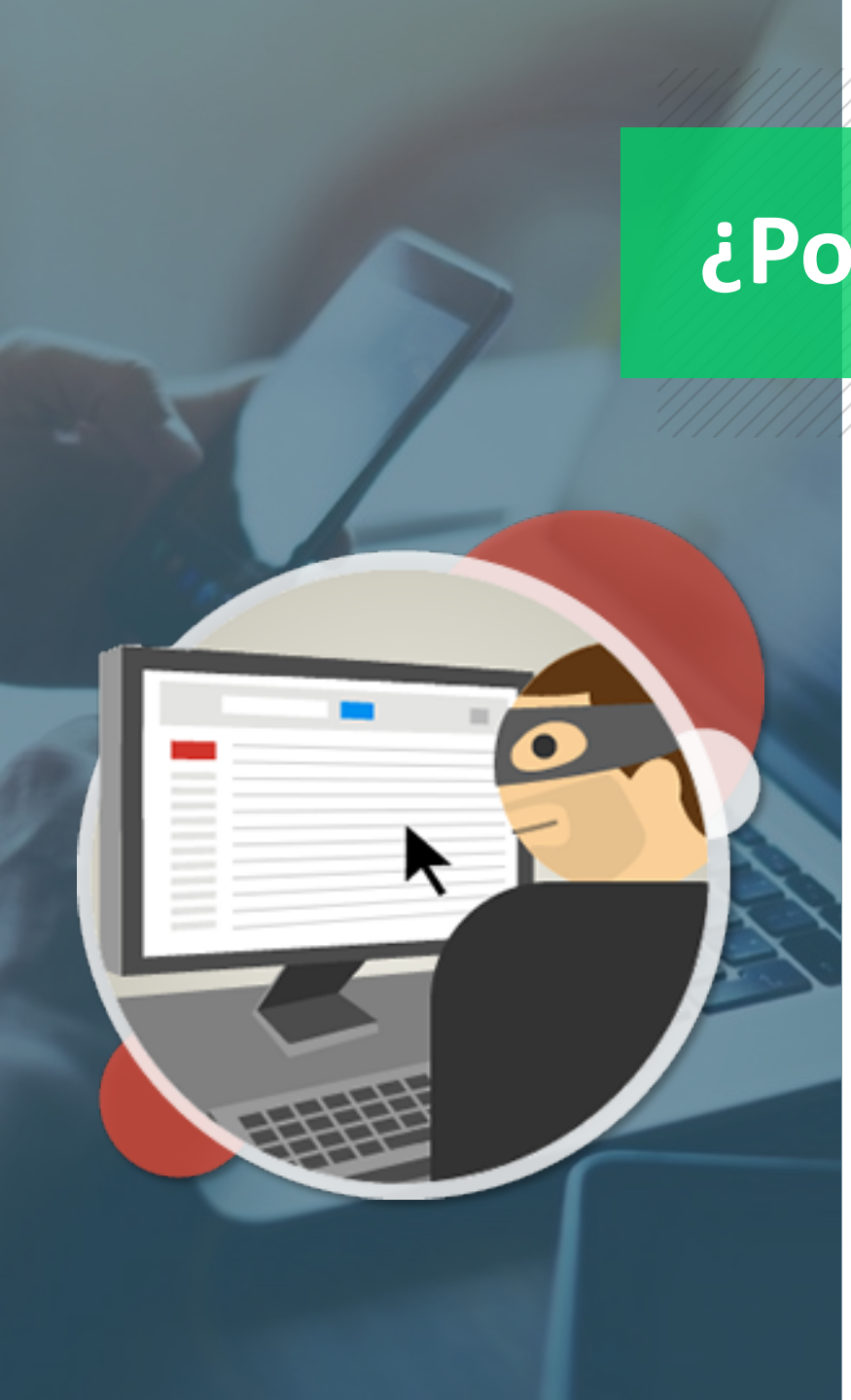
t-Risk

Método de Avaliação de Riscos

Autenticación de Double Factor en la Plataforma t-Risk

Revisado em Junho/2021 A - ES



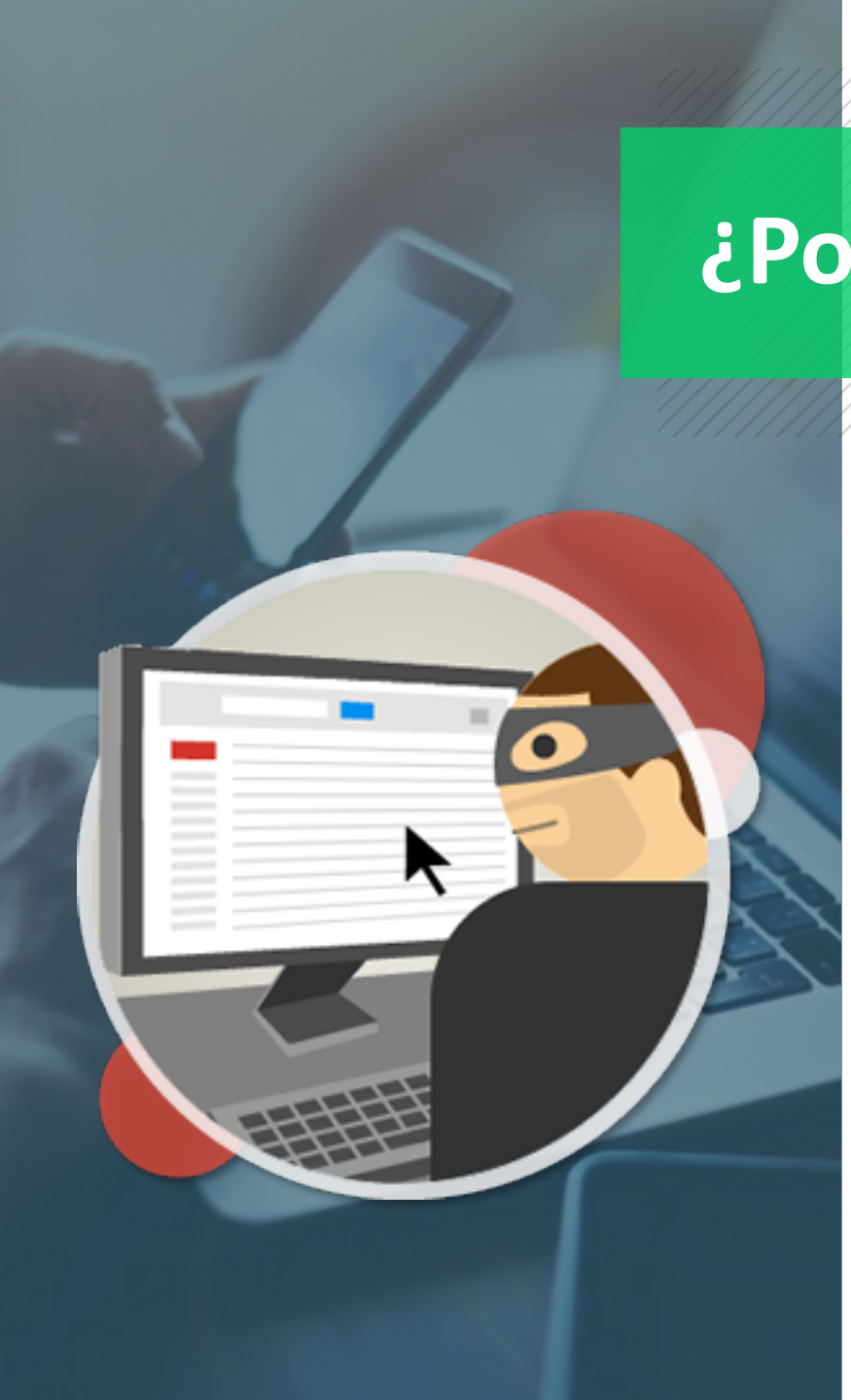
¿Por qué necesitas esto?

Mayor seguridad para su cuenta t-Risk. Con la verificación de 2 pasos, protegerá su cuenta con su contraseña y su teléfono.

Que alguien te robe tu contraseña es mucho más fácil de lo que crees. Cualquiera de estas acciones comunes podría ponerlo en riesgo de que le roben su contraseña:

- Usar la misma contraseña en más de un sitio web;
- Descarga de software de Internet;
- Hacer clic en los enlaces enviados por mensajes de correo;

La verificación en dos pasos puede ayudar a mantener alejadas a las personas malintencionadas, incluso si conocen su contraseña.



¿Por qué necesitas esto?

Imagínese perder el acceso a su cuenta y todo lo que contiene. Cuando una persona malintencionada roba su contraseña, puede bloquear su acceso a su cuenta y hacer cosas como:

- Acceder e incluso eliminar sus proyectos, información sobre sus proyectos, fotos etc.;
- Pasarse por tú y enviar solicitudes de tareas a tus contactos a través del Plan de acción 5W2H;
- Utilizar su cuenta para restablecer contraseñas, eliminar o agregar usuarios a su cuenta corporativa de t-Risk.

¿Como funciona?

¡Iniciar sesión en su cuenta será un poco diferente!

1

Ingresa tu contraseña.
Siempre que inicie sesión en t-Risk, ingresará su contraseña como de costumbre.

2

Se solicita otra información.
El código que se genera automáticamente en la *App Google Authenticator* en su teléfono móvil registrado debe ingresarse como segundo factor de autenticación.

¿Cómo te protege?

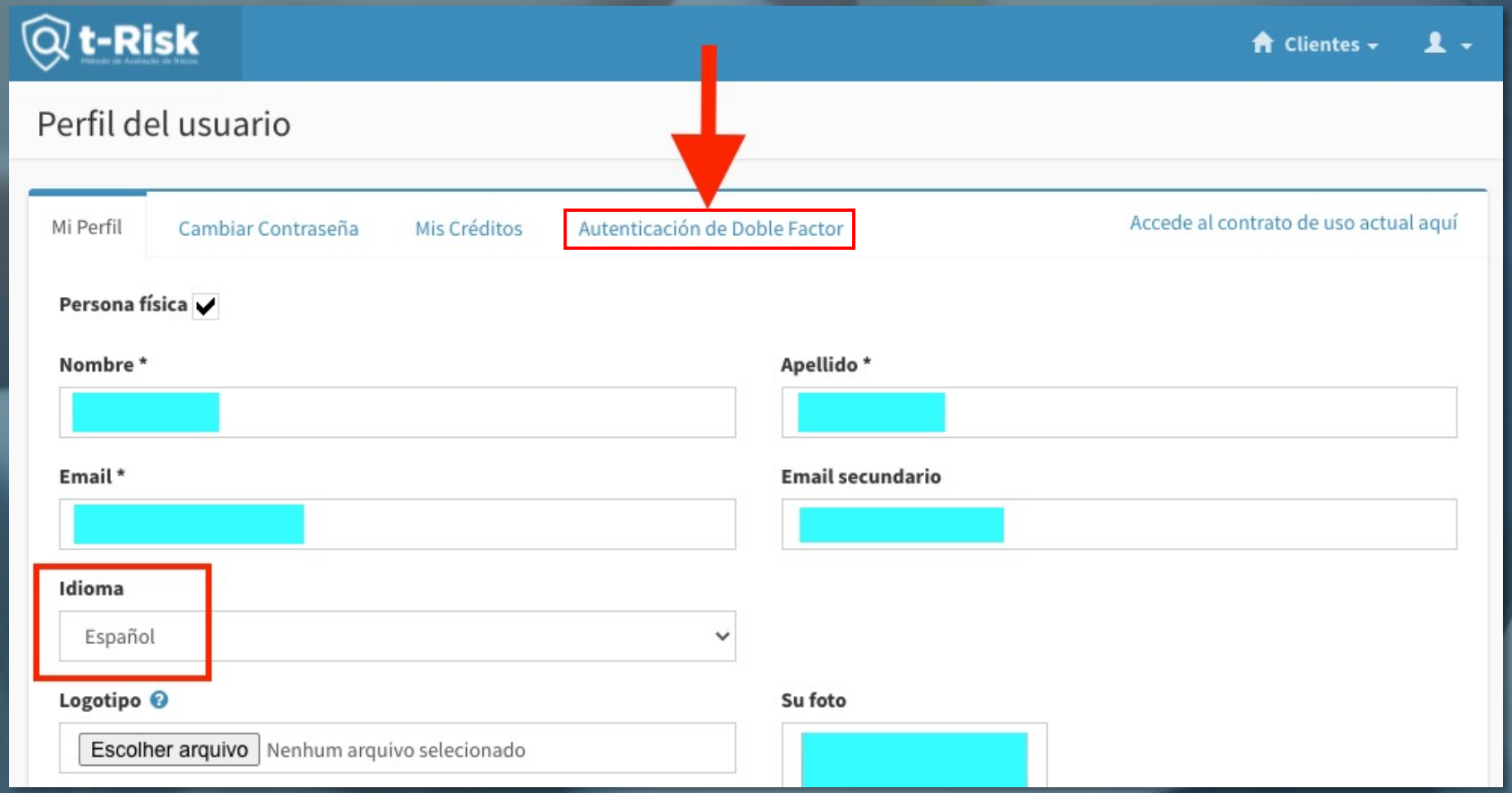
Una capa extra de seguridad. La mayoría de las personas tienen solo una capa para proteger sus cuentas: su contraseña. Con la verificación de 2 pasos, si un hacker informático irrumpe en su capa de contraseña, también necesitará su smartphone con la *App Google Authenticator* para iniciar sesión en su cuenta.

Iniciar sesión requerirá algo que sepa y algo que tenga. Con la verificación en 2 pasos, protege su cuenta con algo que sabe (su contraseña) y algo que tiene (su smartphone con la *App Google Authenticator*).

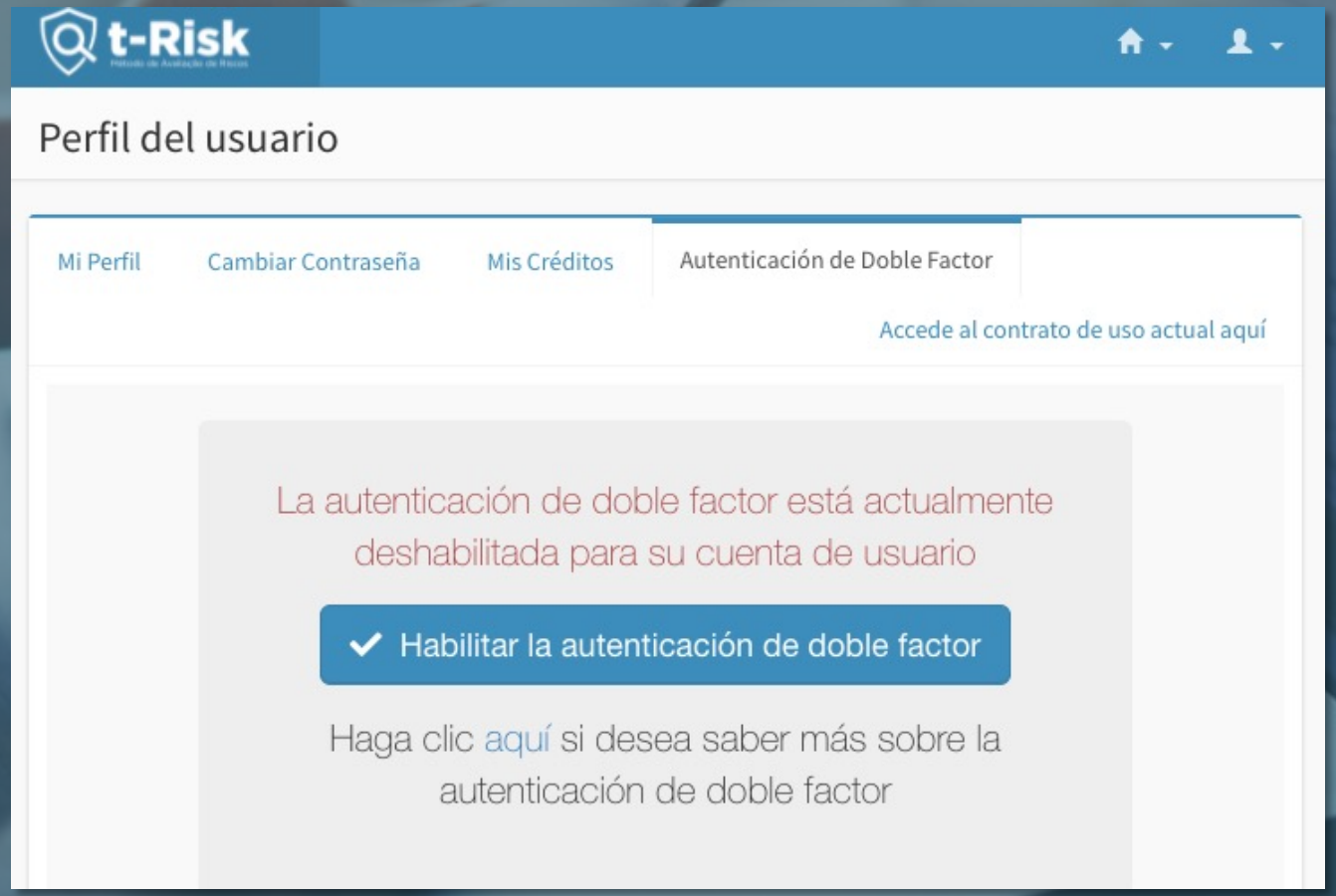
¿Cómo te protege?

Códigos de verificación creados solo para ti. Los códigos se crean exclusivamente para su cuenta cuando los necesita. Cada código solo se puede usar una vez.

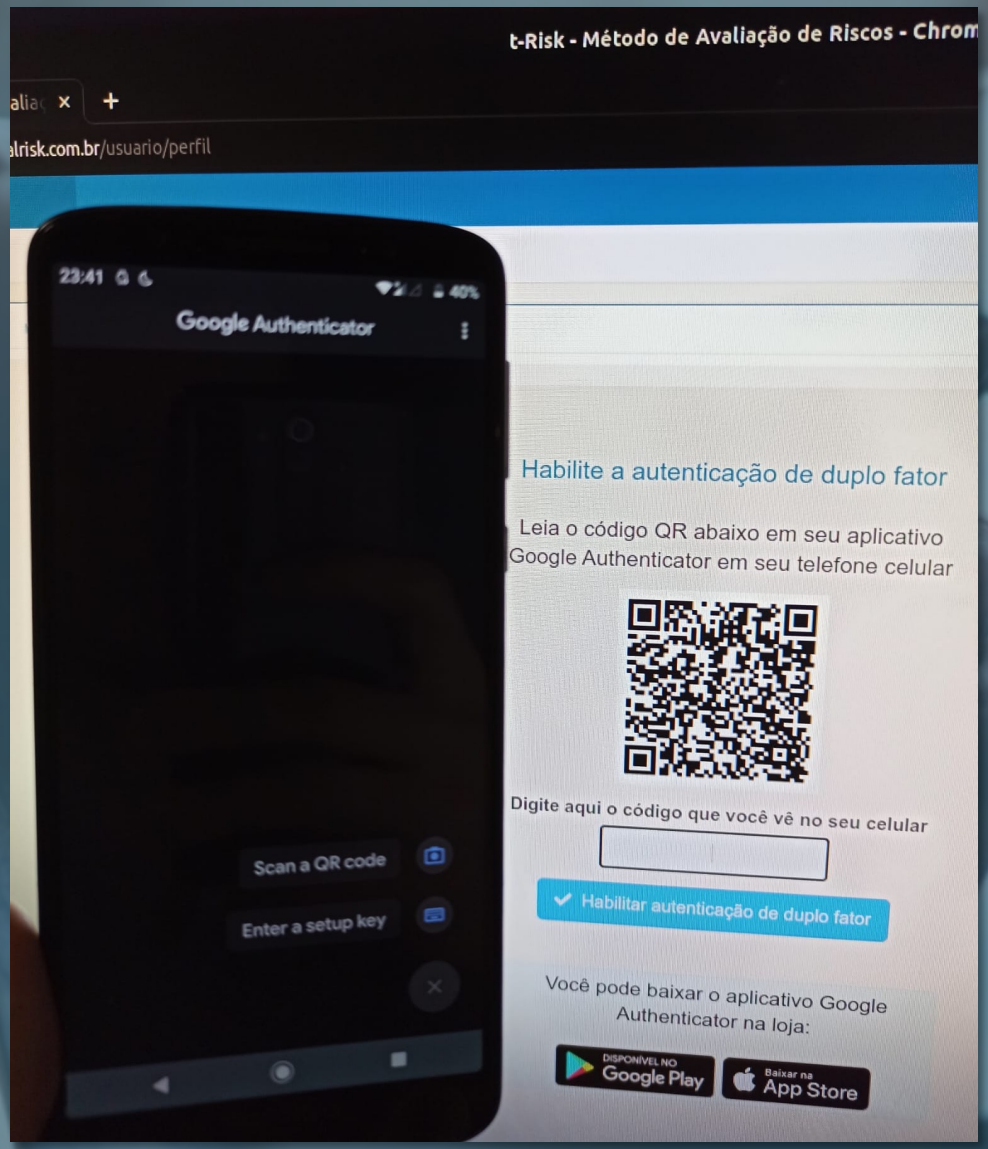
Siga los pasos a continuación para habilitar la autenticación de dos factores en la plataforma t-Risk.



1 Acceda a su perfil de usuario y haga clic en la pestaña "Autenticación de doble factor".



2 Haga clic en el botón "Habilitar autenticación de doble factor".

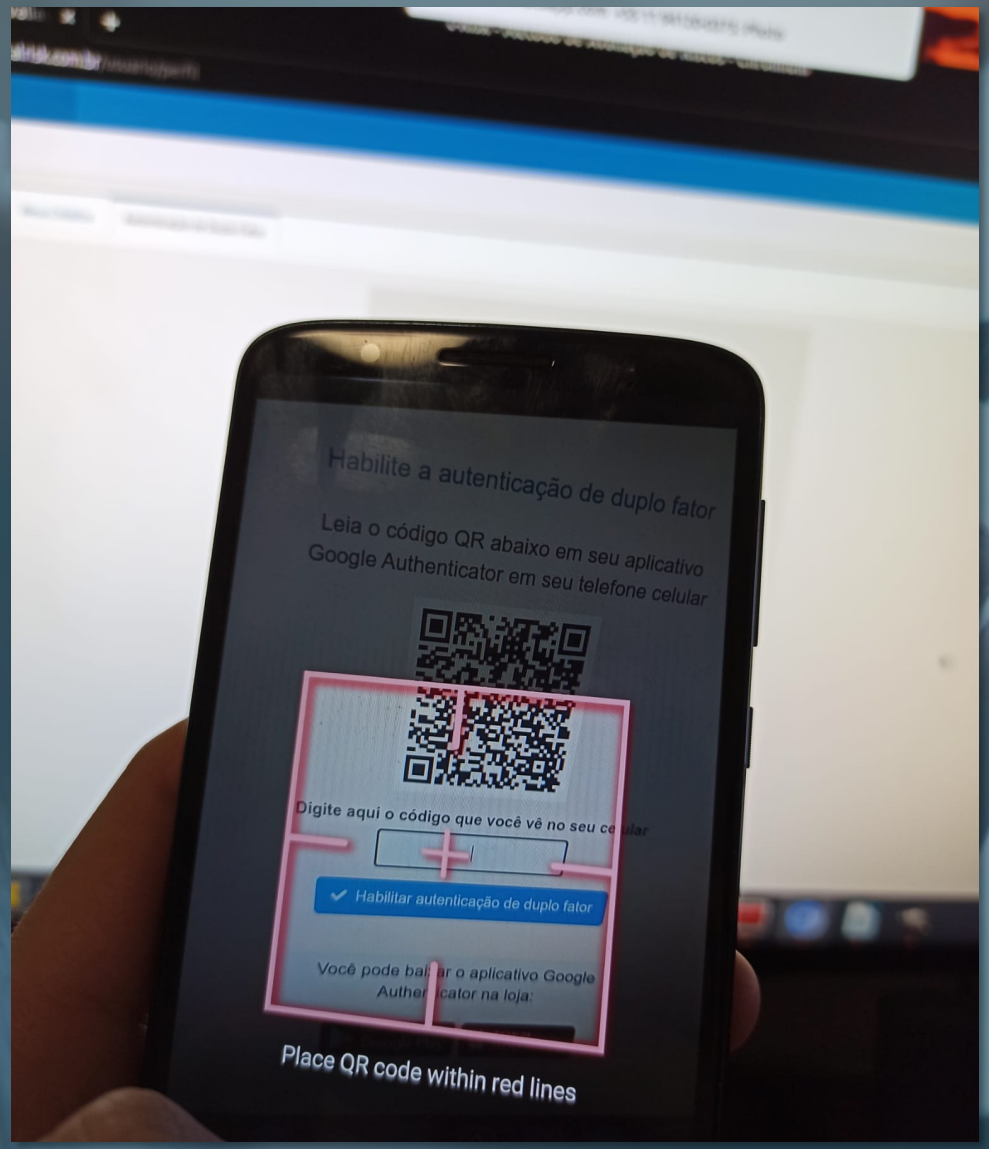


3 Abra la aplicación *Google Authenticator* en su móvil. Si aún no tiene la aplicación instalada, use los enlaces de la página para descargarla.

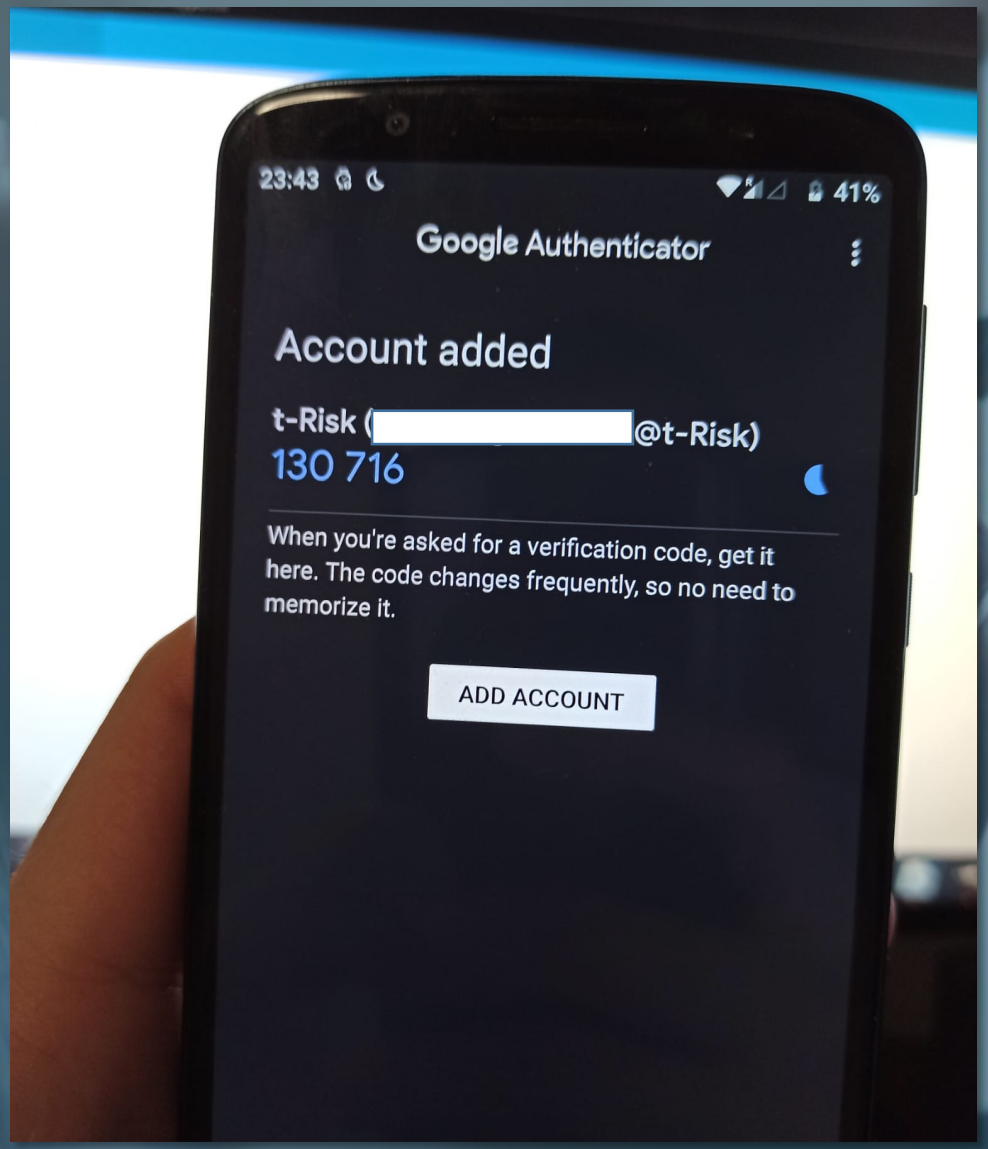
¿Sin conexión? Sin problemas. La aplicación *Google Authenticator* para Android, iPhone o BlackBerry puede generar códigos de verificación. Funciona incluso cuando su dispositivo no tiene conexión de datos o teléfono.

Enlace a Apple
https://apps.apple.com/br/app/google-authenticator/id388497605

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



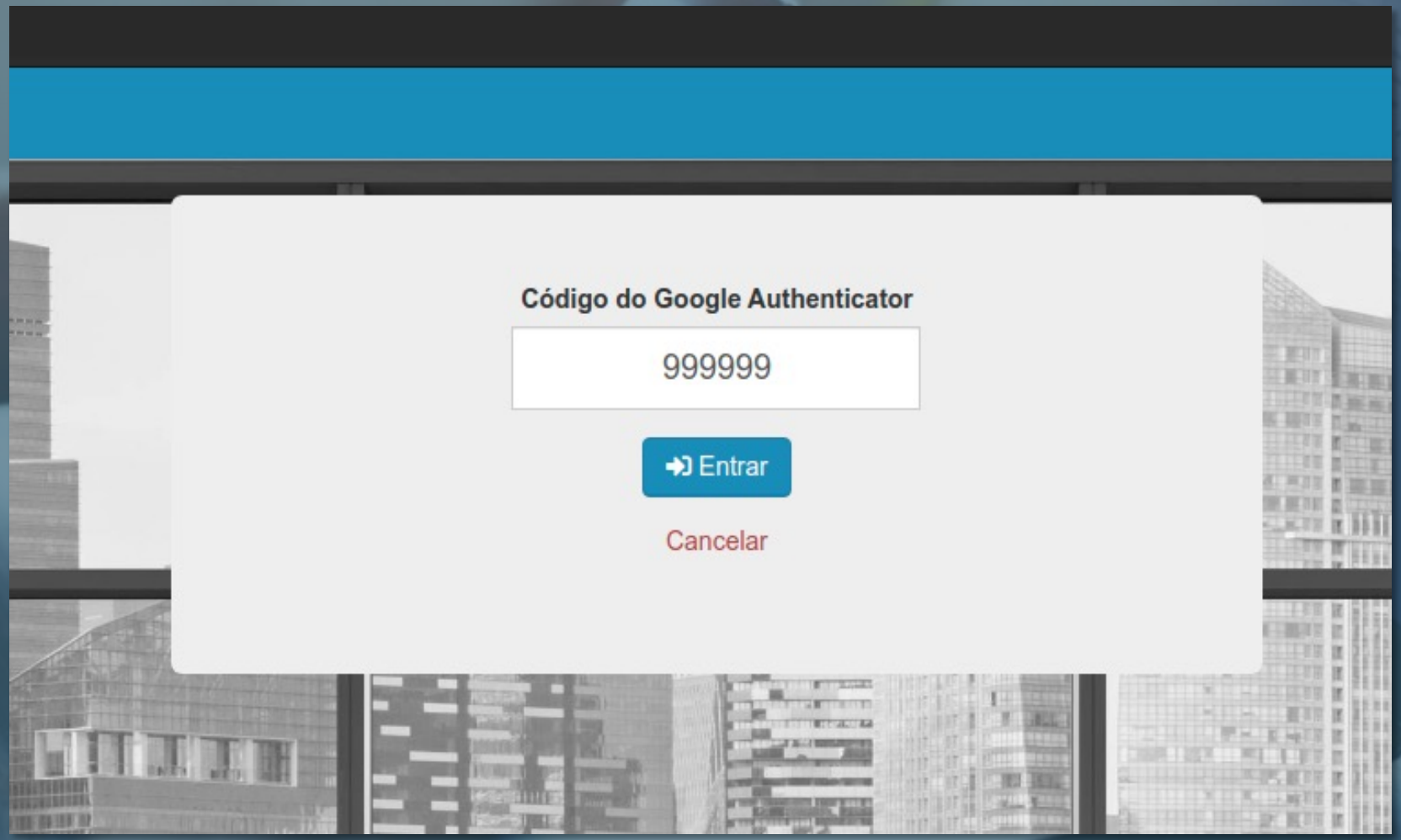
4 Luego deberá escanear la imagen que se muestra en la aplicación.



5 Una vez escaneada correctamente la imagen, verá su cuenta registrada en la aplicación con un código para la primera validación.

6 Ingrese el código que se muestra en la aplicación *Google Authenticator* en este campo y haga clic en "habilitar la autenticación de doble factor".

7 Debería ver la confirmación de que la autenticación de dos factores se ha habilitado correctamente.



8

Desde su próximo acceso, justo después de ingresar el nombre de usuario y la contraseña, deberá ingresar el código del App *Google Authenticator* para continuar en el sistema.

t-Risk

Método de Avaliação de Riscos

Badge t-Risk Practitioner

¡Agregue la insignia t-Risk a su historial de trabajo y compártala!

Para mas información contáctenos.