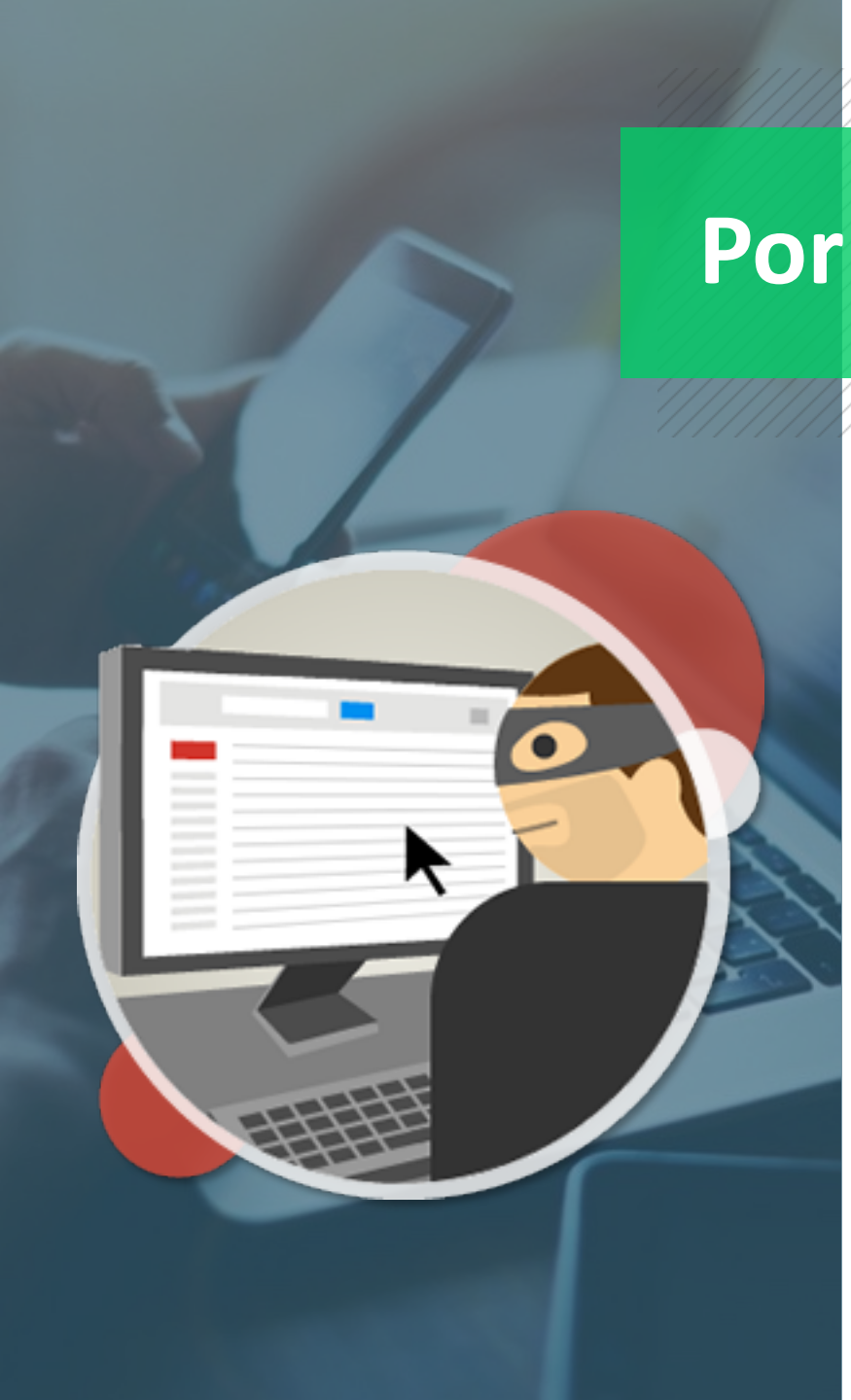
t-Risk

Método de Avaliação de Riscos

Autenticação de Duplo Fator na Plataforma t-Risk

Revisado em Junho/2021 A



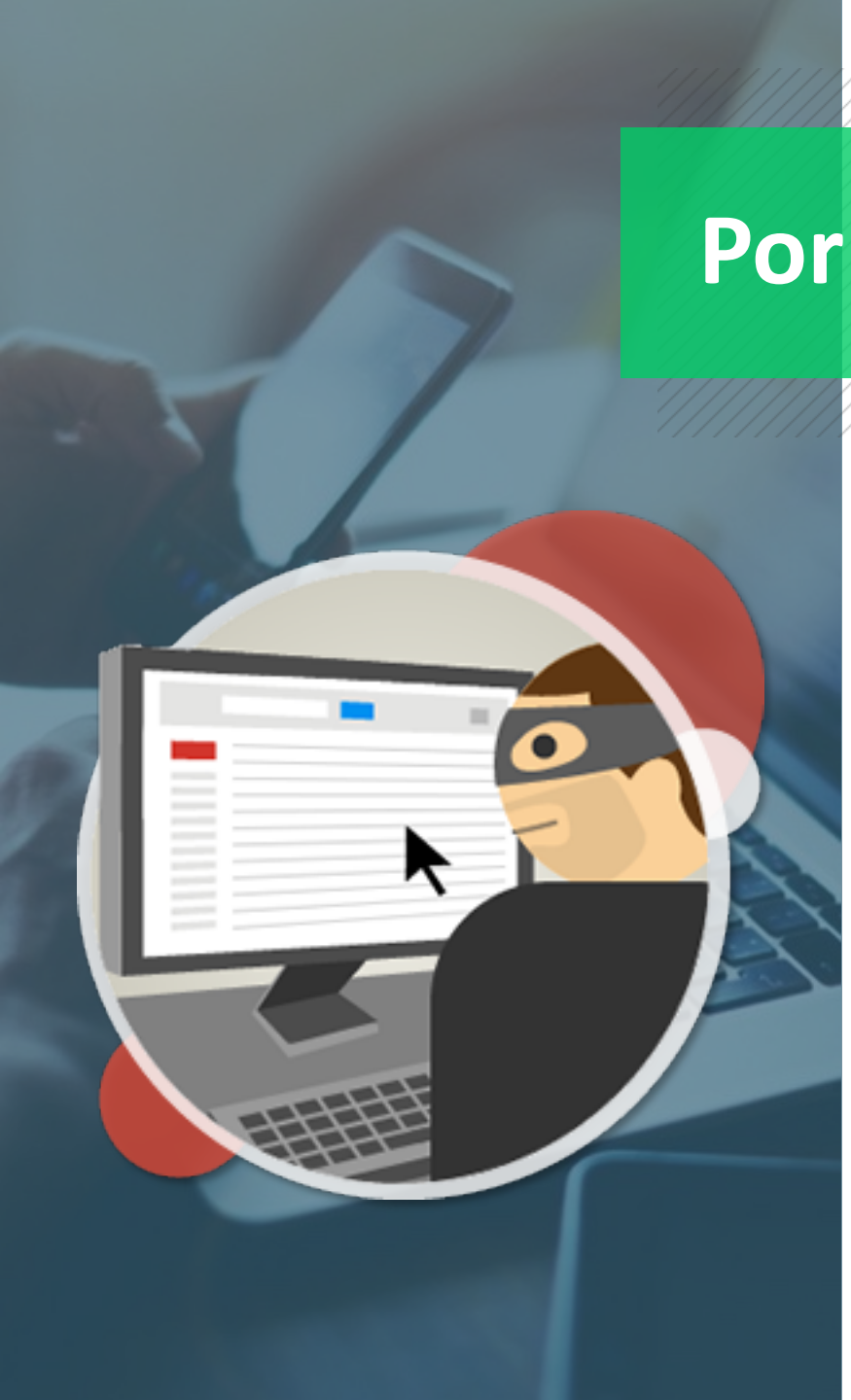
Por que você precisa disso?

Maior segurança para sua conta do t-Risk. Com a verificação em duas etapas, você protegerá sua conta com sua senha e seu telefone.

Ter sua senha roubada por alguém é muito mais fácil do que você pensa. Qualquer uma dessas ações comuns poderia colocar você em risco de ter sua senha roubada:

- Usar a mesma senha em mais de um site;
- Fazer download de software pela Internet;
- Clicar em links enviados por mensagens de e-mail;

A verificação em duas etapas pode ajudar a manter afastadas pessoas má intencionadas, mesmo que elas saibam sua senha.



Por que você precisa disso?

Imagine perder o acesso à sua conta e a tudo o que há nela. Quando uma pessoa mal intencionada rouba sua senha, ela pode bloquear o seu acesso à sua conta e fazer coisas como:

- Acessar e até mesmo excluir seus projetos, informações sobre seus projetos, fotos, e etc.;
- Fingir que é você e enviar solicitações de tarefas a seus contatos através do Plano de Ação 5W2H;
- Usar sua conta para redefinir as senhas, excluir ou incluir usuários na sua conta corporativa do t-Risk.

Como funciona?

O login em sua conta será um pouco diferente!

1

Você digita sua senha. Sempre que fizer login no t-Risk, você digitará sua senha como de costume.

2

Outra informação é solicitada. O código que é gerado automaticamente no *App Google Authenticator* em seu celular cadastrado deve ser inserido como segundo fator de autenticação.

Como ela protege você?

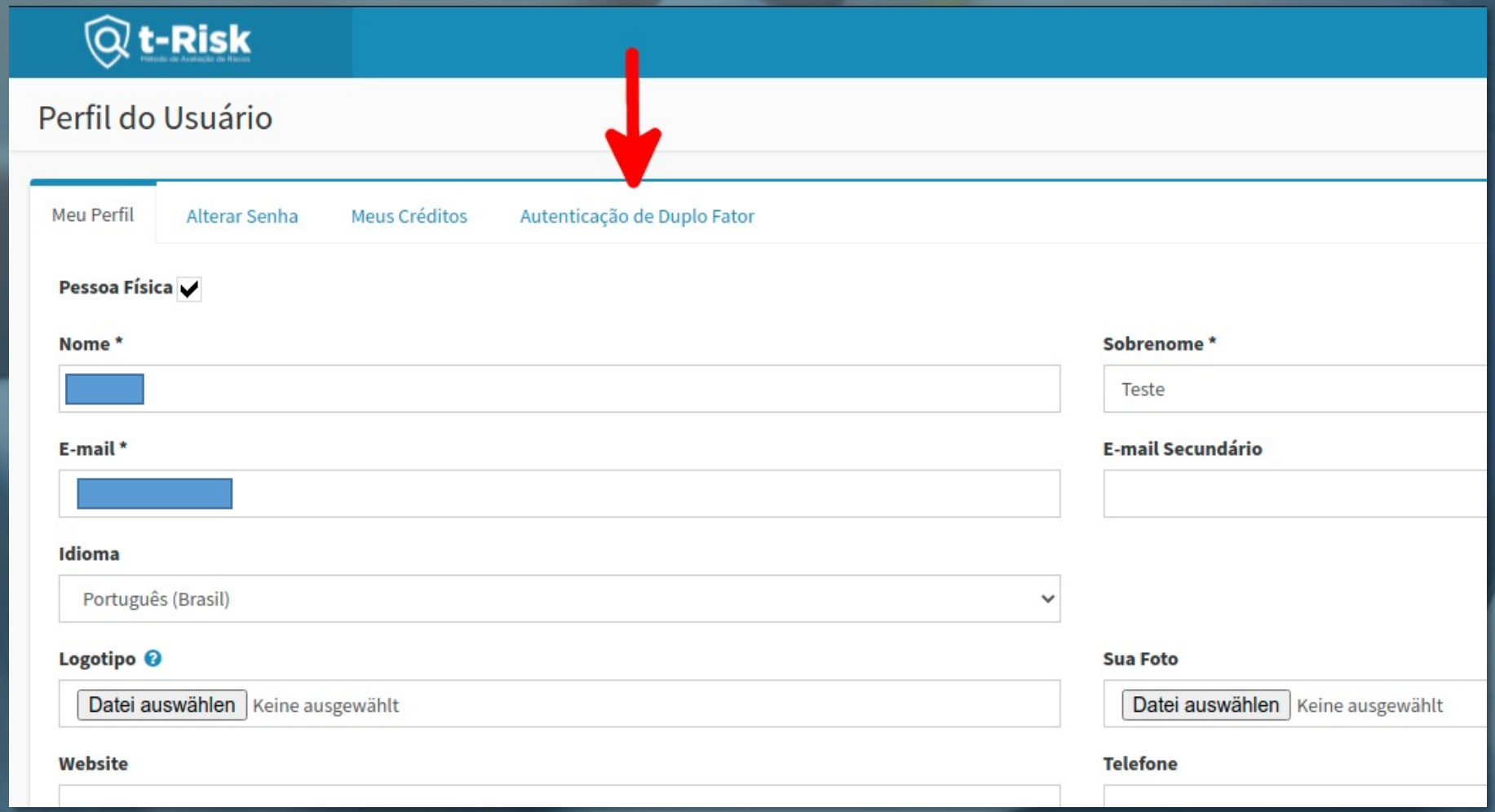
Uma camada extra de segurança. A maioria das pessoas tem apenas uma camada para proteger suas contas: a senha. Com a verificação em duas etapas, se um hacker invadir sua camada de senha, ele precisará também do seu smartphone com o *APP Google Authenticator* para entrar na sua conta.

O login exigirá algo que você sabe e algo que você tem. Com a verificação em duas etapas, você protege sua conta com algo que você conhece (sua senha) e algo que você tem (seu smartphone com o *APP Google Authenticator*).

Como ela protege você?

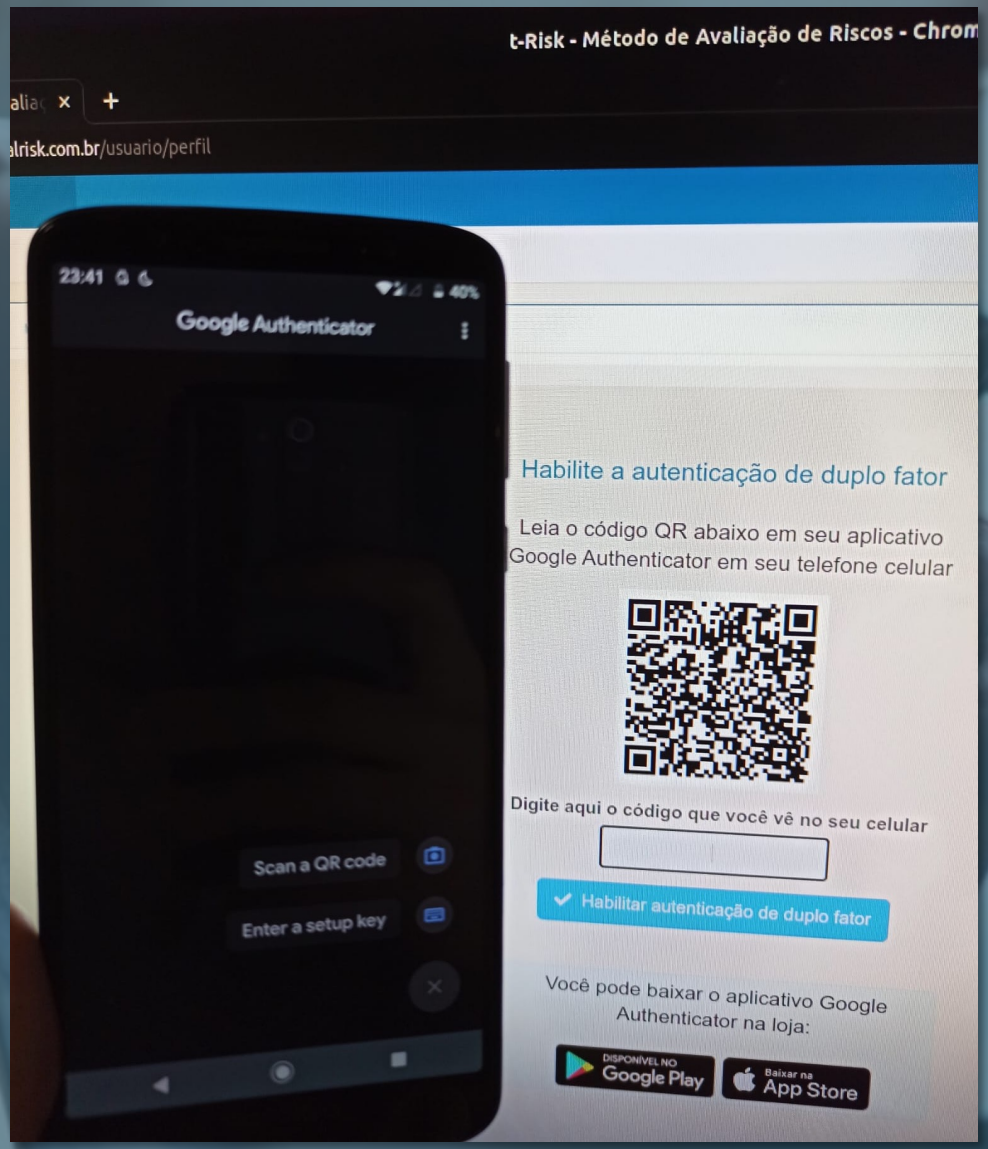
Códigos de verificação criados apenas para você. Os códigos são criados exclusivamente para sua conta quando você precisa deles. Cada código só pode ser usado uma vez.

Siga os passos a seguir para habilitar a autenticação de duplo fator na Plataforma t-Risk.



1 Acesse seu perfil de usuário e clique na aba "Autenticação de Duplo Fator".

2 Clique no botão "habilitar autenticação de duplo fator".



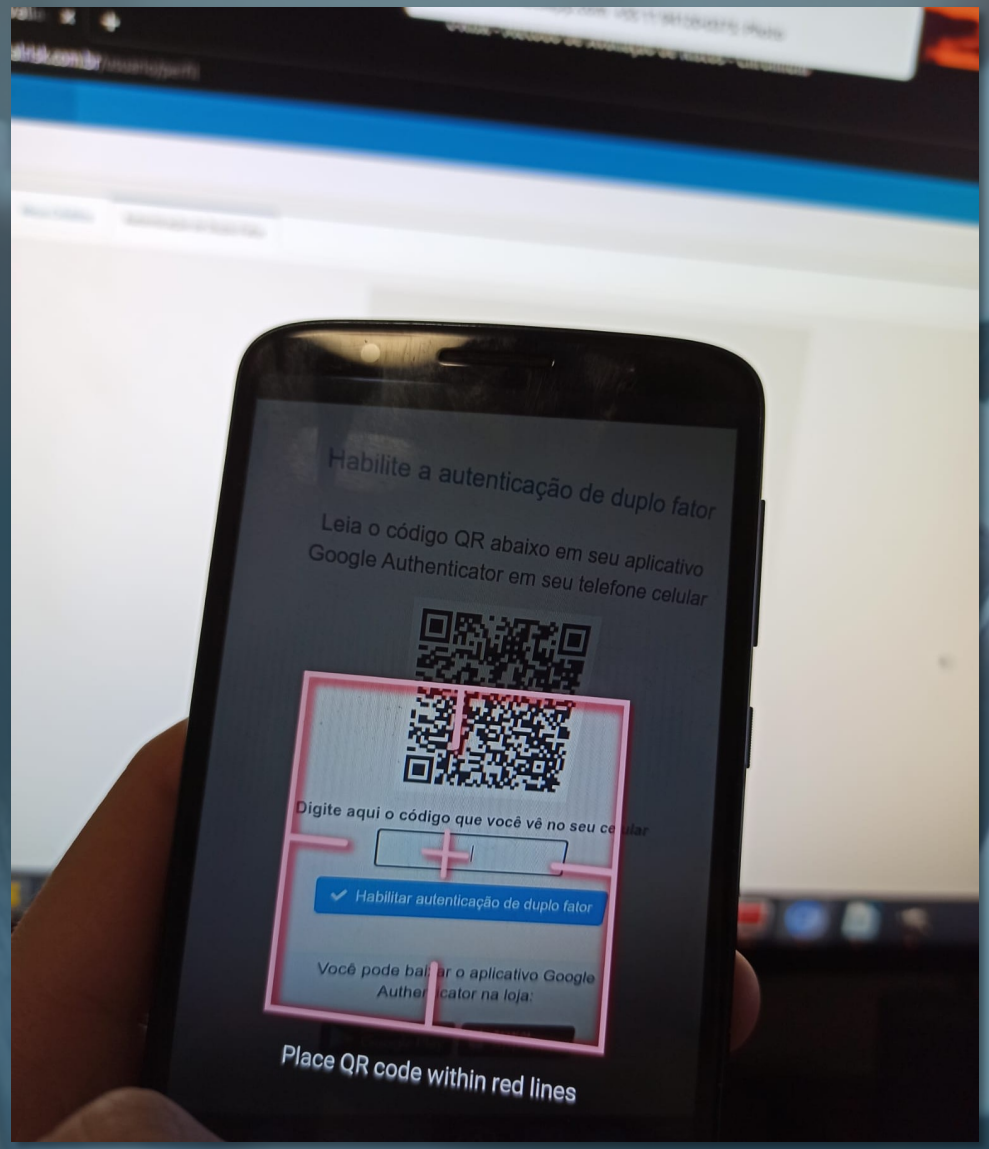
3

Abra o aplicativo Google Authenticator em seu celular. Caso você ainda não possua o aplicativo instalado, utilize os links da página para baixá-lo.

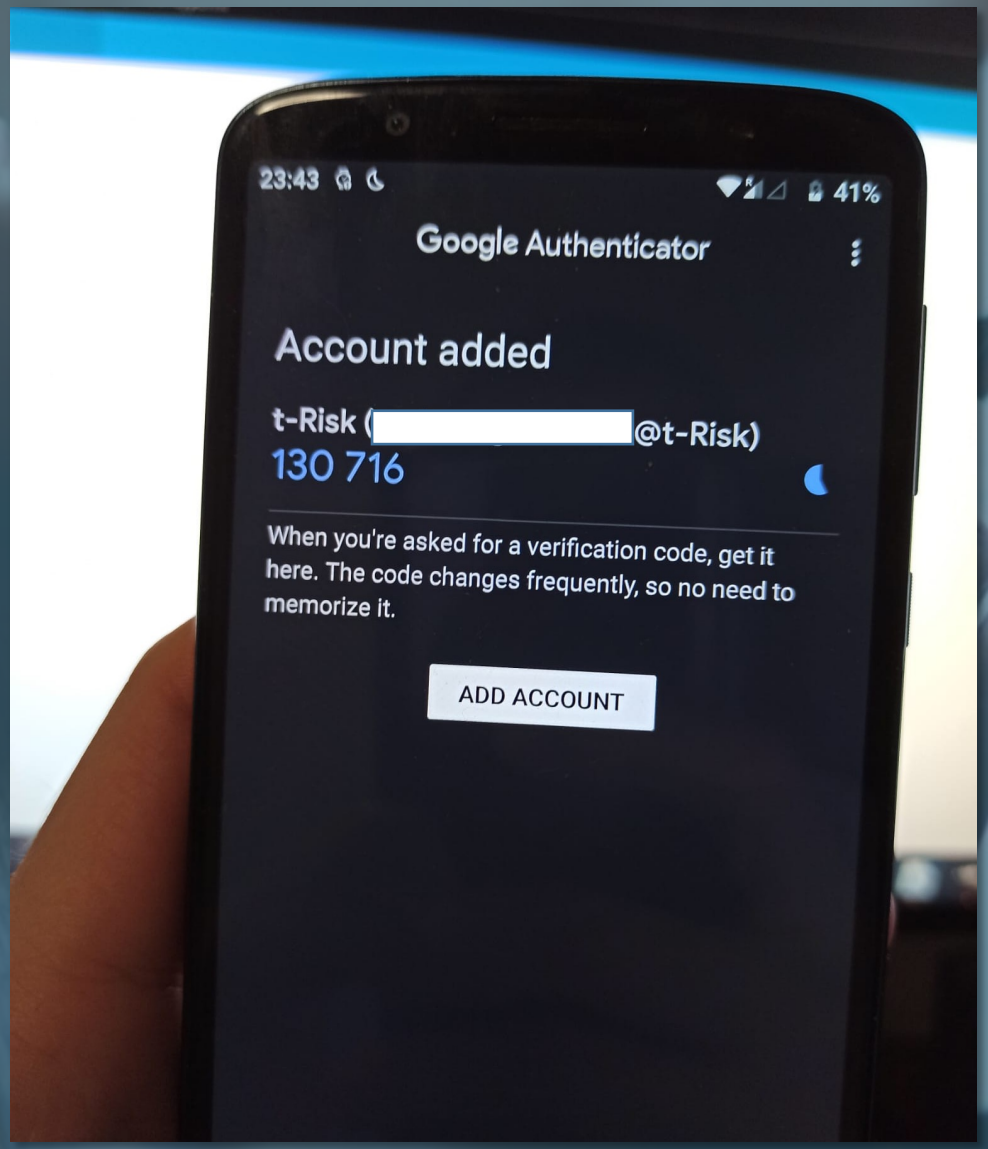
Sem conexão? Sem problemas. O aplicativo Google Authenticator para Android, iPhone ou BlackBerry pode gerar códigos de verificação. Ele funciona até mesmo quando seu dispositivo não tem conexão de dados ou telefone.

Link para Apple
https://apps.apple.com/br/app/google-authenticator/id388497605

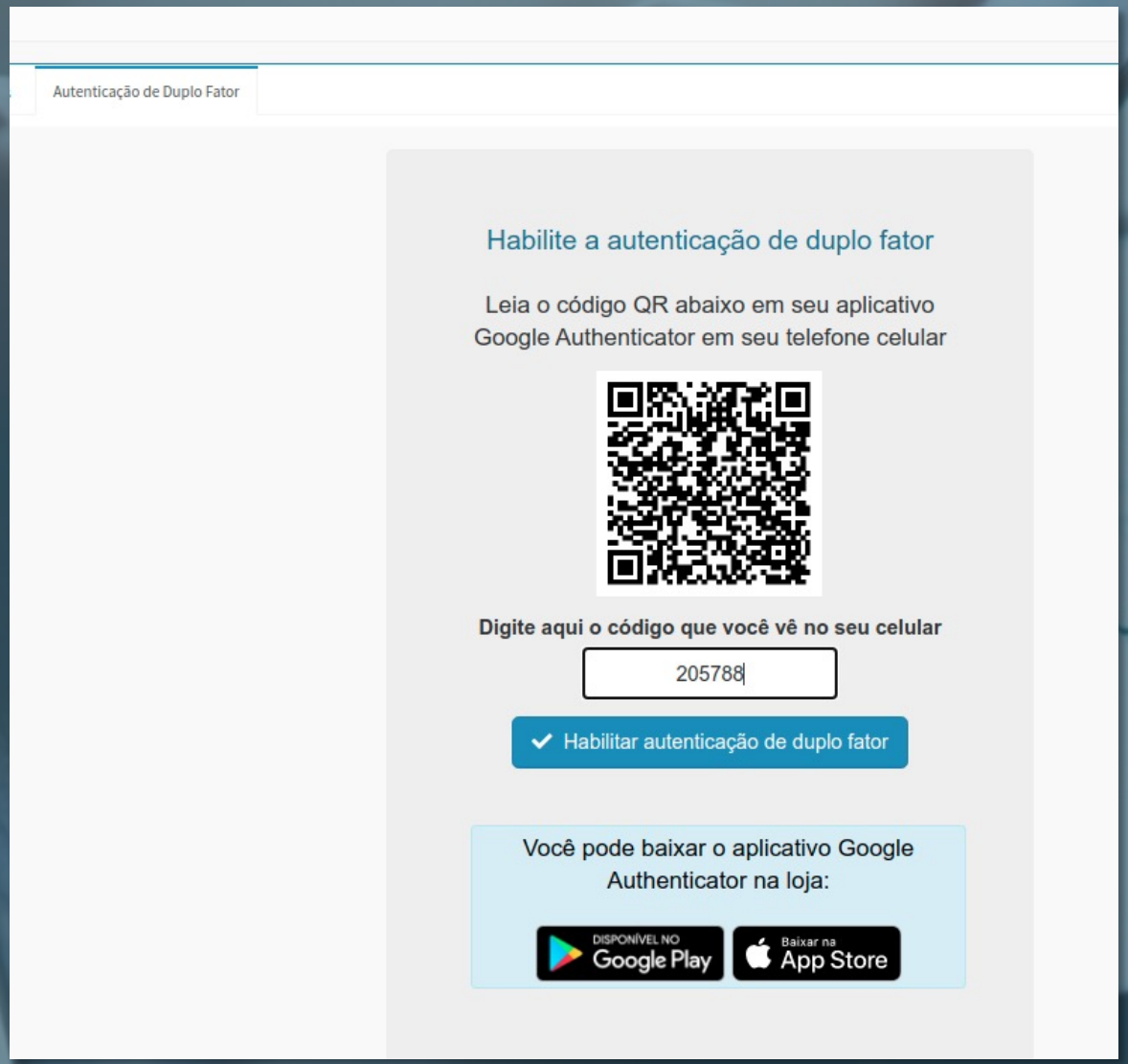
Link para Google Play
https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2



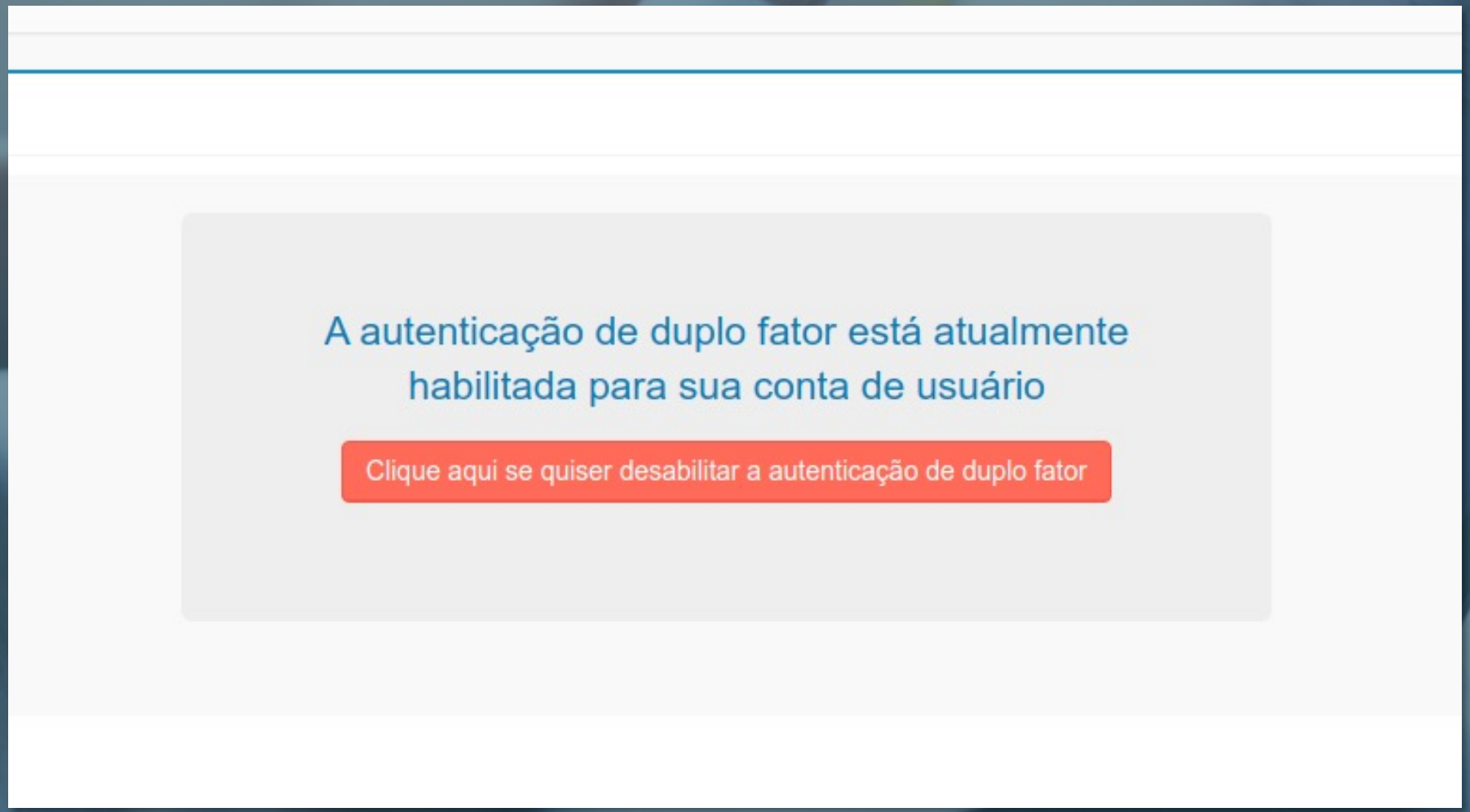
4 Em seguida, você deverá escanear a imagem exibida no aplicativo.



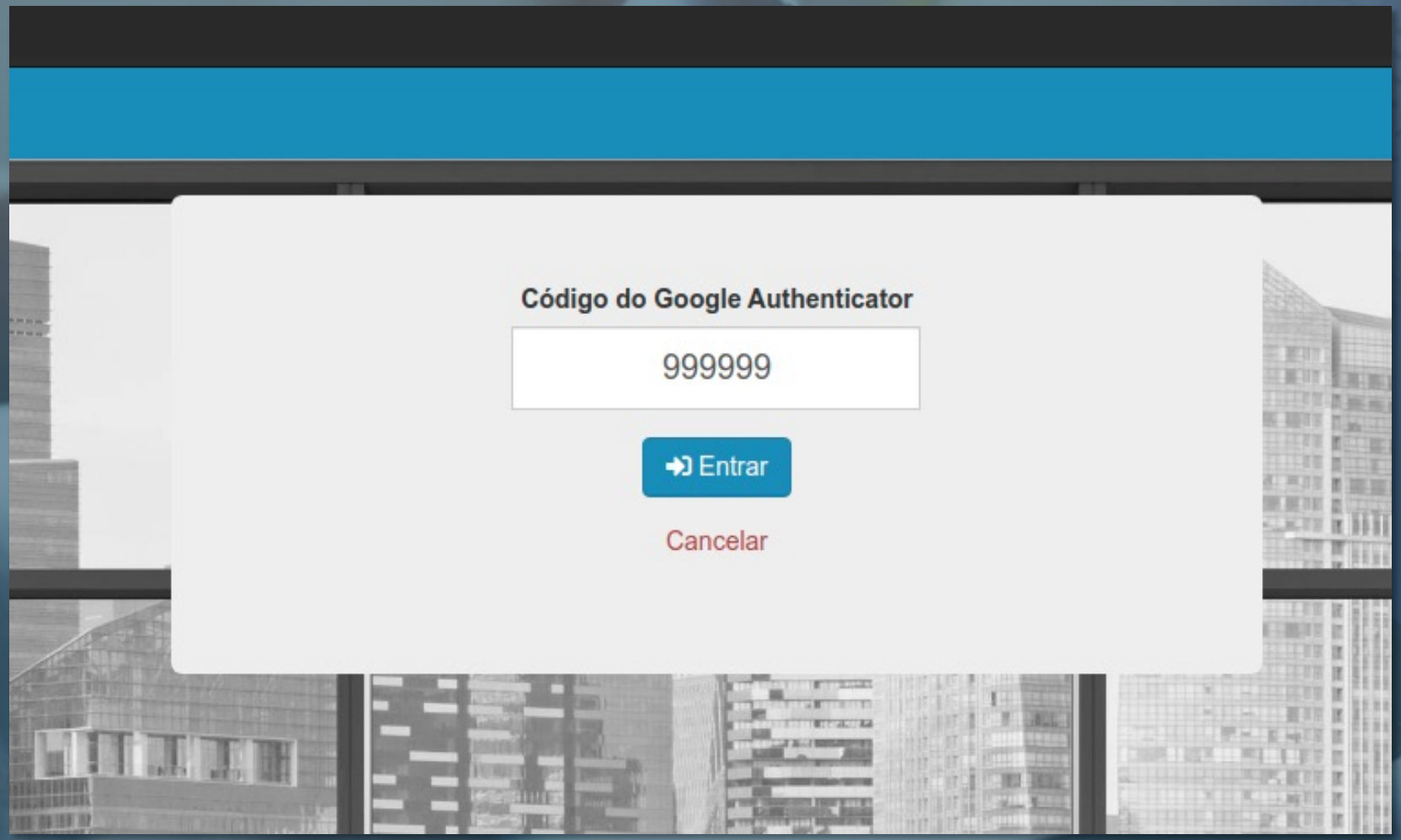
5 Uma vez que a imagem for escaneada com sucesso, você verá a sua conta cadastrada no aplicativo com um código para a primeira validação.



6 Digite neste campo o código exibido no aplicativo Google Authenticator e clique em “habilitar autenticação de duplo fator”.



7 Você deverá ver a confirmação de que a autenticação de duplo fator foi habilitada com sucesso.



8

A partir de seu próximo acesso, logo após digitar login e senha, será necessário digitar o código do aplicativo Google Authenticator para poder prosseguir no sistema.

t-Risk

Método de Avaliação de Riscos

Badge t-Risk Practitioner

Adicione a *Badge* t-Risk ao seu histórico profissional e compartilhe-a!

Para mais informações, fale conosco.