

MÚLTIPLO FATOR DE AUTENTICAÇÃO (MFA) - EMAIL



**PODER JUDICIÁRIO
DO ESTADO DE RORAIMA**

Secretaria de Tecnologia
da Informação

O QUE É MÚLTIPLO FATOR DE AUTENTICAÇÃO?

Múltiplo Fator de Autenticação (MFA) é uma medida de segurança que adiciona uma camada extra ao processo de autenticação de usuários em sistemas online, exigindo dois elementos distintos, como senha e um dispositivo móvel, para verificar a identidade.

Essa prática, cada vez mais comum, dificulta ataques de invasores, mesmo que tenham a senha, pois o segundo fator muda regularmente. Isso reduz significativamente o risco de acesso não autorizado e protege informações críticas. Em linha com essa preocupação, o Conselho Nacional de Justiça (CNJ), por meio da Portaria Presidência nº 140/2024, estabelece a adoção do MFA como requisito para acesso a sistemas judiciais sensíveis, visando fortalecer a segurança tanto para usuários internos quanto externos.



COMO HABILITAR O ACESSO UTILIZANDO MÚLTIPLO FATOR DE AUTENTICAÇÃO NO SMARTPHONE?



É importante ressaltar que após a configuração do múltiplo fator de autenticação, você passará a fazer login na sua conta utilizando sua senha e seu smartphone. **Com essa implementação, sempre que houver uma tentativa de acesso a sua conta, o seu dispositivo configurado será notificado, alertando-o da ocorrência.**

Pronto ! Agora podemos iniciar a configuração.



Passo 01:

Certifique de que a opção de Data e hora automáticas esteja ativada em seu smartphone.

Continuação na próxima página



BAIXANDO GMAIL E GOOGLE AUTHENTICATOR

Passo 02: Acesse o aplicativo Gmail pelo smartphone usando seu e-mail institucional com a terminação @tjrr.jus.br.



Caso não possua, baixe na loja se aplicativos **Play Store** (para usuários de android) e **App Store** (Para usuários de IOS).

Passo 03: Baixe o aplicativo Google Authenticator em seu Smartphone.



Estará representado pelo seguinte ícone

Baixe na Play Store ou App Store. Basta pesquisar por **Google Authenticator**.

Continuação na próxima página



CONFIGURANDO O GOOGLE AUTHENTICATOR



Passo 04: Abra o aplicativo Google Authenticator em seu smartphone.

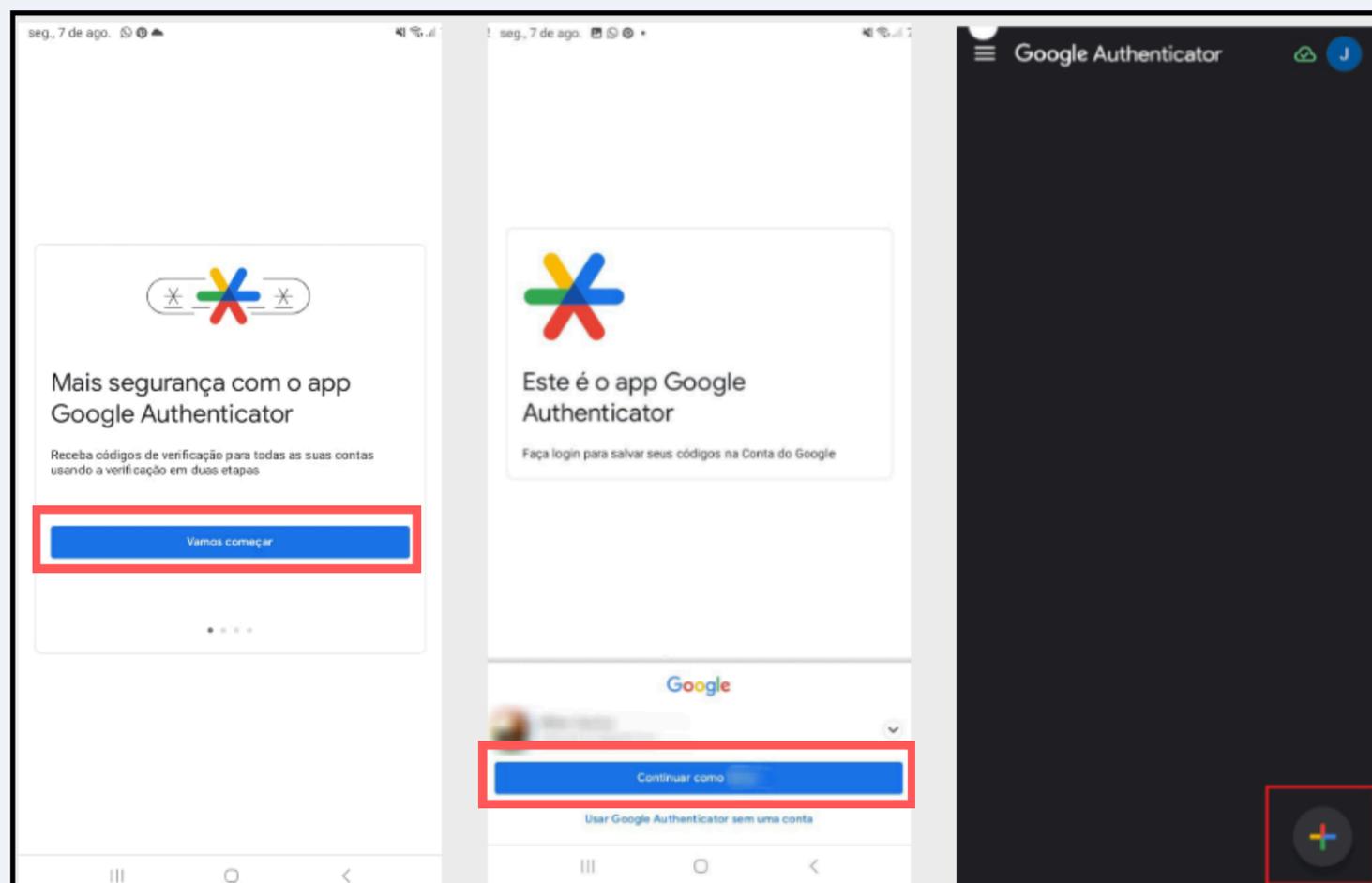


Imagem 01

Imagem 02

Imagem 03

- 1 Clique em **Vamos Começar** (Imagem 01).
- 2 Conforme a Imagem 02, selecione a sua conta institucional do TJRR.
- 3 Você será direcionado para a tela principal do aplicativo, conforme o exemplo da Imagem 03.

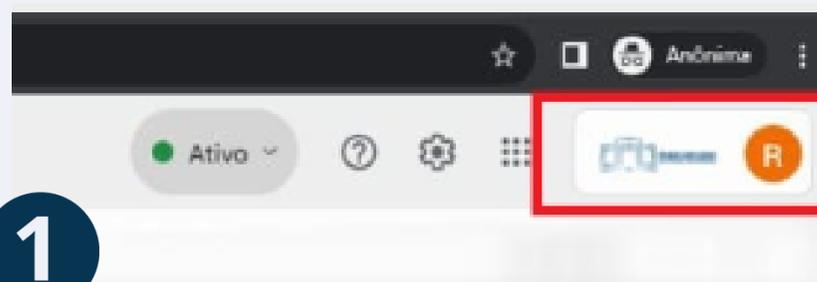
Continuação na próxima página



CONFIGURANDO O E-MAIL

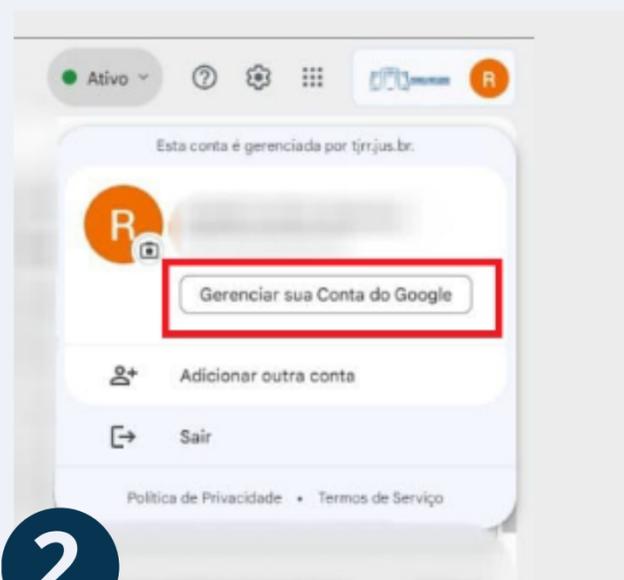


Passo 05: Acesse sua conta institucional (@tjrr.jus.br) do Gmail no computador.



1

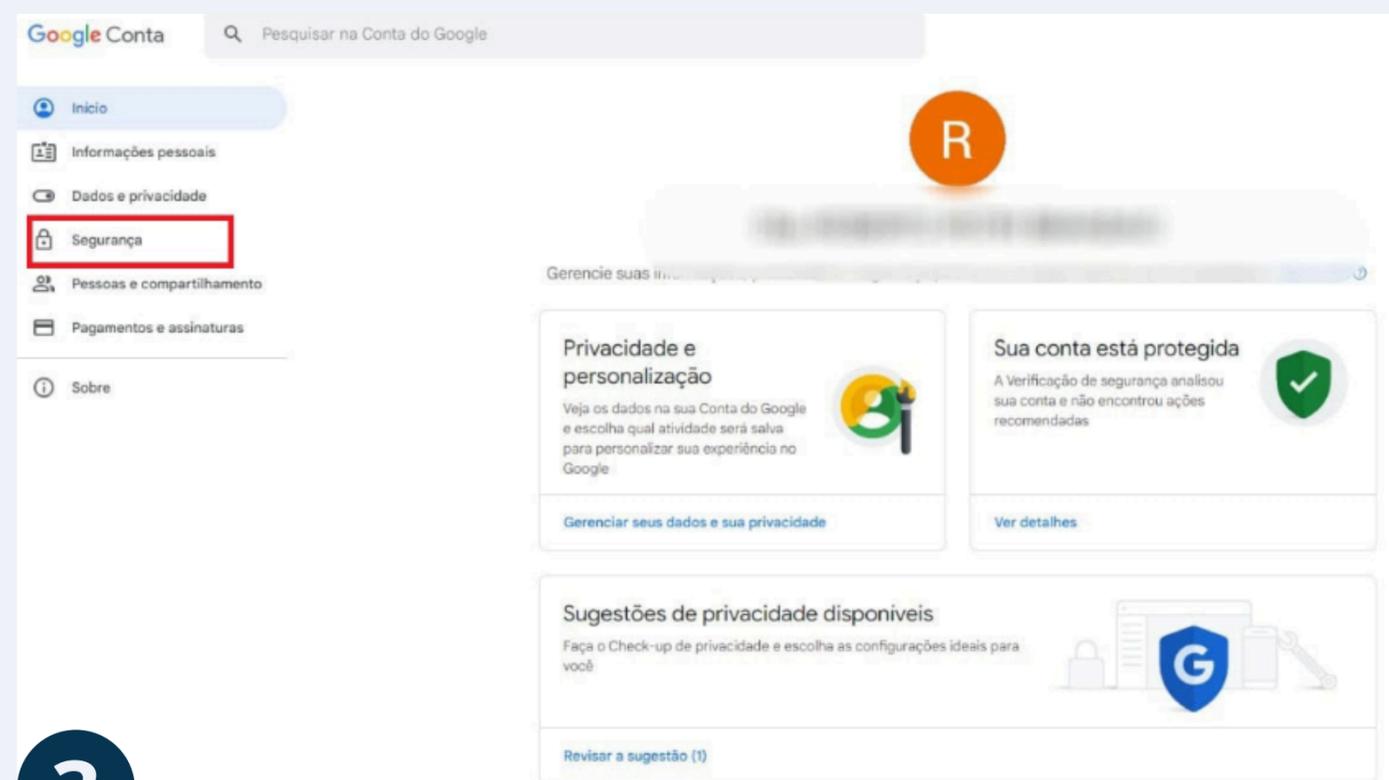
Clique no ícone conforme a imagem acima.



2

Clique em **Gerenciar sua Conta do Google**.

3



Clique em **Segurança**.

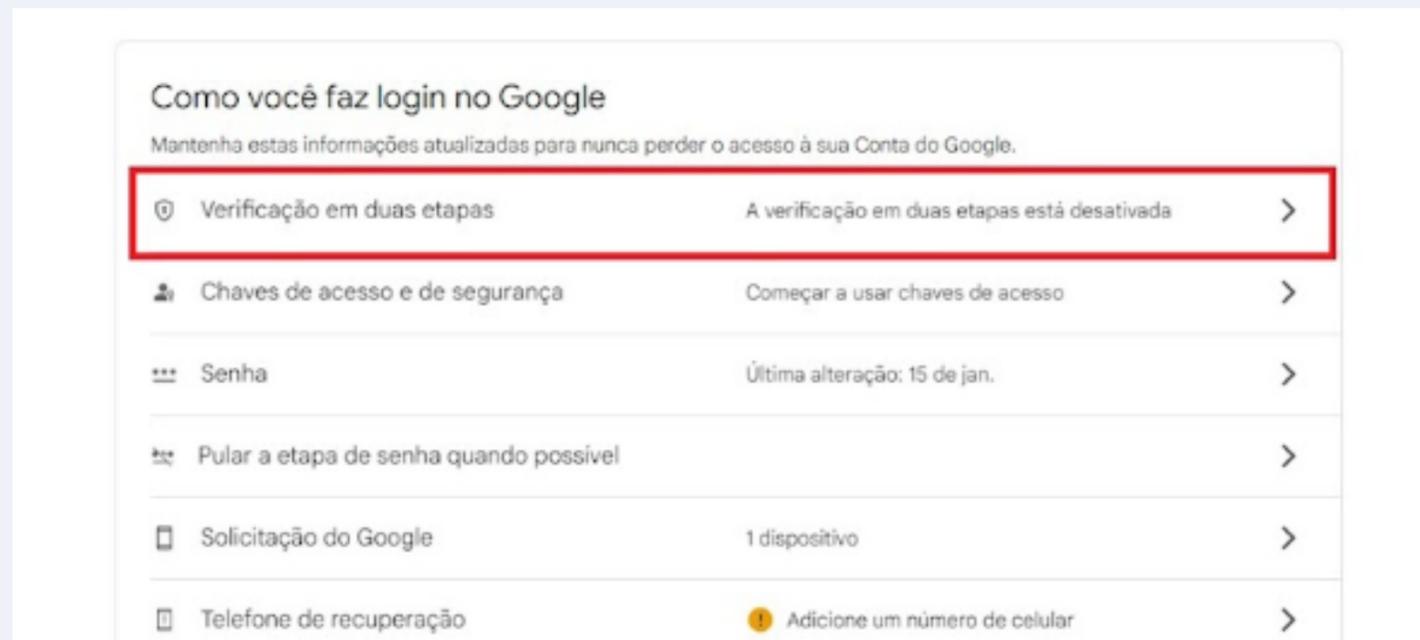
Continuação na próxima página



CONFIGURANDO O E-MAIL

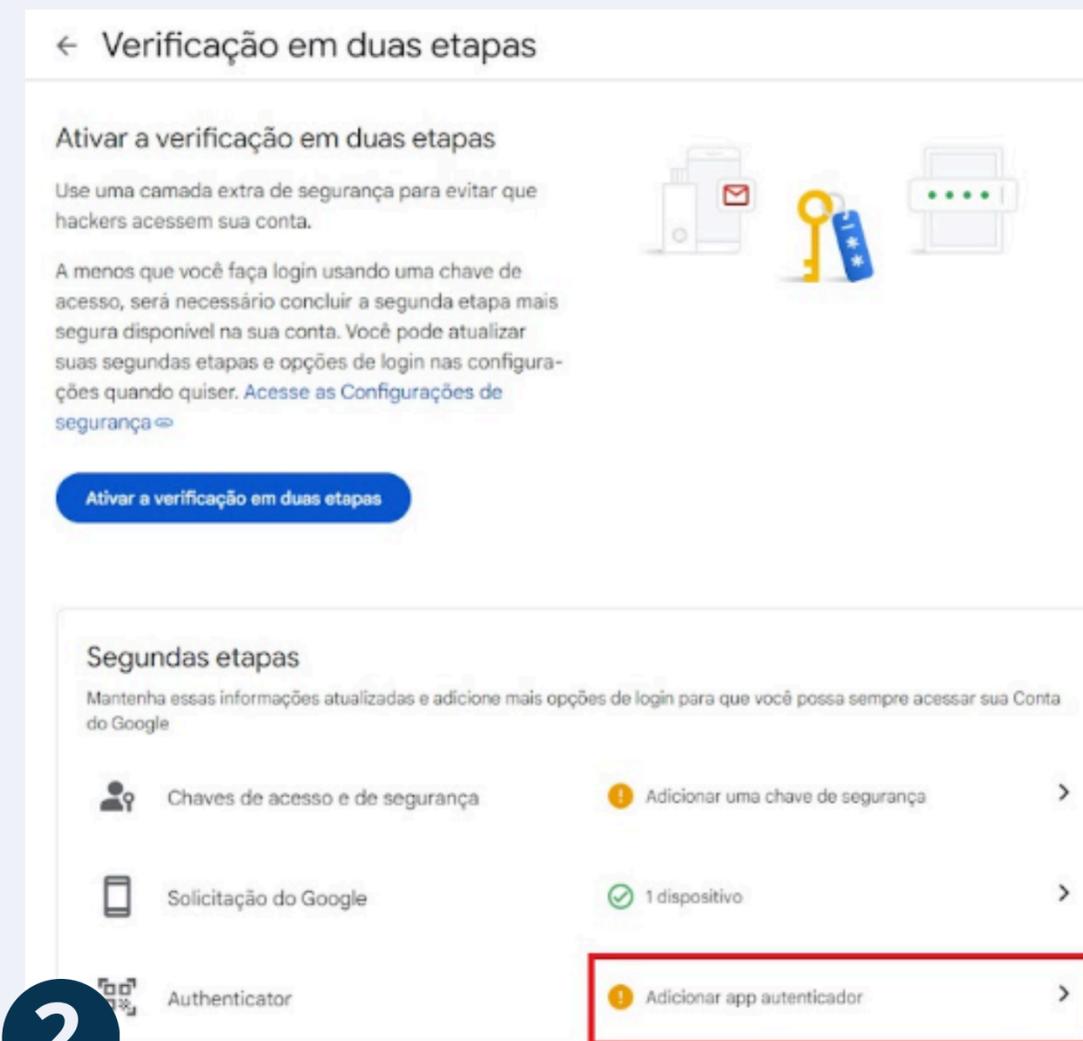


Passo 06: Na mesma página de **Segurança**. Localize e clique na sessão **“Verificação em duas etapas”**, conforme a Imagem abaixo.



1

Atenção: Pode ser necessário confirmar suas credenciais neste momento.



Clique em **Adicionar app autenticador**.

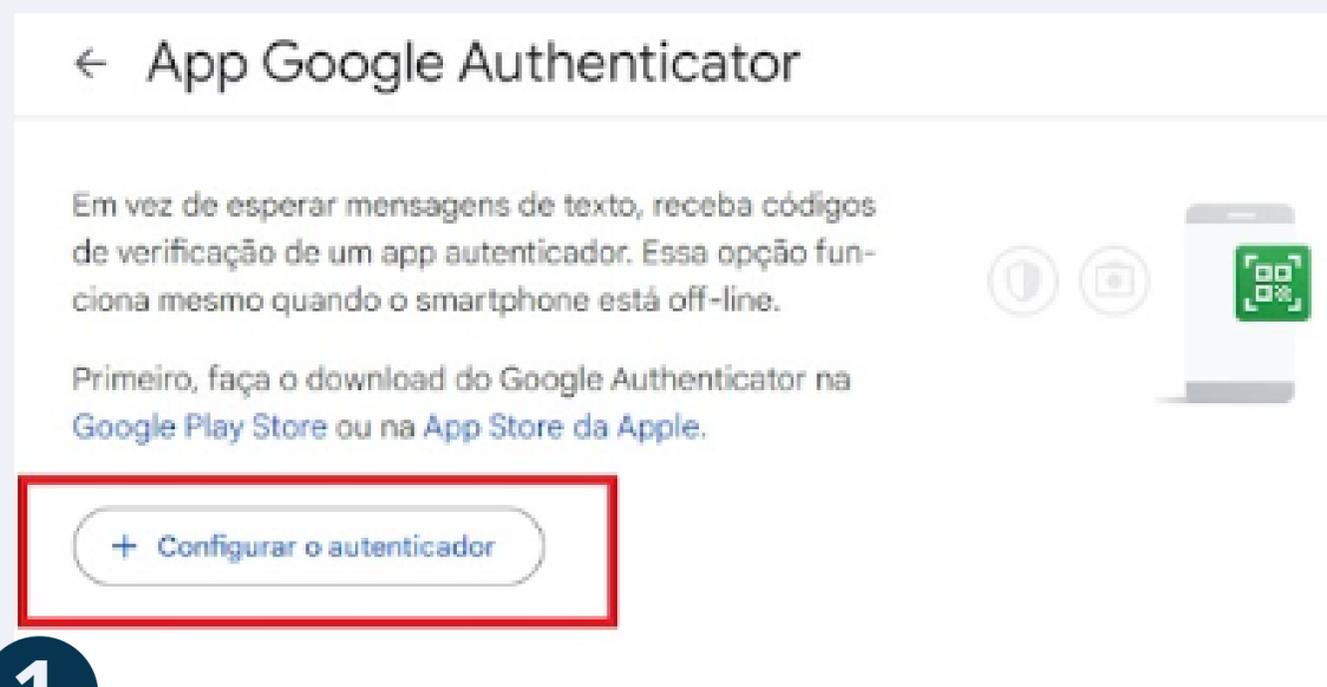
Continuação na próxima página



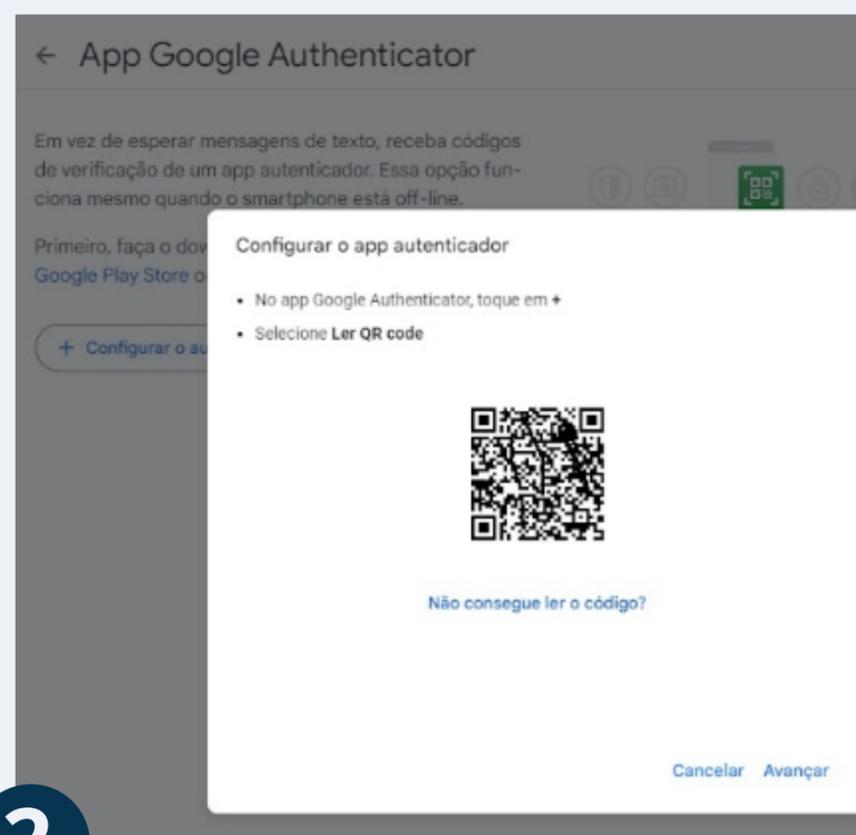
CONFIGURANDO O E-MAIL



Passo 07: Clique no campo "**+ Configurar o autenticador**", conforme a Imagem abaixo.



1



2

Neste passo, será apresentado um código (QR code), conforme a Imagem ao lado. Abra o aplicativo Google Authenticator em seu smartphone.

Continuação na próxima página



CONFIGURANDO O E-MAIL



Passo 08: Para dar continuidade ao Passo 07, abra o aplicativo GOOGLE AUTHENTICATOR no celular e siga os passos abaixo.



Imagem 01

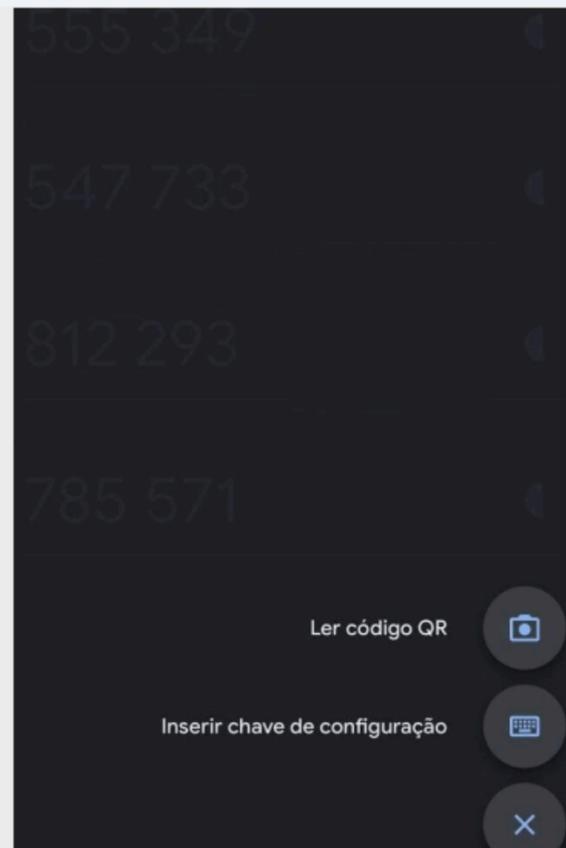


Imagem 02

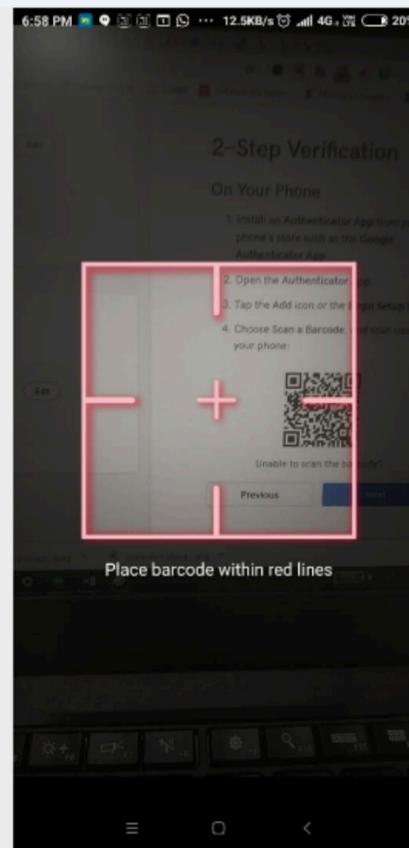


Imagem 03

- 1 *Clique na opção + (Imagem 01).*
- 2 *Clique em Ler código QR (Imagem 02).*
- 3 *Digitalize o código QR, que foi gerado no navegador, conforme o **Passo 07** e Imagem 03.*

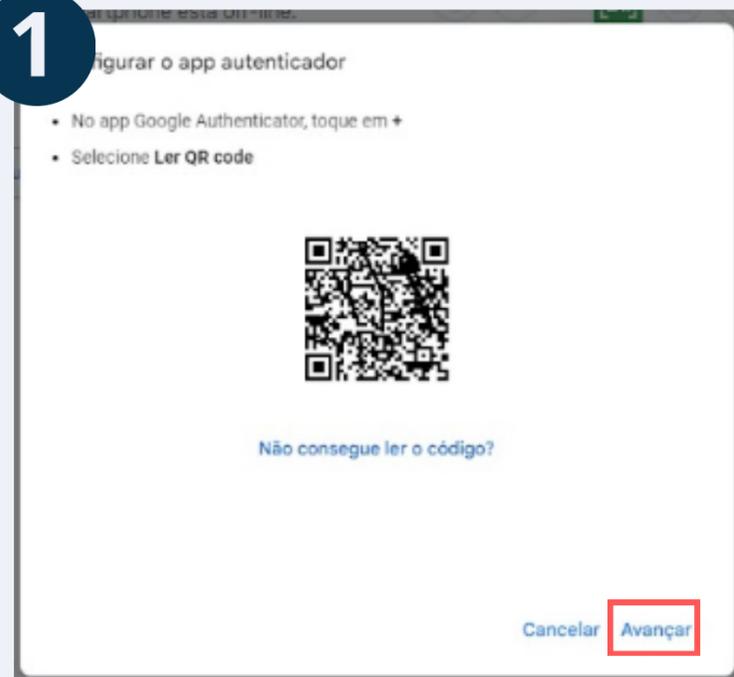
Continuação na próxima página



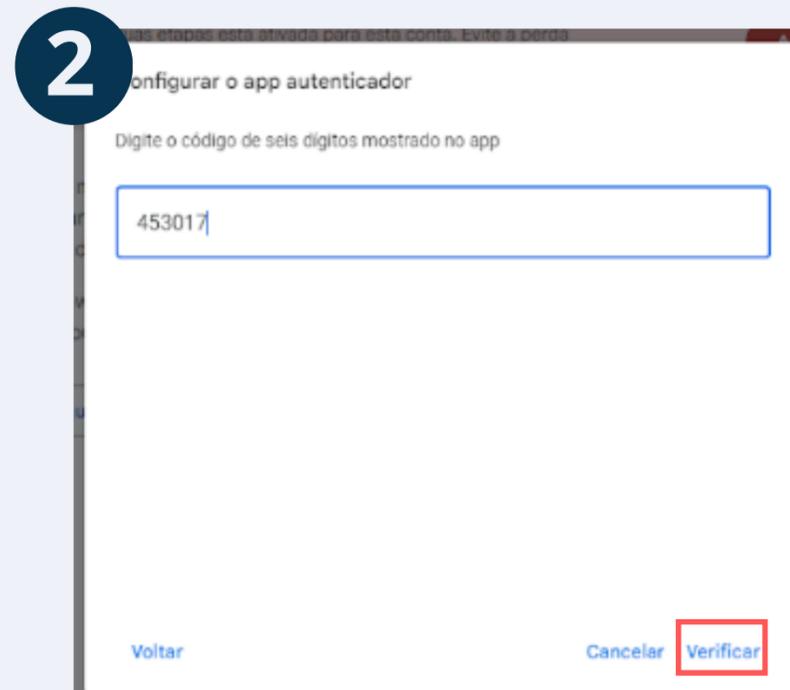
CONFIGURANDO O E-MAIL



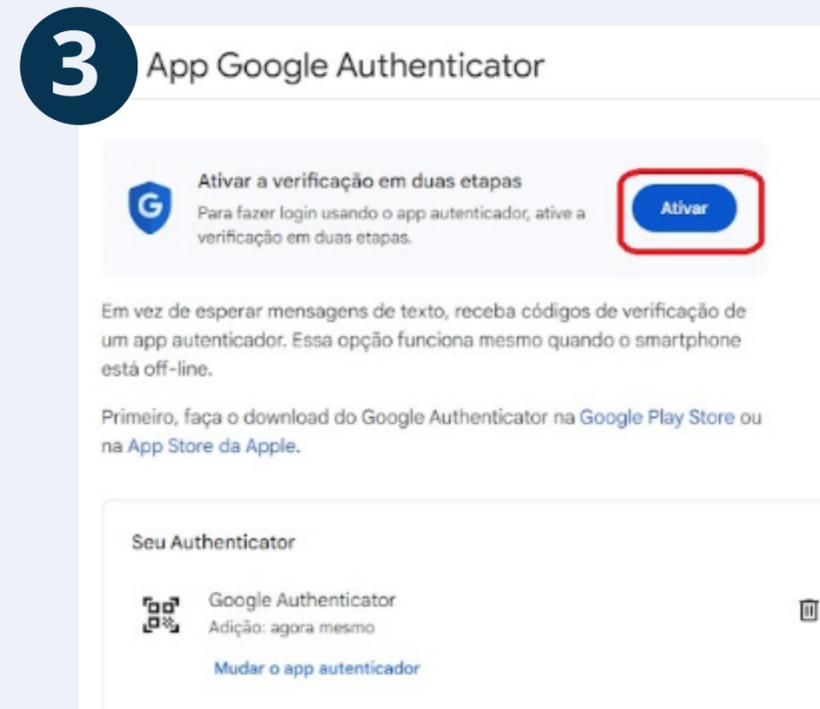
Passo 09: Após a leitura, clique em Avançar no computador/Navegador e, logo em seguida, insira o código numérico de seis dígitos, gerado no aplicativo autenticador, no campo indicado.



Após a leitura do QR clique em **Avançar**.



Insira o código de 6 dígitos gerado no aplicativo Google Authenticator e clique em **Verificar**.



Após configurar o seu Autenticador, clique no botão **"Ativar"**.

O app autenticador foi configurado

Continuação na próxima página



CONFIGURANDO O E-MAIL

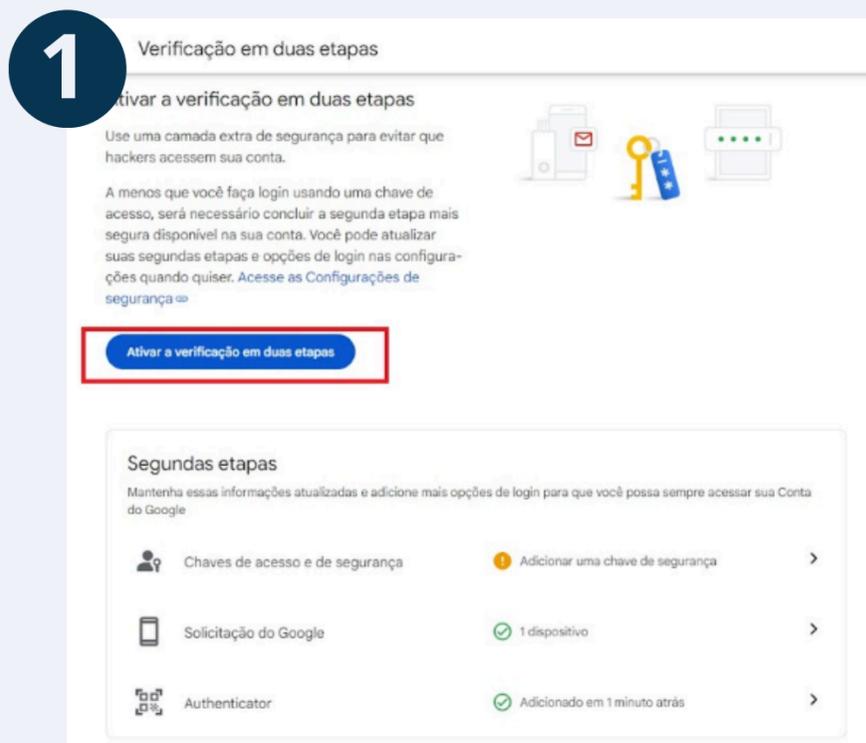


Passo 10: Agora que você configurou dois métodos de autenticação (Solicitações do Google e Authenticator), ative a verificação em duas etapas clicando no botão "**Ativar a verificação em duas etapas**".

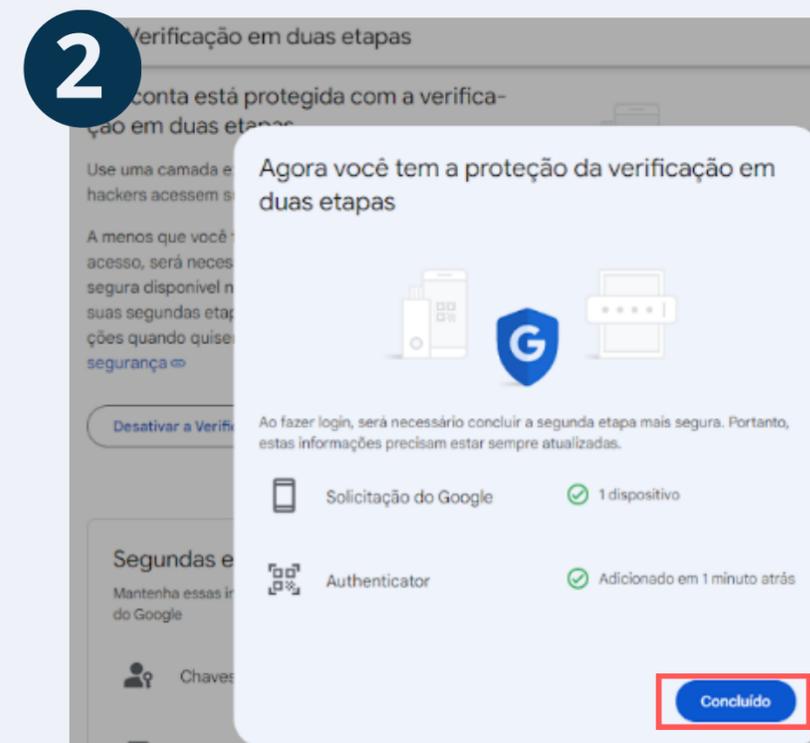


Finalizamos!

Agora, seu acesso ao e-mail institucional está ainda mais seguro.



Clique no ícone azul (**Ativar a verificação em duas etapas**).



Após seguir os passos indicados, uma tela de confirmação da verificação em duas etapas será exibida no seu computador/navegador, mostrando as duas formas de autenticação ativadas.

Continuação na próxima página



ACESSANDO O GMAIL APÓS ATIVAÇÃO DO MFA



Passo 11: Para acessar sua conta, digite o e-mail no campo designado e clique em "**Avançar**", conforme a imagem abaixo.

1

Passo 12: Insira a senha referente a sua conta Google no campo "**Digite sua senha**", e clique em "**Avançar**".

2

Continuação na próxima página



ACESSANDO O GMAIL APÓS ATIVAÇÃO DO MFA



Importante: Após inserir a senha, você receberá instruções sobre como proceder com a autenticação. Se sua conta estiver logada em um smartphone Android, analise e clique na notificação recebida. Caso esteja utilizando um iPhone, abra o aplicativo Gmail.

1

Verificação em duas etapas

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

@tjrr.jus.br



Verifique seu Galaxy A32

O Google enviou uma notificação para seu Galaxy A32. Toque em Sim na notificação para confirmar sua identidade.

Não perguntar novamente neste dispositivo

Reenviar

Tentar de outro jeito



Atenção: Marcando a opção "Não perguntar novamente neste dispositivo", conforme a imagem ao lado, você não receberá mais solicitações de múltiplo fator de autenticação neste aparelho.

Procedimento no Smartphone



2



Acesse seu smartphone e clique em "Sim, sou eu".

Atenção: Caso não seja você que esteja realizando o acesso à sua conta, clique em "Não, não permitir".



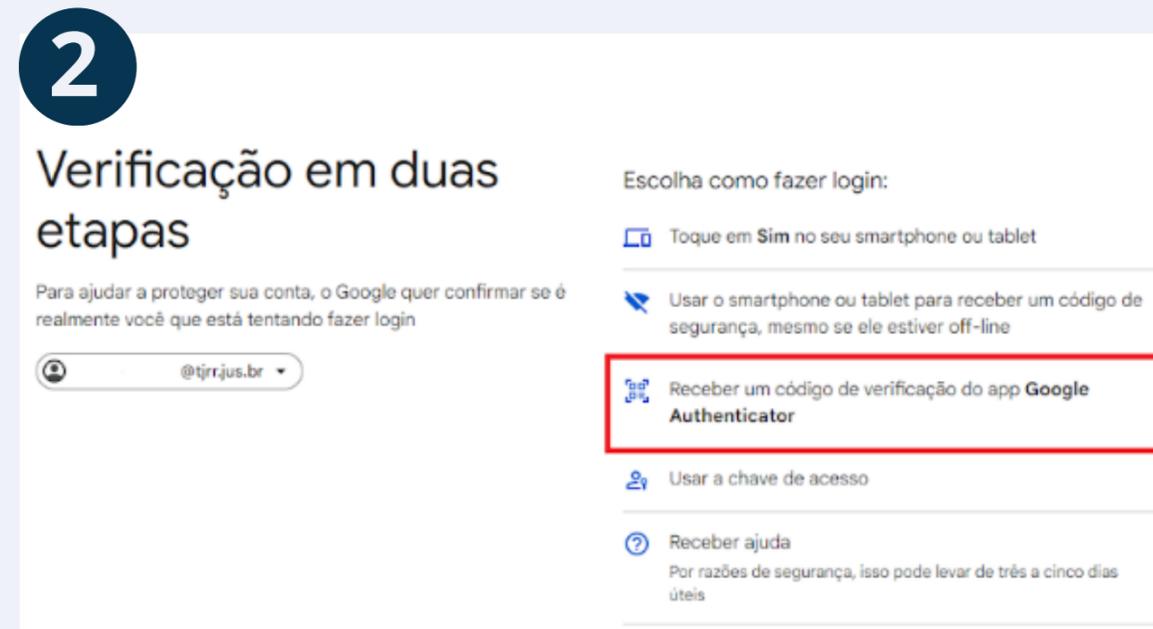
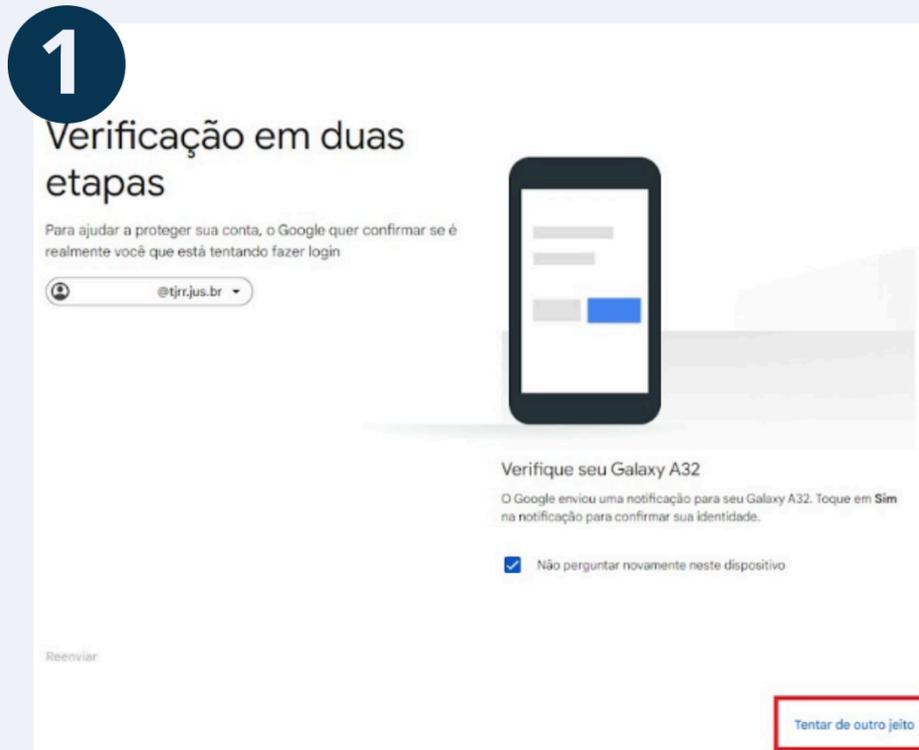
Continuação na próxima página



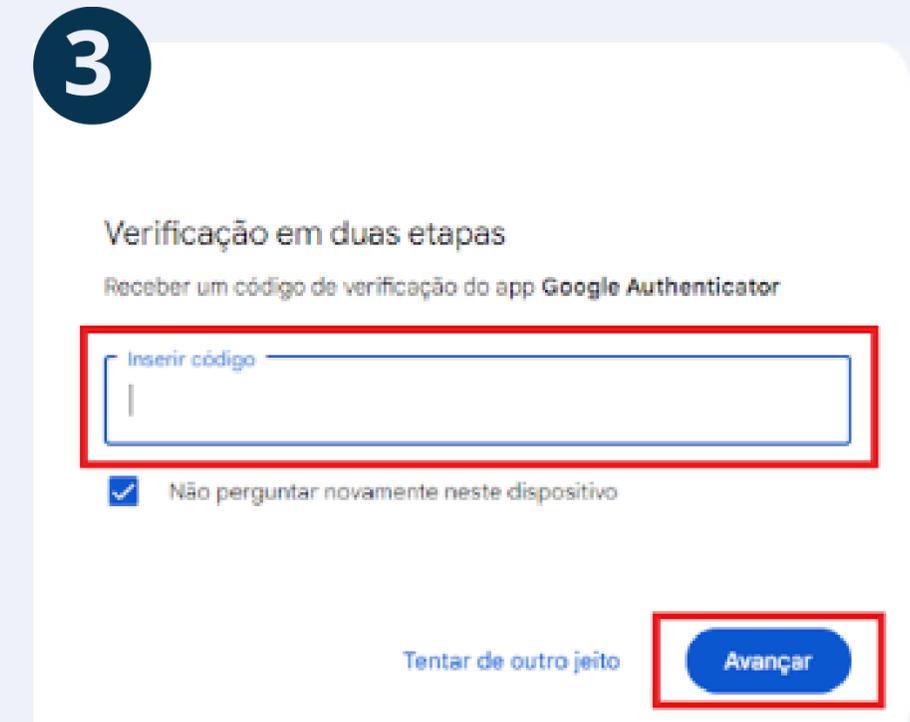
ACESSANDO O GMAIL APÓS ATIVAÇÃO DO MFA



Passo 13: Outra forma de autenticar na sua conta, seria clicando em "Tentar de outro jeito".



Clique em "**Receber um código de verificação do app Google Authenticator**"



Abra o aplicativo Google Authenticator no seu smartphone e insira o código gerado no campo "**Inserir código**", e clique em "**Avançar**", conforme a imagem acima. Note que nessa tela também aparece a opção "**Não perguntar novamente neste dispositivo**". Após, será possível o acesso ao seu e-mail.

Continuação na próxima página



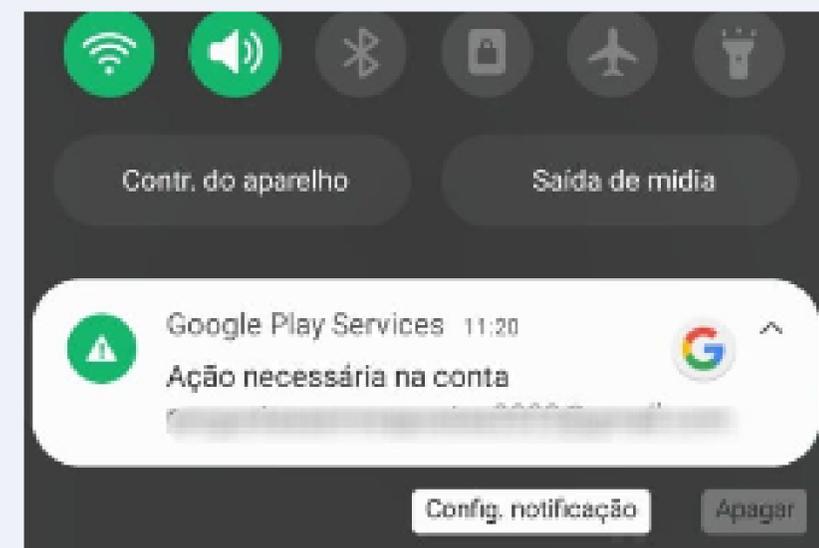
PROCEDIMENTOS APÓS REDEFINIÇÃO DE SENHA

Passo 1: Após a redefinição da senha, aguarde cerca de 20 minutos para que a nova senha sincronize e possa ser utilizada.

Passo 2: Após o sincronismo, seu e-mail será desconectado do smartphone e do computador/navegador em uso. Diante disso, uma notificação "Ação necessária na conta" aparecerá na barra superior do seu dispositivo móvel, conforme ilustrado na Imagem ao lado.

Passo 3: Clique na notificação e insira a nova senha. Em seguida, será solicitado o código de seis dígitos do Google Authenticator. Abra o aplicativo autenticador e digite o código gerado no local indicado. Após concluir este passo, seu smartphone estará novamente configurado como um dispositivo confiável.

Passo 4: Após concluir os passos anteriores, seu smartphone recuperará o acesso ao e-mail.



DICAS IMPORTANTES

Dica 01: Antes de iniciar a configuração, certifique-se de que a opção de data e hora automáticas esteja ativada em seu smartphone. Isso permitirá que o dispositivo sincronize automaticamente as informações fornecidas pela rede.

Dica 02: Ao trocar de smartphone, acesse seu e-mail no novo dispositivo, instale o aplicativo Google Authenticator e vincule a conta do TJRR no aplicativo autenticador. Vale destacar, que esses procedimentos devem ser feitos antes de realizar o reset no antigo smartphone.

Dica 03: Ao iniciar uma nova sessão, ele terá a opção de marcar uma caixa para estabelecer confiança no computador. Contudo, caso o usuário encerre a sessão do dispositivo ou redefina os cookies de login, será necessário realizar novamente a verificação em duas etapas para acessar o equipamento.

Dica 04: Sempre manter os códigos do Google Authenticator sincronizados nos dispositivos móveis, para evitar problemas no futuro. Verifique se há um ícone de nuvem verde ao lado da foto de perfil no App Authenticator, pois isso indica que os códigos estão sincronizados e salvos em backup na conta do Google.

DICAS IMPORTANTES

Atenção: Após a ativação do Múltiplo Fator de Autenticação (MFA) no E-mail, todos os serviços do Google Workspace associados à sua conta Google do TJRR passarão a utilizar essa camada adicional de segurança. Isso inclui o acesso aos serviços abaixo, dentre outros:

- Google Drive 
- YouTube 
- Planilhas Google 
- Formulários 
- Agenda/Calendário 
- Google Meet 
- Documentos 
- Google Fotos 

Dessa forma, será necessário autenticar sua identidade utilizando o MFA sempre que acessar essas ferramentas, garantindo uma proteção extra às suas informações.

SUPORTE TÉCNICO

Em caso de dúvidas, estaremos disponíveis nos seguintes canais de atendimento:



atendimento@tjrr.jus.br

Para regiões com DDD 95



0800 723 1783

Demais Regiões



(95)3198-4141

Nosso horário de atendimento é de segunda a sexta-feira, das 8h às 18h