número de telefone ✕

Para confirmar se esse número é seu, o Google enviará a você um código de verificação. Sujeito a cobrança de tarifa.



CANCELAR RECEBER CÓDIGO

4.1.6 Insira o código recebido e clique em “**VERIFICAR**”.



← Telefone de recuperação


Seu número de telefone de recuperação será usado para entrarmos em contato com você, se detectarmos uma atividade incomum na sua conta. [Saiba mais](#)

ADICIONE UM NÚMERO DE TELEFONE DE RECUPERAÇÃO

Pode haver outros números de telefone associados à sua conta. [Gerenciar suas configurações](#)

Seus números de telefone são gerenciados separadamente.

Adicione um número de telefone ✕



Acabamos de enviar a você um SMS com um código. Digite-o para confirmar seu telefone.

Não recebeu o SMS? [Tentar novamente](#)

Insira o código

CANCELAR VERIFICAR

4.1.7 Pronto, o telefone de recuperação foi cadastrado.

5. GMAIL - CÓDIGOS DE BACKUP

Os códigos de backup são conjuntos exclusivos de códigos que proporcionam uma camada adicional de autenticação e recuperação de conta.

É essencial armazenar esses códigos em um local seguro e de fácil acesso, garantindo que estejam prontamente disponíveis em caso de perda do dispositivo móvel (smartphone/celular).

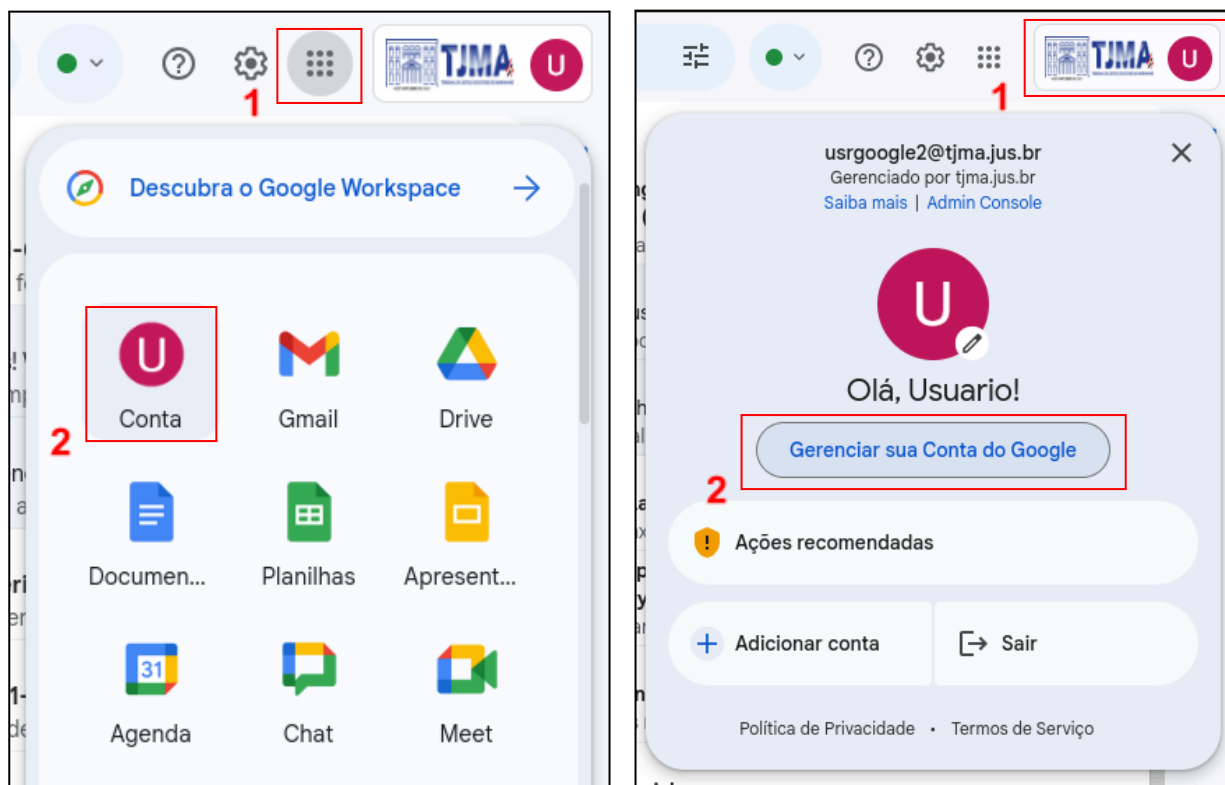
5.1 Como conseguir?

5.1.1 Logue na sua conta de e-mail do domínio **tjma.jus.br** (conta corporativa) e informe sua senha.

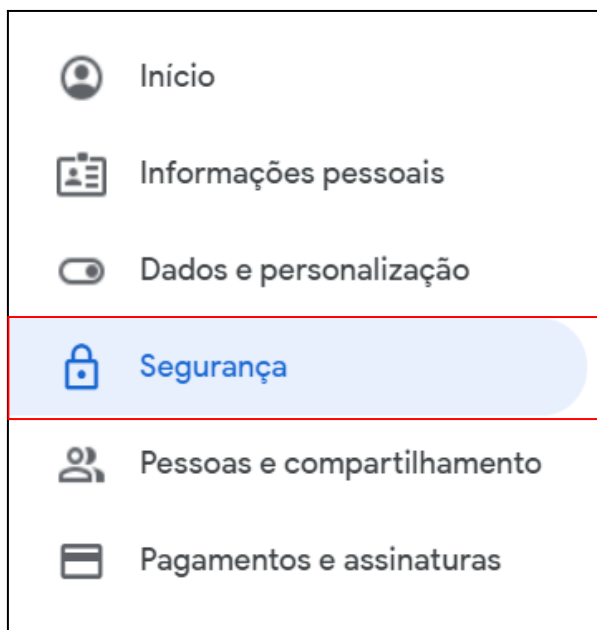
5.1.2 Existem 02 (duas) formas de chegar na opção “**Segurança**”:

a) No menu do aplicativo do Google “**Google Apps**” selecione “**Conta**”.

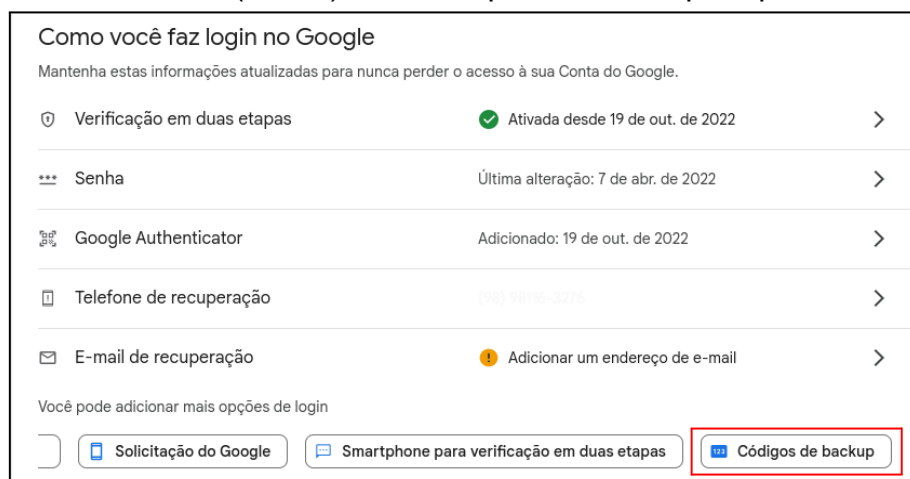
b) Em “**Conta do Google**” selecione “**Gerenciar sua Conta do Google**”.



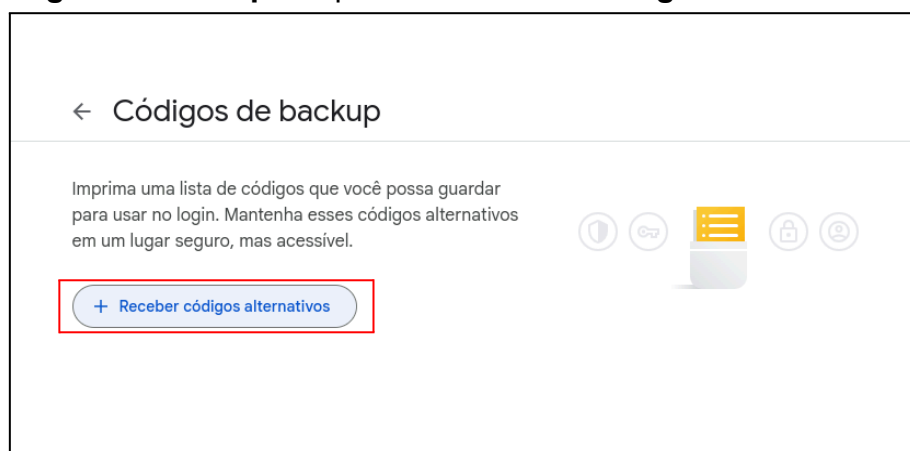
5.1.3 Na opção “**Segurança**”.



5.1.4 Em **"Como você faz login no Google"** clique em **"Códigos de backup"**. Esta opção pode estar escondida (oculta), então clique nas setas para procurar.



5.1.5 Em **"Códigos de backup"** clique em **"Receber códigos alternativos"**.



5.1.6 Imprima ou faça o download dos códigos de backup e mantenha-os em um local seguro e acessível, pois podem ser úteis em situações de perda do dispositivo móvel.

← Códigos de backup

Imprima uma lista de códigos que você possa guardar para usar no login.
Mantenha esses códigos alternativos em um lugar seguro, mas acessível.

Seus códigos alternativos

10 códigos alternativos restantes

Criação: agora mesmo



XXXXXXXXXX

XXXXXXXXXX

XXXXXXXXXX

XXXXXXXXXX

XXXXXXXXXX

XXXXXXXXXX

XXXXXXXXXX

XXXXXXXXXX

XXXXXXXXXX

XXXXXXXXXX



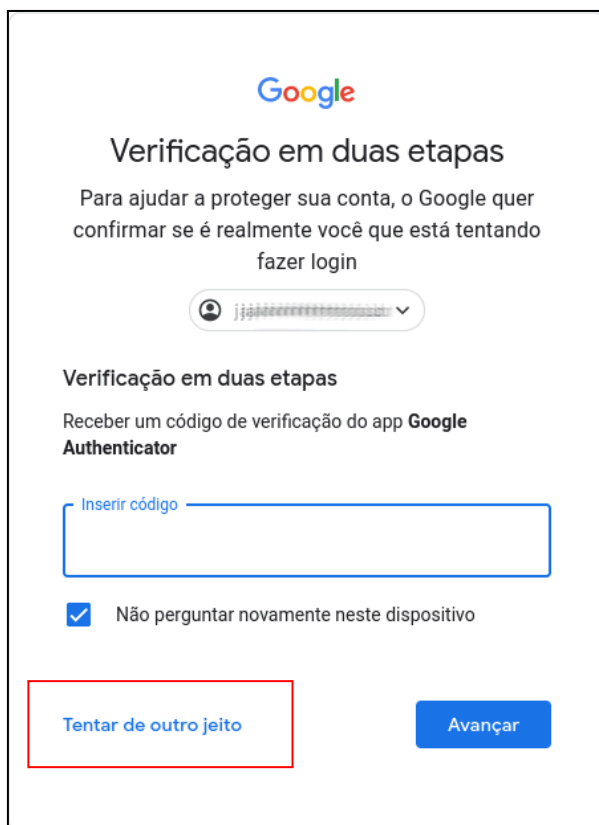
Imprimir códigos



Fazer o download dos códigos

5.2 Como utilizar?

5.2.1 Logue na sua conta de e-mail do domínio **tjma.jus.br** (conta corporativa), informe sua senha e no momento de inserir o código clique em **“Tentar de outro jeito”**.



Google

Verificação em duas etapas

Para ajudar a proteger sua conta, o Google quer confirmar se é realmente você que está tentando fazer login

Verificação em duas etapas

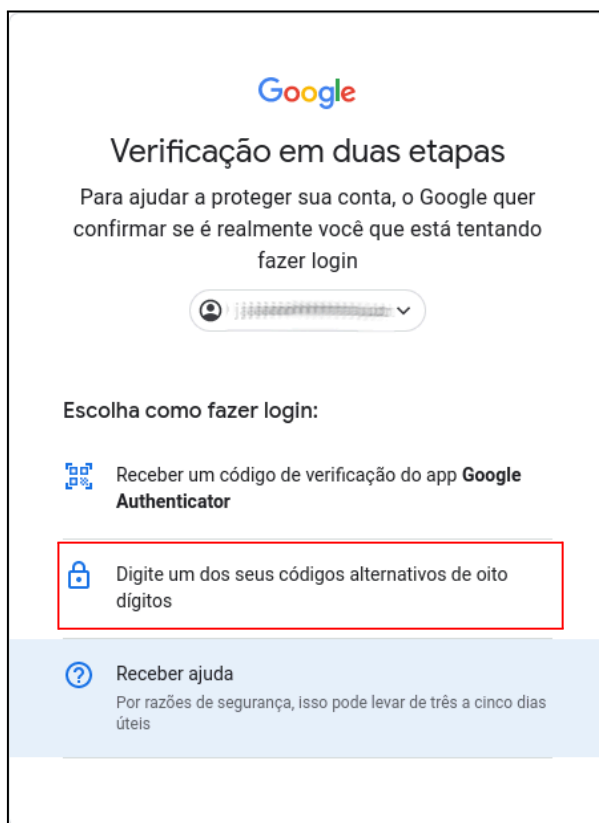
Receber um código de verificação do app **Google Authenticator**

Inserir código

☒ Não perguntar novamente neste dispositivo

[Tentar de outro jeito](#) [Avançar](#)

5.2.2 Clique em **“Digite um dos seus códigos alternativos de oito dígitos”** e informe um dos códigos de backup coletados anteriormente.





Google


Verificação em duas etapas

Para ajudar a proteger sua conta, o Google quer confirmar se é realmente você que está tentando fazer login

Escolha como fazer login:

 Receber um código de verificação do app **Google Authenticator**

 **Digite um dos seus códigos alternativos de oito dígitos**

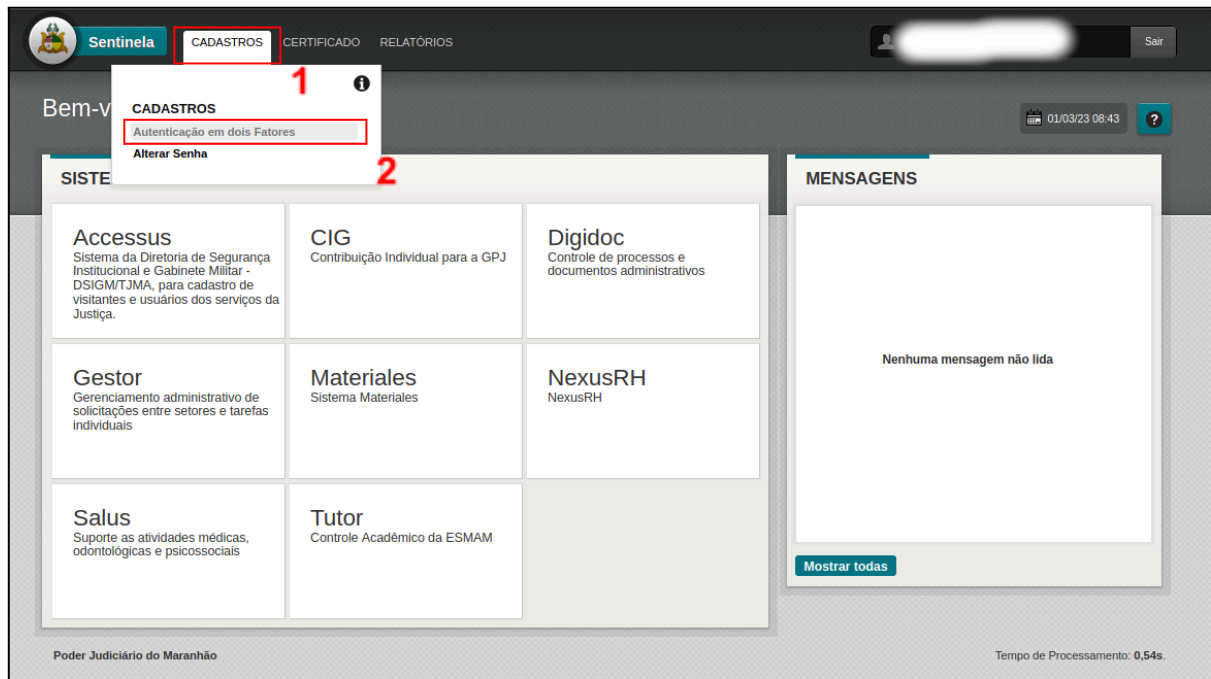
 **Receber ajuda**
Por razões de segurança, isso pode levar de três a cinco dias úteis

6. SENTINELA - GOOGLE AUTHENTICATOR

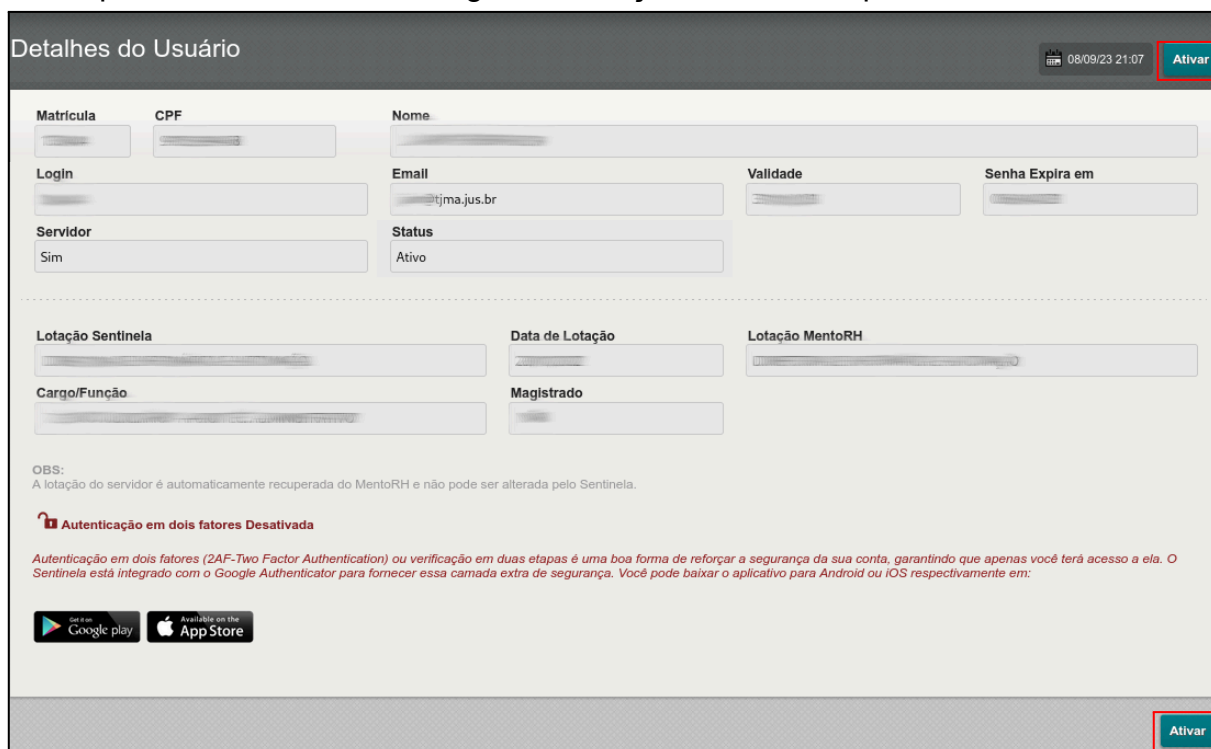
6.1 Como ativar?

6.1.1 Acesse e logue no sistema “SENTINELA” (<https://sistemas.tjma.jus.br/sentinela/>).

6.1.2 Selecione o menu “CADASTROS” e clique em “Autenticação em dois Fatores”.



6.1.3 Clique no botão “Ativar” e siga as instruções descritas apresentadas na tela.

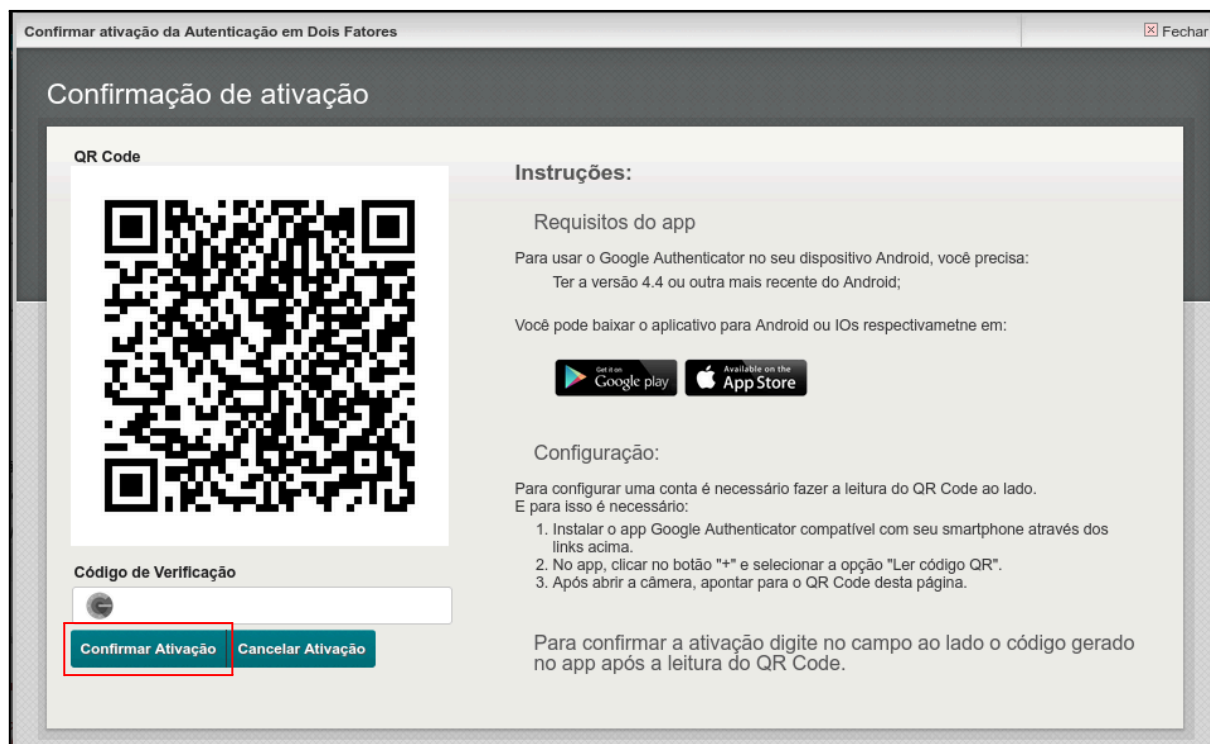


6.1.4 No dispositivo móvel (smartphone/celular) utilizando o aplicativo **“Google Authenticator”** (já instalado), toque em **“+”**.

a) Selecione **“Ler código QR”** ou **“Scan a QR Code”**.

b) Após abrir a câmera, aponte para o **“QR Code”** e faça a leitura do mesmo.

c) Informe o Código de Verificação e clique em **“Confirmar Ativação”**.



6.1.5 Após a ativação, clique em **“Mostrar Códigos de Recuperação”** para coletar os códigos de recuperação. Eles permitirão o acesso ao sistema SENTINELA em casos de problemas com o dispositivo móvel ou com o aplicativo "Google Authenticator". Após obter os códigos, anote-os cuidadosamente e guarde-os em um local seguro.

QR Code



Instruções:

Requisitos do app

Para usar o Google Authenticator no seu dispositivo Android, você precisa:

- Ter a versão 4.4 ou outra mais recente do Android;

Configuração:

Para configurar uma conta é necessário fazer a leitura do QR Code ao lado. E para isso é necessário:

1. Instalar o app Google Authenticator compatível com seu smartphone através dos links acima.
2. No app, clicar no botão "+" e selecionar a opção "Ler código QR".
3. Após abrir a câmera, apontar para o QR Code desta página.

As configurações serão armazenadas automaticamente.

O app gera um novo código de confirmação a cada 30 segundos. Esse é o tempo que ele estará disponível para uso.

Esse código será solicitado após o login com seu usuário e senha, caso a Autenticação em Duas Etapas esteja ativada.

Caso o app de autenticação não esteja disponível por qualquer motivo você pode usar um código único de recuperação.

[Mostrar Códigos de Recuperação](#)

6.1.6 Ativação finalizada.

6.1.7 Ao acessar novamente o sistema **"SENTINELA"**, insira o código gerado pelo aplicativo do **"Google Authenticator"**. Se este for um dispositivo confiável, selecione **'Não perguntar novamente neste dispositivo pelos próximos 120 dias'**.



SENTINELA
Verificação em duas etapas

Esta etapa extra mostra que é realmente você que está tentando fazer login

☐ Não perguntar novamente neste dispositivo pelos próximos 120 dias.

Entrar

Caso esteja sem acesso ao Google Authenticator no momento, use um dos Códigos de Recuperação.

Os aplicativos são homologados para execução em Mozilla Firefox e Google Chrome

ÚLTIMOS AVISOS

06
11/2023

Convidamos cordialmente você, servidor(a), a habilitar a autenticação em duas etapas (2FA) em sua conta de e-mail corporativa para acessar o sistema.

⚠ O **dispositivo mencionado** está relacionado ao navegador e não ao computador utilizado. Se mais de um navegador for usado para acessar o sistema **"SENTINELA"**, a mesma pergunta poderá ocorrer novamente. A repetição dessa pergunta também poderá surgir após a limpeza de cache e de cookies do(s) navegador(es).

7. SOLUÇÃO DE PROBLEMAS

Caso a ativação da 2FA no sistema “**SENTINELA**” utilizando o “**Google Authenticator**” não funcione como esperado, siga as dicas abaixo:

7.1 Solução 01

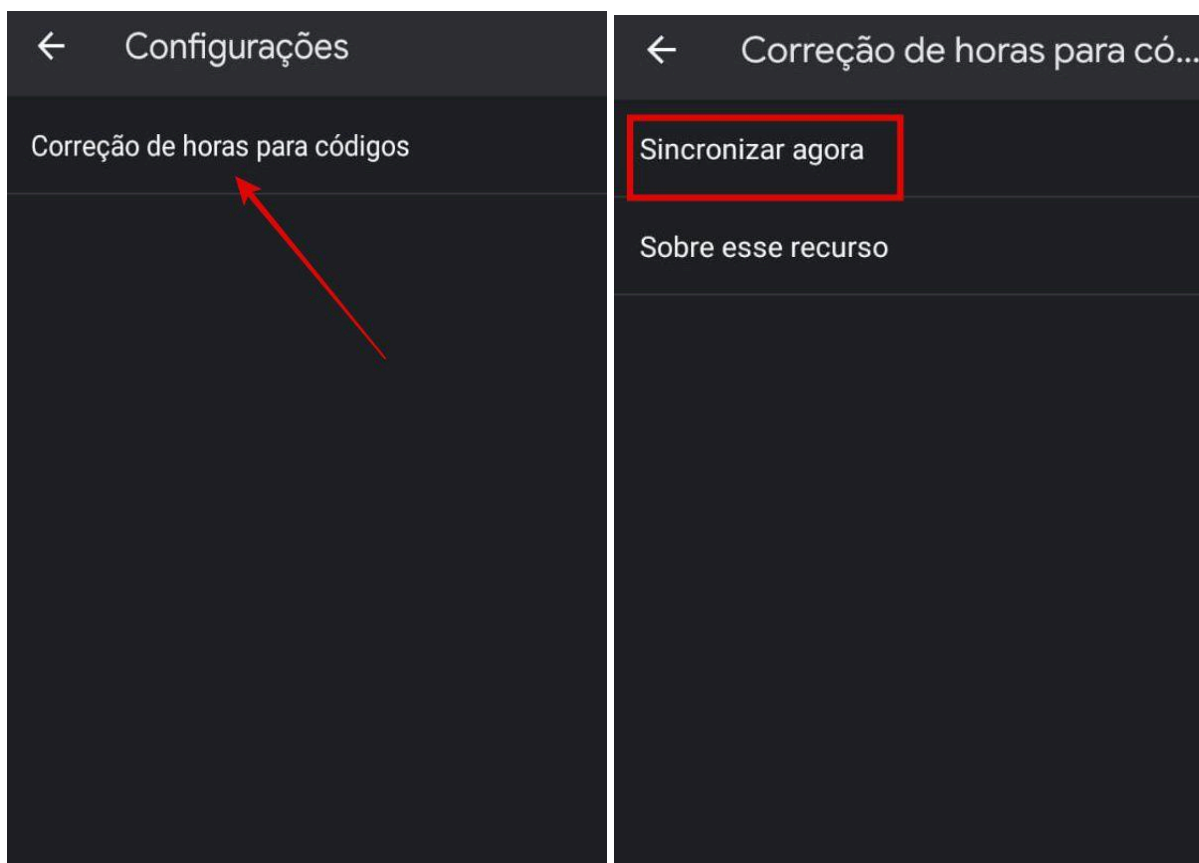
7.1.1 Utilize navegador (chrome/firefox/safari/edge) no modo anônimo, também conhecido como aba ou janela anônima, para realizar o procedimento.

7.2 Solução 02

7.2.1 Acesse o aplicativo “**Google Authenticator**”.

7.2.2 Localize “**Configurações/Settings**” e clique.

7.2.3 Selecione “**Correção de horas para códigos/Time correction for codes**” e clique em “**Sincronizar agora/Sync now**”.



7.3 Solução 03

7.3.1 Navegue até o menu “**Configurações/Settings**” do seu dispositivo móvel (smartphone/celular).

7.3.2 Vá até a opção “**Aplicativos/APP**” e clique em “**Gerenciar Apps/Apps Settings**”.

7.3.3 Localize o “**App Google Authenticator**” e clique.

7.3.4 Localize a opção “**Forçar Parada/Force stop**” e clique.

7.3.5 Localize a opção “**Armazenamento e Cache/Storage**” e clique em Limpar Cache/Clear cache.

⚠ **NÃO** execute a opção “**Limpar dados/Clear data**” sob pena de **DELETAR TODOS** os registros do aplicativo “**Google Authenticator**” existentes.

⚠ Se ocorrer um erro, ainda no aplicativo “**Google Authenticator**” selecione o registro criado e remova-o, clicando na lixeira para exclusão. Execute novamente as dicas acima na mesma ordem. **NÃO remova o aplicativo.**

8. FAQ

⚠ Caso você tenha alguma dúvida ou precise de assistência técnica durante o processo de cadastro da autenticação em duas etapas, entre em contato com a **Coordenação de Atendimento ao Usuário (CAU)** pelos canais oficiais de comunicação do TJMA.

8.1 Dúvidas conceituais

8.1.1 O que é autenticação em duas etapas (2FA)?

A autenticação em duas etapas (2FA), originária do inglês "**two-factor authentication**", também conhecida como verificação em duas etapas ou autenticação de dois fatores é uma camada extra de proteção ativada em contas de serviços online, que requer uma segunda verificação de identidade do(a) usuário(a) no momento do acesso.

8.1.2 Qual a importância da 2FA?

A autenticação em duas etapas (2FA) é vital para proteger dados online. Ela adiciona uma camada extra de segurança, dificultando invasões, sendo essencial para ambientes digitais mais seguros.

8.1.3 Onde posso usar a 2FA?

A autenticação em duas etapas está disponível para diversos serviços online, como bancos, sítios eletrônicos de compras on-line (Amazon, PayPal, Google Play), serviços de e-mail (Gmail, Microsoft, Yahoo, Outlook), redes sociais (Facebook, Instagram, LinkedIn, Tumblr, Twitter, Snapchat, etc.), entre outros.

8.1.4 A autenticação em duas etapas (2FA) é segura?

Sim, a 2FA é segura. Essa medida de segurança adiciona uma camada extra de segurança, dificultando significativamente o acesso não autorizado à sua conta, mesmo que tenham conhecimento da senha.

8.1.5 A autenticação em duas etapas (2FA) é a prova de falhas?

Não, a 2FA é eficaz para reforçar a segurança de contas online, mas nenhum sistema é completamente à prova de falhas. Sua eficácia depende, em parte, da implementação correta e do cuidado do(a) usuário(a) ao gerenciar suas credenciais.

8.1.6 Existem níveis de segurança para o uso da 2FA?

Sim, existem diferentes níveis de segurança associados ao uso da autenticação em duas etapas (2FA). A eficácia da 2FA pode variar dependendo dos métodos escolhidos. **Nível Baixo de Segurança:** Verificação por SMS ou Chamada Telefônica. **Nível Intermediário de Segurança:** Solicitações do Google ou Autenticação Push. **Nível Alto de Segurança:** Aplicativos Autenticadores (Google Authenticator, etc.). **Segurança Adicional:** Chaves de Segurança Físicas (tokens USB ou NFC).

8.1.7 Quais métodos de 2FA o Poder Judiciário do Estado do Maranhão (PJMA) utiliza?

Verificação por SMS ou Chamada Telefônica, Aplicativos Autenticadores (utilizando o Google Authenticator), Códigos de Backup e Solicitações do Google.

8.1.8 Qual é o método de autenticação mais indicado para utilizar no Poder Judiciário do Estado do Maranhão (PJMA)?

O método mais indicado é o Google Authenticator, proporcionando segurança adicional ao gerar códigos temporários para proteger o acesso ao e-mail corporativo e ao sistema SENTINELA.

8.1.9 Todos(as) do PJMA devem habilitar a 2FA?

Sim, é crucial que todos(as) os(as) usuários(as), incluindo unidades administrativas e judiciais, habilitem a 2FA no e-mail corporativo e no sistema SENTINELA.

8.2 Dúvidas do método “Verificação por SMS ou Chamada Telefônica”

8.2.1 Por que a “verificação por SMS ou chamada telefônica” é considerada um método menos seguro para autenticação em duas etapas (2FA)?

A “verificação por SMS ou chamada telefônica” é classificada como um método de Nível Baixo de Segurança devido a vulnerabilidades específicas. Esse método é suscetível à exploração por invasores habilidosos, tornando-o menos seguro.

8.2.2 Quais são as vulnerabilidades associadas à “verificação por SMS”?

a) Ataques de troca de SIM: Invasores podem transferir seu número de telefone para outro cartão SIM, assumindo o controle das mensagens SMS.

b) Phishing ou Smishing: Ataques de phishing podem levar à divulgação involuntária de códigos por SMS.

c) Interceptação de mensagens: A possibilidade de interceptação de mensagens SMS, especialmente em redes sem fio não seguras.

8.2.3 Por que a “verificação por chamada telefônica” também pode ser vulnerável?

a) Reprodução de voz: Alguns ataques podem envolver a gravação e reprodução de uma voz autorizada para enganar o sistema.

b) Interceptação de chamadas: Similar à interceptação de mensagens, chamadas telefônicas também podem ser interceptadas.

8.2.4 É recomendável evitar o uso da verificação por SMS ou chamada telefônica?

Sim, este método deve ser utilizado apenas como a primeira etapa da autenticação em duas etapas. Recomenda-se migrar para o Google Authenticator posteriormente, pois é o método padrão do TJMA e que oferece maior segurança.

8.2.5 O que fazer se eu for vítima de um ataque relacionado à “verificação por SMS ou chamada telefônica”?

Se você enfrentar problemas de segurança após utilizar a “verificação por SMS ou chamada telefônica”, especialmente se tiver ignorado o método seguro de autenticação recomendado neste manual, e suspeitar de atividades maliciosas em sua conta, entre em contato imediatamente com a Coordenação de Atendimento ao Usuário (CAU). Não ignore os métodos seguros recomendados inicialmente. Além disso, é crucial atualizar suas configurações de segurança imediatamente e priorizar a migração para métodos mais seguros, como autenticadores de aplicativos, a exemplo do Google Authenticator.

8.2.6 Quais alternativas mais seguras à verificação por SMS ou chamada telefônica?

Para uma autenticação mais segura, o uso do Google Authenticator é altamente recomendado. Ele oferece uma segurança robusta e é o padrão adotado pelo Tribunal de Justiça do Estado do Maranhão.

8.3 Dúvidas do método “Google Authenticator”

8.3.1 O que é Google Authenticator e por que devo utilizá-lo?

O Google Authenticator é um aplicativo de autenticação em duas etapas (2FA) que gera códigos temporários e aleatórios, complementando a senha para acessar uma conta. Esse é o método recomendado pela DIA para acessar o e-mail corporativo e o sistema SENTINELA.

8.3.2 Como configurar o Google Authenticator em minha conta de e-mail corporativo?

Baixe e instale o Google Authenticator na loja de aplicativos do seu dispositivo (smartphone) móvel e siga os passos detalhados no tópico 3 deste manual.

8.3.3 Como configurar o Google Authenticator no sistema SENTINELA?

Baixe e instale o Google Authenticator na loja de aplicativos do seu dispositivo (smartphone) móvel e siga os passos detalhados no tópico 6 deste manual.

8.3.4 Posso usar o Google Authenticator em vários dispositivos (smartphones)?

O Google Authenticator está vinculado ao dispositivo em que foi inicialmente configurado. Para utilizá-lo em vários dispositivos, é necessário configurá-lo individualmente em cada um, seguindo as orientações detalhadas no item 3.3 deste manual.

8.3.5 O que fazer se eu perder meu dispositivo (smartphone) com o Google Authenticator?

Em caso de perda do dispositivo com o Google Authenticator, é recomendável utilizar os códigos de backup salvos, armazenados em um local seguro. Além disso, registre um boletim de ocorrência imediatamente e comunique a Diretoria de Informática e Automação (DIA) para proceder com a desvinculação do dispositivo e outras providências.

8.3.6 Como obtenho códigos de backup da minha conta corporativa?

Para obter os códigos de backup, siga os passos detalhados no tópico 5 deste manual. Guarde esses códigos em um local seguro, pois eles podem ser usados em caso de perda do dispositivo.

8.3.7 Os códigos do Google Authenticator expiram?

Sim, os códigos gerados pelo Google Authenticator são temporários e têm um tempo de validade curto, geralmente em torno de 30 segundos. Após esse período, um novo código é gerado.

8.3.8 Posso usar o Google Authenticator em serviços além do Google?

Sim, muitos serviços online oferecem suporte ao Google Authenticator para 2FA. Você pode configurá-lo em várias contas, como redes sociais, serviços de e-mail e outros que adotam esse método de segurança.

8.3.9 Posso desativar a autenticação em duas etapas (2FA) se decidir não usá-la mais?

Sim, em muitos serviços, é possível desativar a autenticação em duas etapas. No entanto, é altamente recomendável manter essa camada de segurança ativada para garantir a integridade da sua conta. A desativação pode comprometer a segurança do acesso ao seu e-mail corporativo ou ao sistema SENTINELA. Caso seja necessário, verifique neste manual como reativar a 2FA.

8.4 Dúvidas do método “Solicitações do Google”

8.4.1 Por que a verificação por “Solicitações do Google” é considerada um método de Nível Intermediário de Segurança?

A verificação por “Solicitações do Google”, que envolve o envio de notificações para dispositivos conectados, é considerada um método de Nível Intermediário de segurança devido a certas vulnerabilidades e riscos associados.

8.4.2 Quais são as vulnerabilidades potenciais da verificação por “Solicitação do Google”?

a) Phishing de solicitação: pessoas podem criar solicitações falsas para enganar os(as) usuários(as), levando-os a aprovar a autenticação sem intenção.

b) Acesso não autorizado a dispositivos conectados: Se um dispositivo estiver desprotegido, alguém com acesso físico a esse dispositivo pode aprovar solicitações fraudulentas.

8.4.3 Como a autenticação “Solicitações do Google” funciona?

A autenticação por “Solicitações do Google” envia uma notificação para um dispositivo previamente autenticado, solicitando a aprovação da tentativa de login. O(A) usuário(a) precisa confirmar a autenticação através do dispositivo conectado.

8.4.4 O que os(as) usuários(as) devem considerar ao optar pela verificação por “Solicitações do Google”?

a) Segurança do dispositivo conectado: Garantir que os dispositivos conectados estejam seguros e protegidos contra acesso não autorizado.

b) Consciência de solicitações suspeitas: Estar atento a solicitações inesperadas ou suspeitas para evitar a aprovação involuntária.

8.4.5 Como reforçar a segurança ao usar a verificação por “Solicitações do Google”?

a) Ativar PIN ou autenticação biométrica: Reforçar a segurança do dispositivo conectado com PINs ou autenticação biométrica.

b) Configurar notificações seguras: Certificar-se de que as notificações do Google sejam enviadas de maneira segura e autenticada.

8.4.6 O que fazer se eu suspeitar de uma solicitação fraudulenta ou de atividade suspeita na verificação por “Solicitações do Google”?

Se suspeitar de atividades suspeitas, recuse a aprovação da solicitação seguindo as instruções no aplicativo. Além disso, troque imediatamente sua senha para garantir a segurança da sua conta. Entre em contato imediatamente com a Coordenação de Atendimento ao Usuário (CAU) para relatar a suspeita e obter assistência.