

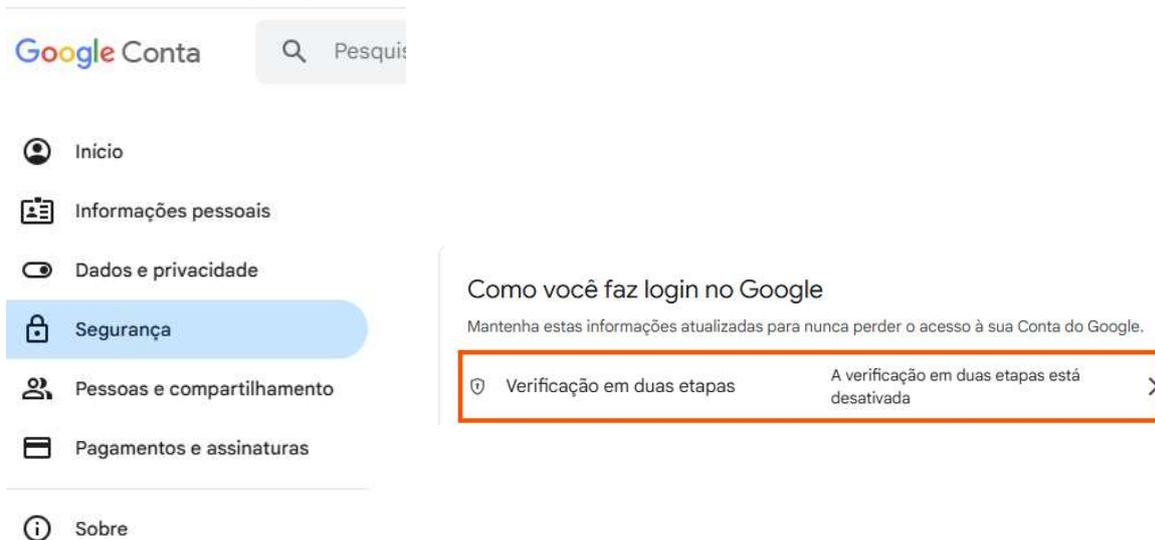
## Como configurar a autenticação do e-mail institucional em duas etapas?

Para permitir a verificação em duas etapas, cada usuário precisa seguir os passos a seguir:

1. Abra sua conta de e-mail institucional e clique no ícone do seu perfil no canto superior direito da tela, e depois em **“Gerenciar sua Conta do Google”**, como mostra a figura.



2. Em seguida, clique na seção **“Segurança”** e no item **“Como você faz login no Google”**, clique em **“Verificação em duas etapas”**. Caso a tela de login apareça, apenas entrar com as credenciais e seguir para o próximo passo.



3. Configure a segunda etapa à sua Conta do Google clicando no ícone + na opção **“Adicione um número de telefone”**.

## ← Verificação em duas etapas

### Ativar a verificação em duas etapas

Use uma camada extra de segurança para evitar que hackers acessem sua conta.

A menos que você faça login usando uma chave de acesso, será necessário concluir a segunda etapa mais segura disponível na sua conta. Você pode atualizar suas segundas etapas e opções de login nas configurações quando quiser. Acesse as [Configurações de segurança](#)



**Ativar a verificação em duas etapas**

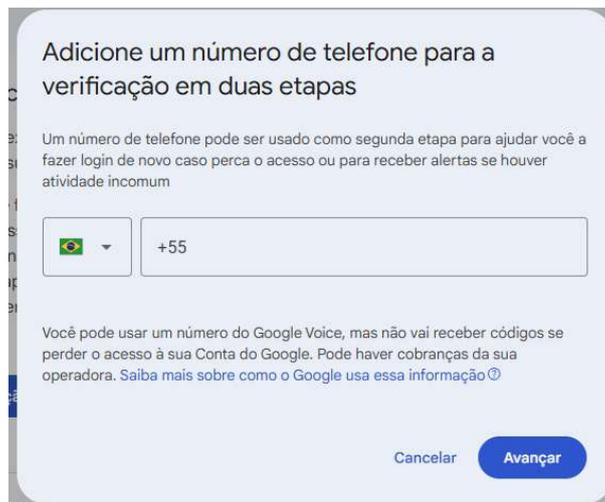
NÃO clique agora neste botão, primeiro adicione o número do telefone na opção abaixo

### Segundas etapas

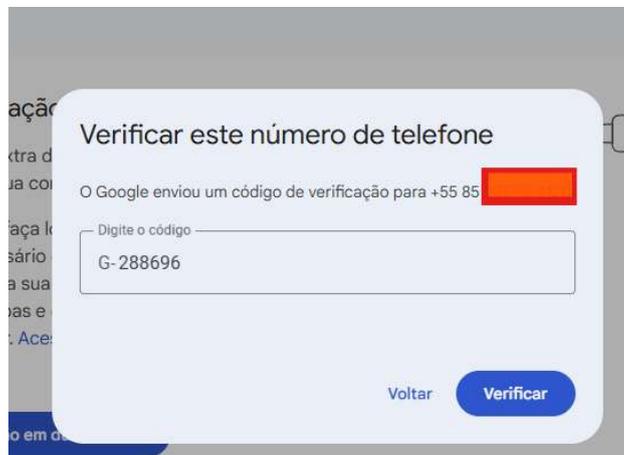
Mantenha essas informações atualizadas e adicione mais opções de login para que você possa sempre acessar sua Conta do Google

	Chaves de acesso e de segurança	Adicionar uma chave de segurança	>
	Solicitação do Google	3 dispositivos	>
	Authenticator	Adicionar app autenticador	>
	Número de telefone	Adicione um número de telefone	+

4. No cadastro do número de celular, escolha o país, forneça **DDD e NÚMERO** e clique em **“Avançar”**.



5. O número de telefone inserido será validado, através do envio de um SMS, com um código validador, que deve ser preenchido como mostra a figura a seguir.



6. Após a verificação, o Google informará que a configuração da Autenticação em Duas Etapas foi feita com sucesso.



7. Pronto! A partir deste momento, sempre que você for efetuar o login na sua conta de e-mail institucional, um código SMS será enviado para seu celular iniciando a verificação em duas etapas.

Além da ativação da Autenticação em Duas Etapas, o DETIC também relembra algumas boas práticas de uso do e-mail:

- A) Alterar a senha frequentemente;
- B) Usar senhas fortes;
- C) Não clicar em links suspeitos ou em anexos não solicitados;
- D) Desconfiar de e-mails solicitando informações pessoais;
- E) Não acessar o e-mail da UECE em equipamentos públicos ou não confiáveis;
- F) Manter atualizados antivírus e similares no celular e demais equipamentos onde o e-mail é acessado;
- G) Mesmo em equipamentos confiáveis, deslogar ao terminar de utilizar o e-mail.

O DETIC enfatiza que a segurança da informação é uma prioridade e conta com a colaboração de todos para tornar o ambiente computacional da Universidade mais seguro.