2025

Autenticação de Dois Fatores (Gmail)

AGETIC
AGÊNCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Sumário

1 – Apresentação

Este documento apresenta um guia para a ativação e uso da autenticação de dois fatores no Gmail. Contém instruções de instalação dos aplicativos, bem como ativação do serviço na conta Google e como utilizá-lo para realizar autenticação.

O passo-a-passo abaixo pode ser executado todo apenas utilizando o smartphone ou dispositivo semelhante, porém recomendamos que utilize um computador em conjunto para facilitar a ativação do serviço.

2 - Justificativa

Autenticação de dois fatores (2FA) é uma camada extra de segurança para proteger o acesso às contas e sistemas da empresa. Com 2FA, além de usar sua senha, você também precisa confirmar sua identidade de uma segunda forma, geralmente por meio de um código enviado para o celular, um aplicativo autenticador ou até biometria, como impressão digital.

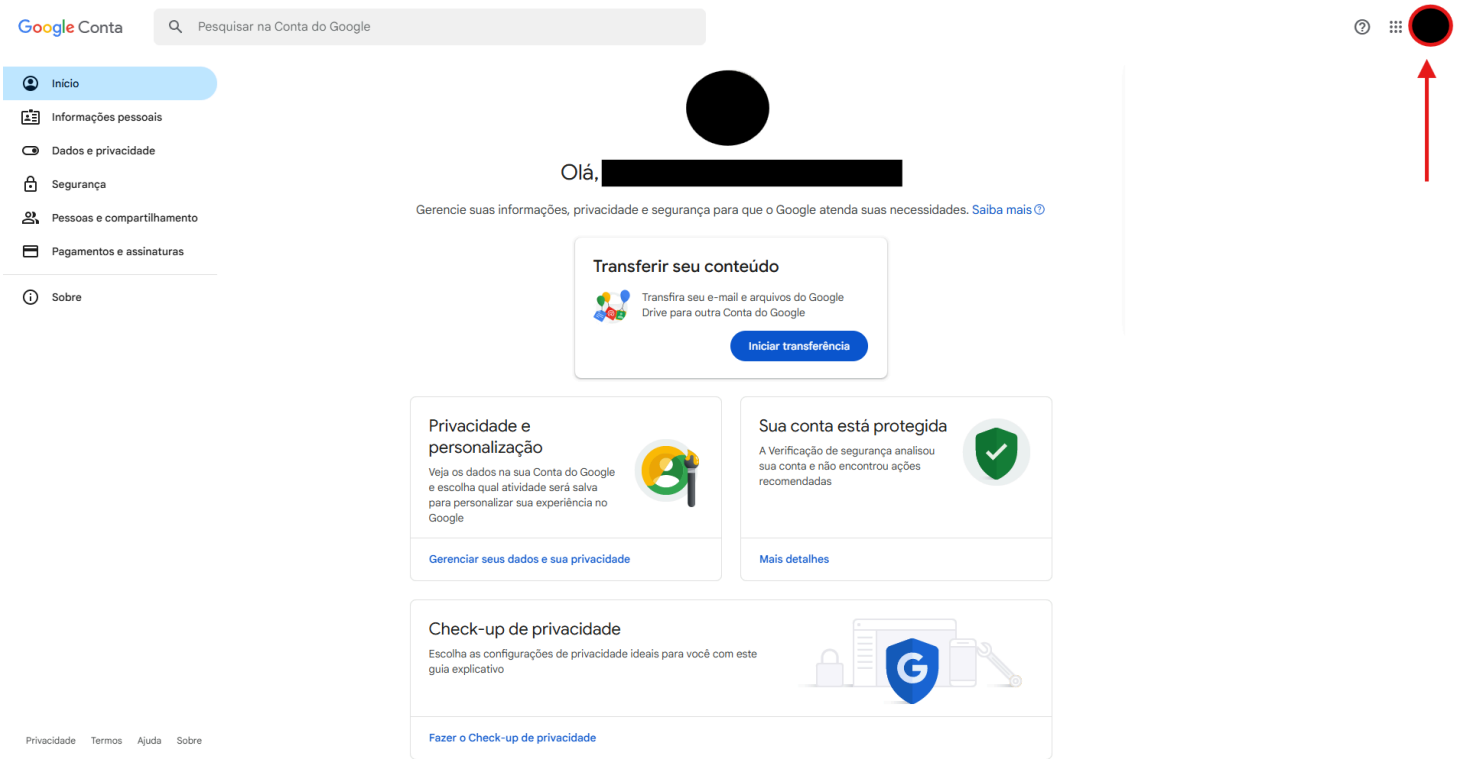
Essa medida foi implementada para garantir que, mesmo que sua senha seja descoberta, só você terá acesso às informações e ferramentas da instituição, pois o segundo fator de autenticação é único e pessoal. É uma maneira simples e eficaz de proteger os dados contra acessos não autorizados e ataques cibernéticos.

Conforme dispõe o parágrafo único do artigo 5º, do Capítulo II, da Instrução Normativa nº 12/2025-AGETIC/RTR/UFMS, de 13 de janeiro de 2025, “Para maior segurança pessoal e institucional, o usuário deverá habilitar a autenticação de dois fatores, sob pena de suspensão de uso do serviço”. Para mais informações acesse a publicação a partir do seguinte link: Boletim Oficial.

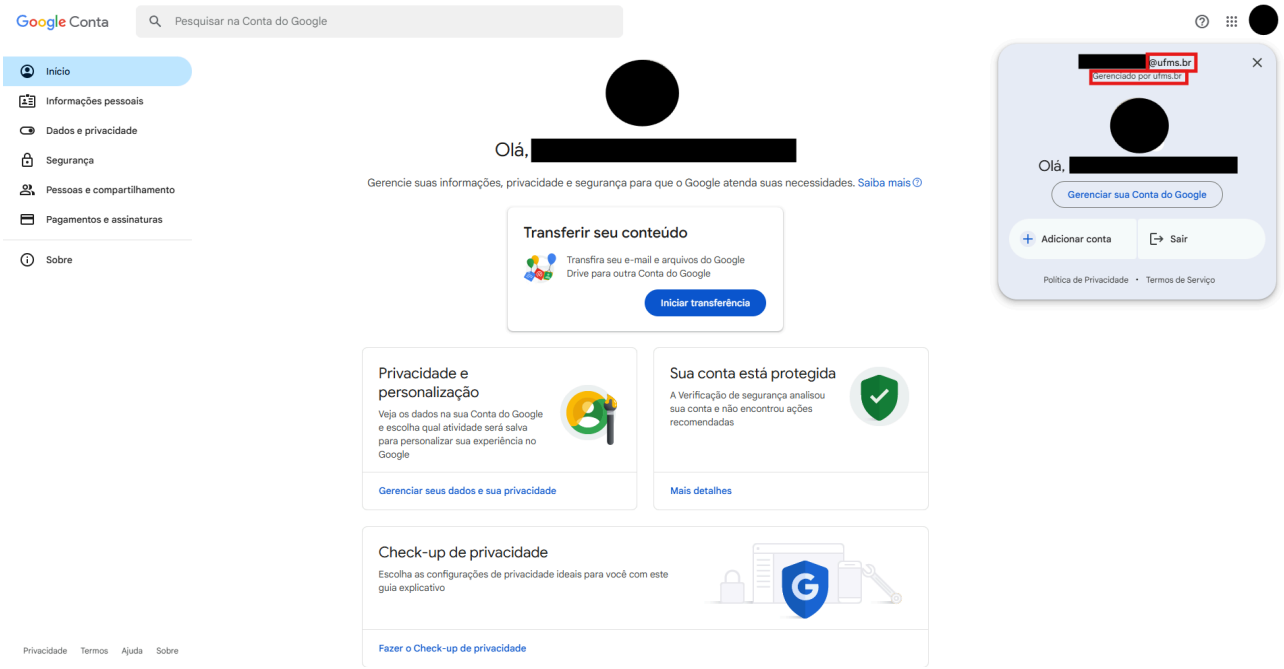
3 - Ativação

Para ativar a autenticação de dois fatores, o primeiro passo é acessar as configurações de sua conta institucional Google por meio do link: https://www.google.com/account.

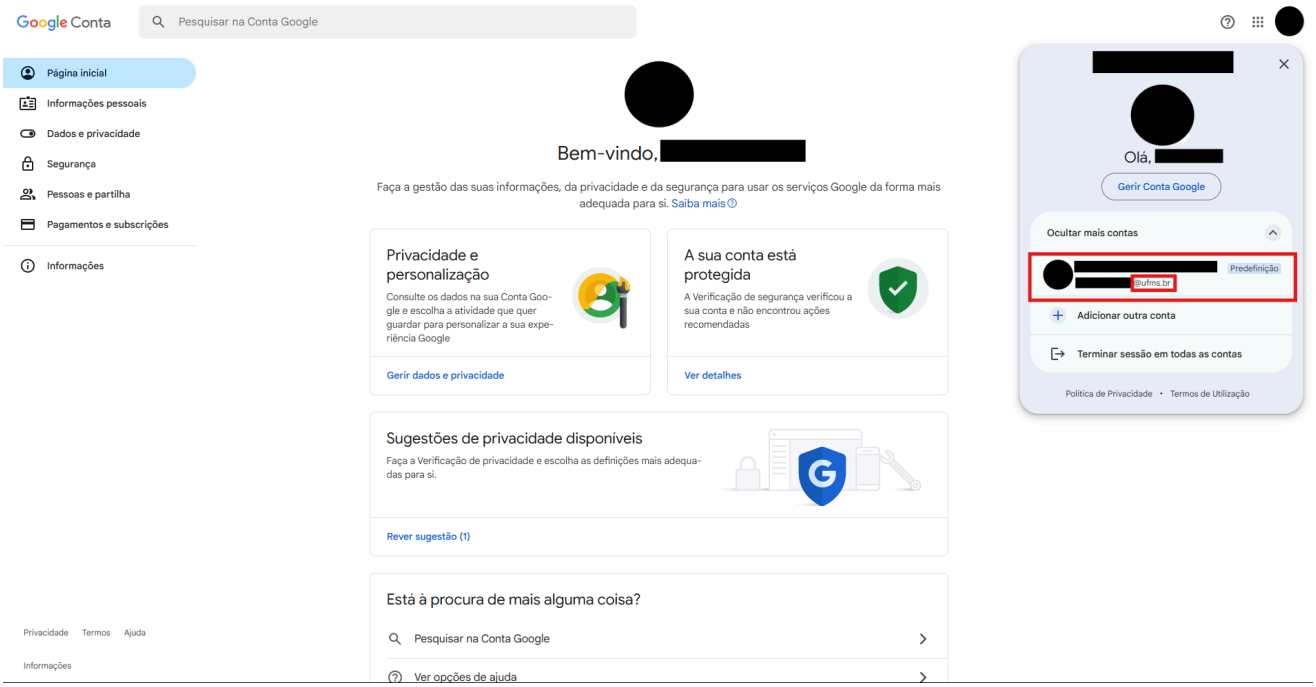
Após realizar o login com seu e-mail e senha institucionais é preciso confirmar se realmente está utilizando o e-mail institucional. Para isso, clique no ícone de sua foto de perfil, presente na extremidade superior direita da tela.



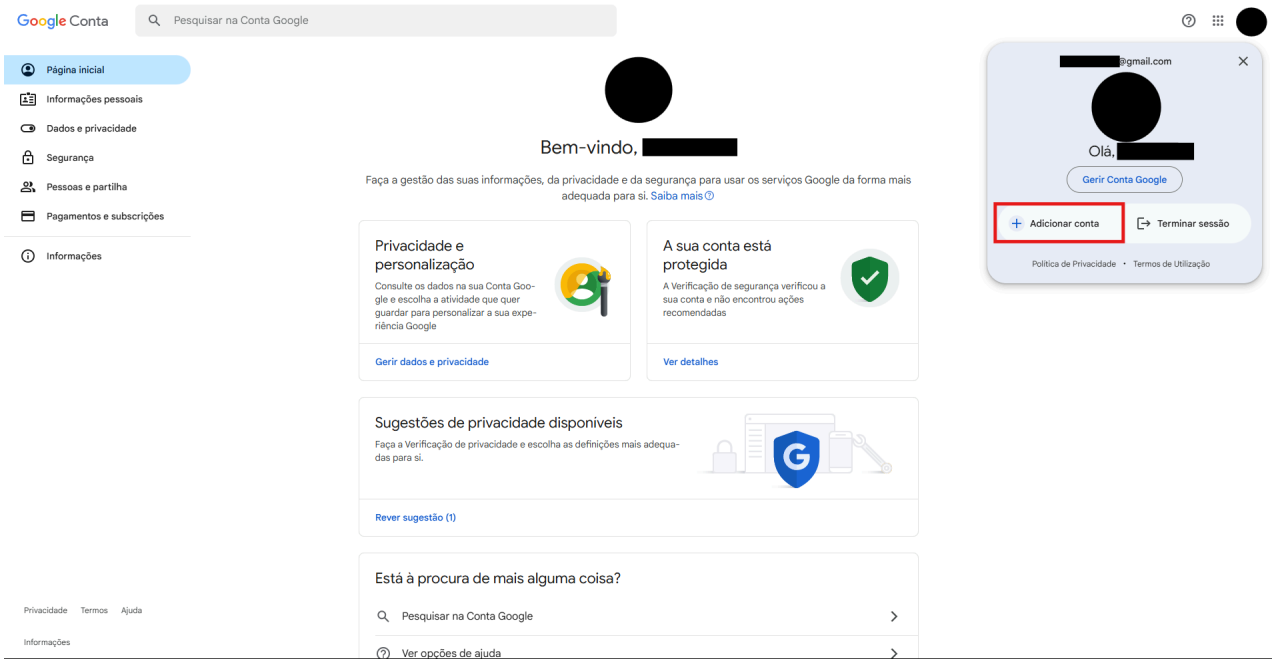
Em seguida, verifique se está utilizando o e-mail UFMS. Note que deve estar escrito “@ufms.br” após seu usuário do passaporte.



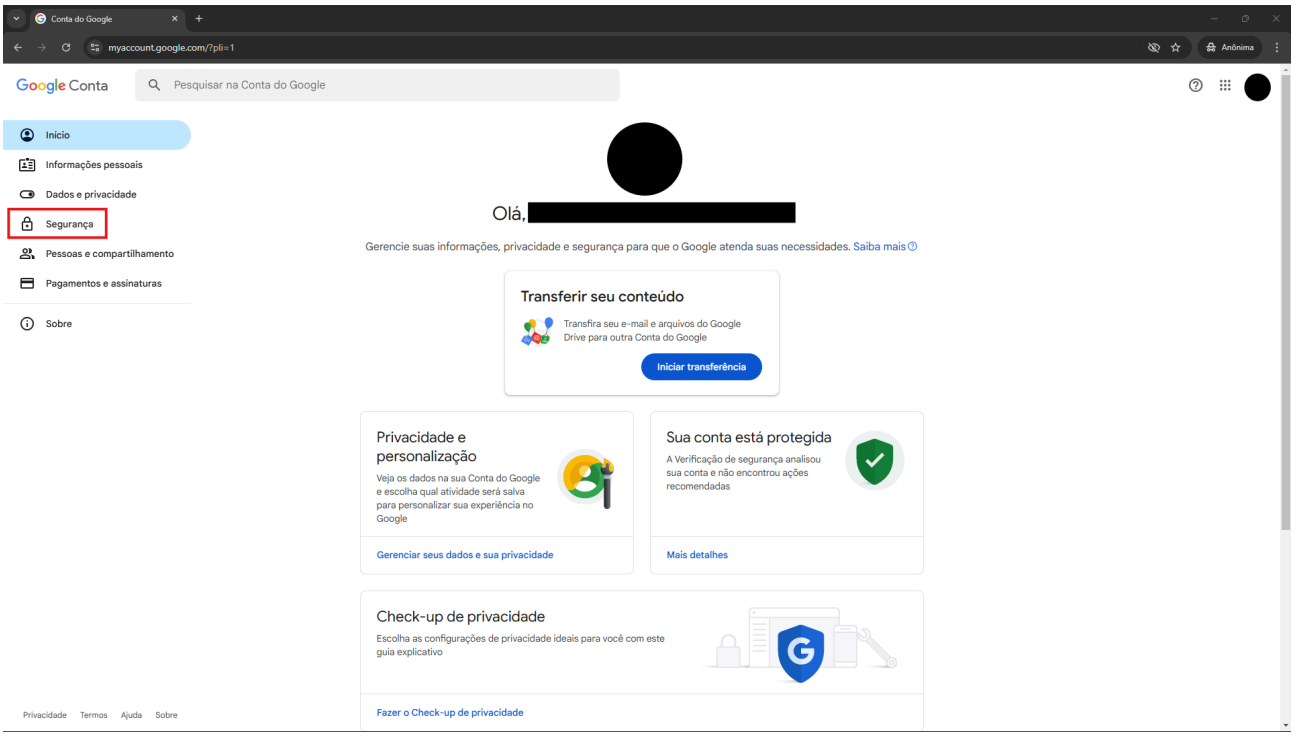
Caso não esteja utilizando o e-mail UFMS, conforme a imagem acima, verifique se o e-mail está aparecendo no menu abaixo de sua foto, e clique no e-mail UFMS para que possa fazer a configuração corretamente.



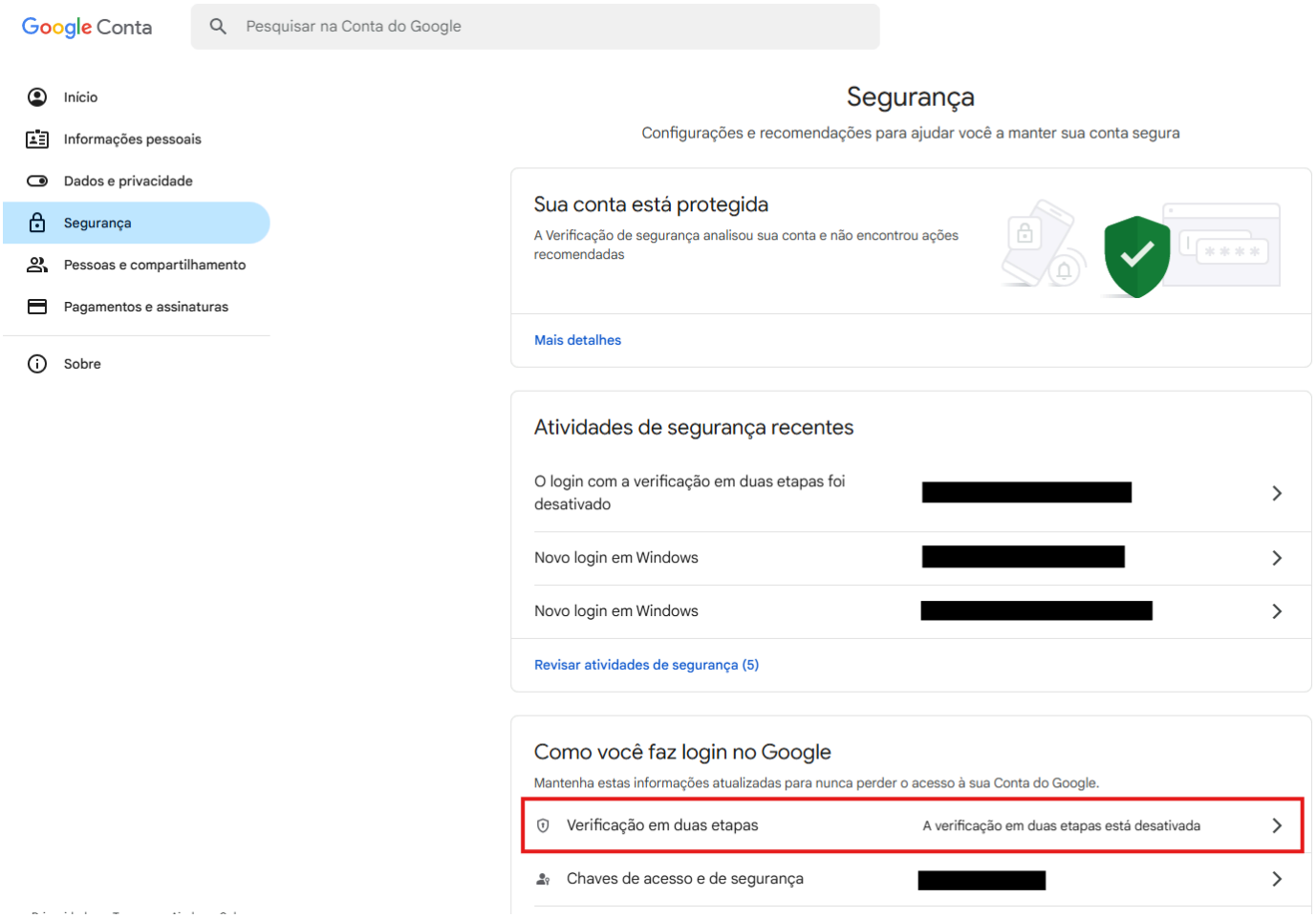
Se notar que o e-mail UFMS não aparece no menu abaixo de sua foto, clique em “Adicionar conta” e realize o login no e-mail institucional utilizando suas credenciais do Passaporte UFMS.



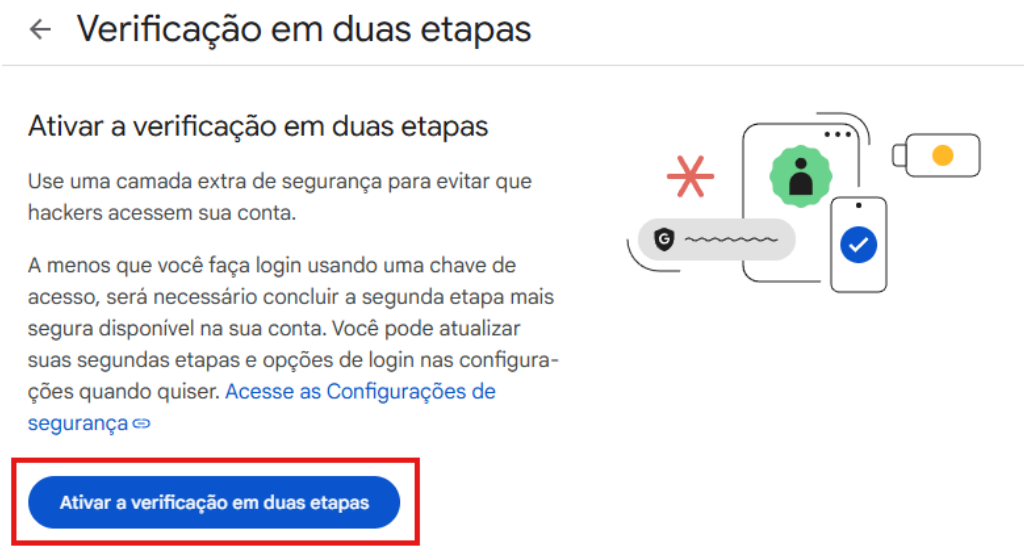
Depois de confirmar que está acessando sua conta UFMS, selecione a seção “Segurança”, presente no menu lateral à esquerda da tela.



Já na aba “Segurança”, selecione a opção “Verificação em duas etapas”, presente na seção “Como você faz login no Google”.

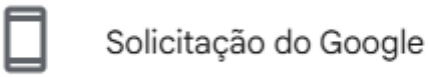


Independente de qual meio de ativação escolher, lembre-se de clicar no botão “Ativar a verificação em duas etapas” após adicionar o meio desejado. Você receberá um e-mail confirmando que o método foi ativado logo após clicar no botão.



Abaixo, seguem os três meios de ativação que recomendamos que sejam utilizados.

3.1 - Solicitação do Google



Para que esse método funcione, sua Conta do Google precisa estar conectada no dispositivo para que você receba uma solicitação.

Ao fazer login na sua Conta do Google, você selecionará uma opção em seu dispositivo, logo após a aparição de uma notificação, para confirmar sua identidade.

Basta selecionar uma opção confirmando que é você quem está tentando realizar o login, e, após seguir as orientações apresentadas na tela, seu login será confirmado.

3.2 - Número de telefone

Número de telefone

Para que esse método funcione, sua Conta do Google deve ter um número de telefone cadastrado, para que a mesma possa enviar o SMS e possíveis alertas de segurança.

Ao fazer login na sua Conta do Google, você receberá uma notificação via SMS no número de telefone cadastrado, aguarde que o código chegue e insira o mesmo no campo que será mostrado na tela de login da sua Conta do Google.

3.3 - Authenticator

Authenticator

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

A primeira etapa é realizar o download do aplicativo Google Authenticator na Play Store (Android) ou na App Store (iOS). **Fique atento e garanta que o aplicativo que será instalado seja o legítimo da Google, evitando semelhantes ou cópias**. Caso prefira, acesse um dos links abaixo para garantir acesso à aplicação oficial.

- Link para **Play Store (Dispositivos Android)**: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=pt_BR&pli=1

- Link para **App Store (Dispositivos iOS)**: https://apps.apple.com/br/app/google-authenticator/id388497605

(Ícone do aplicativo Google Authenticator)

Após o download do aplicativo, ocorrerá um momento onde você escolherá o e-mail de registro, selecione um e-mail que **NÃO** seja seu e-mail institucional,

caso contrário você poderá ficar sem possibilidade de realizar o login em seu e-mail.

Depois de ter realizado seu cadastro no aplicativo, selecione a opção "**Configurar o autenticador**"

Para sincronizar o app e sua conta:

Passo 1: Abra o app no dispositivo;

Passo 2: Clique no botão "**+**" presente no canto inferior direito da tela de seu dispositivo;

Passo 3: Selecione qual método de configuração deseja;

Passo 4: Leia o QR Code que aparece na após clicar no botão "**Configurar o autenticador**", caso seu dispositivo consiga ler o QR Code, caso contrário, clique na opção "**Não consegue ler o código?**".

Após cadastrar o código, clique no botão "Avançar" e insira o código que aparece no aplicativo.

É importante notar que o código se renova automaticamente a cada poucos segundos, assim garantindo a segurança do método, você pode acompanhar o temporizador a partir do relógio que é mostrado à direita do código.

4 - Conclusão

Após realizar as etapas descritas no 3º capítulo deste guia, sua conta institucional UFMS estará protegida. Lembre-se que, apesar da autenticação de dois fatores (2FA) ser uma excelente camada extra de segurança para proteger sua conta institucional, de acordo com o Parágrafo III do art. 15º, do Capítulo III, da Instrução Normativa nº 12/2025-AGETIC/RTR/UFMS, é **obrigação** do usuário **"manter sob sigilo credenciais de acesso, observado o disposto na normativa de uso de recurso de Tecnologia da Informação e Comunicação - TIC e demais normativos vigentes"**.

Lembre-se: a segurança digital é uma combinação de tecnologias e comportamento consciente. A autenticação de dois fatores é um passo importante, mas seu cuidado é essencial para garantir que suas informações permaneçam protegidas.

Caso queira entrar em contato a Agetic, abaixo, segue nossos canais de atendimento:

Suporte via chamada de telefone: (67) 3345-7292;

Suporte via Whatsapp (apenas mensagens): (67) 3345-7258;

E-mail: suporte.agetic@ufms.br.