

# Presto Start

**Sobre este capítulo** — Reúne os artigos de onboarding e configuração do *Presto Start*, o produto gratuito de 2FA compartilhado da Oystre. Guiam o cliente do cadastro da conta até o uso diário dos códigos pela extensão.

- [O que é o Presto Start](#)
- [Como criar sua conta no Presto Start](#)
- [Como cadastrar sua primeira chave 2FA](#)
- [Como exportar os códigos do Google Authenticator](#)
- [Como convidar sua equipe e adicionar usuários](#)
- [Como cadastrar a chave de 2FA depois do primeiro acesso](#)
- [Como instalar a extensão do Presto no Chrome](#)
- [Como usar os códigos 2FA](#)
- [Perguntas Frequentes \(FAQ\)](#)

# O que é o Presto Start

**Resumo** — Explica o que é o *Presto Start*, qual problema de 2FA ele resolve e como a equipe passa a acessar sistemas sem depender de um único celular. Leia antes de começar a configuração.

## O que é

O *Presto Start* é um **cofre compartilhável para as chaves de 2FA da equipe**: gratuito, sem cartão e ativado pelo próprio cliente. O administrador cadastra a chave secreta do 2FA uma única vez, e a equipe passa a ver o **código TOTP** no momento do login — sem nunca ver a credencial original.

## O problema que ele resolve

Escritórios e empresas compartilham credenciais todo dia, por WhatsApp, planilha ou na memória de alguém. Quando o token de 2FA fica em um único celular, a operação depende de quem está com o aparelho na mão: se essa pessoa sai ou está indisponível, todo protocolo, assinatura ou acesso crítico para.

O *Presto Start* coloca esse 2FA em um cofre digital compartilhável. A equipe acessa os sistemas sem ver, copiar ou guardar a credencial original, e o administrador define quem pode usar cada chave.

## Como funciona no dia a dia



Figura 1 — A extensão do Presto entrega os códigos 2FA no navegador, prontos para copiar.

No login de um portal, o fluxo passa a ser:

1. O usuário entra com login e senha, como sempre fez.
2. O portal pede o código de verificação — em vez de procurar alguém, o usuário clica na extensão do Presto.
3. A extensão mostra o código da chave que o administrador cadastrou; o usuário copia com um clique.
4. Ele cola no portal e está dentro — sem nunca ter visto a chave secreta.

São poucos segundos, no lugar de minutos esperando um colega responder.

# Como criar sua conta no Presto Start

**Resumo** — Passo a passo para criar a conta do *Presto Start* a partir da landing page e chegar ao primeiro acesso ao console. É totalmente self-service: nenhuma etapa depende do time da Oystre.

## Pré-requisitos

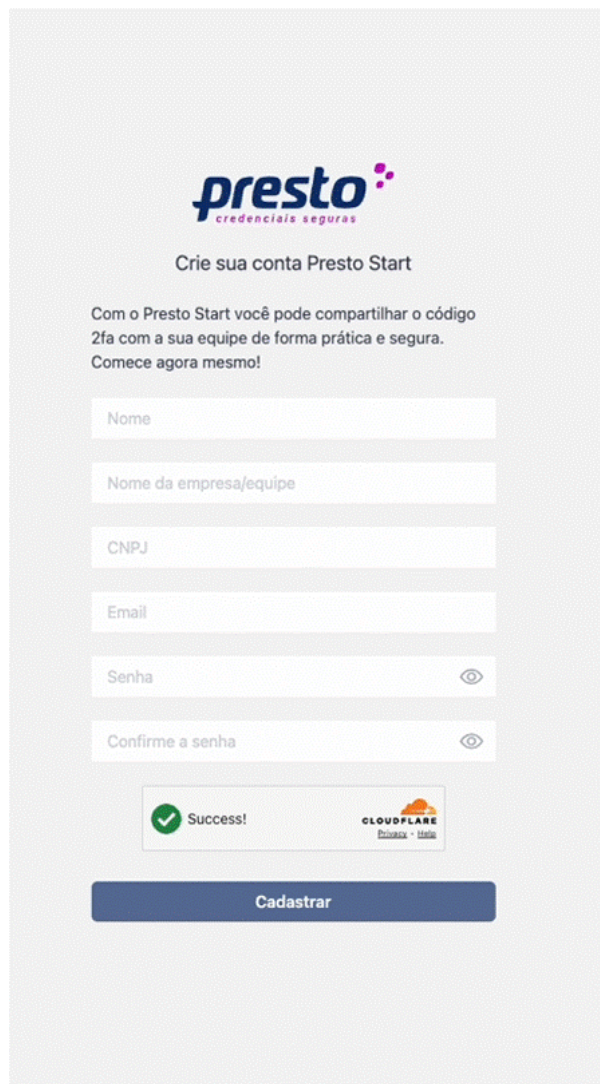
- E-mail (recomendado usar o e-mail corporativo da empresa)
- Dados da empresa: nome, CNPJ

## 1. Acessar a landing page

Acesse a página do produto: [conteudo.oyster.com.br/presto-start](https://conteudo.oyster.com.br/presto-start) e clique em **Garantir meu acesso**.

## 2. Preencher o cadastro

Na página de registro ([console.presto.oyster.com.br/register](https://console.presto.oyster.com.br/register)), preencha nome, empresa, CNPJ, e-mail e senha. Leia e aceite os termos de uso e clique em **Cadastrar**. Não é necessário cartão nem contato comercial.



The image shows a web form for creating a Presto Start account. At the top is the Presto logo with the tagline 'credenciais seguras'. Below the logo is the heading 'Crie sua conta Presto Start'. A paragraph explains that with Presto Start, users can share a 2FA code with their team in a practical and secure way, encouraging them to start now. The form consists of several input fields: 'Nome', 'Nome da empresa/equipe', 'CNPJ', 'Email', 'Senha', and 'Confirme a senha'. The 'Senha' and 'Confirme a senha' fields have eye icons to toggle visibility. Below the fields is a success message 'Success!' with a green checkmark icon and the Cloudflare logo. At the bottom is a blue button labeled 'Cadastrar'.

Figura 1 — Formulário de criação da conta do Presto Start.

### 3. Primeiro acesso ao console

Após o cadastro, você chega ao console. O estado inicial está vazio e conduz direto para a próxima ação: cadastrar o primeiro 2FA.

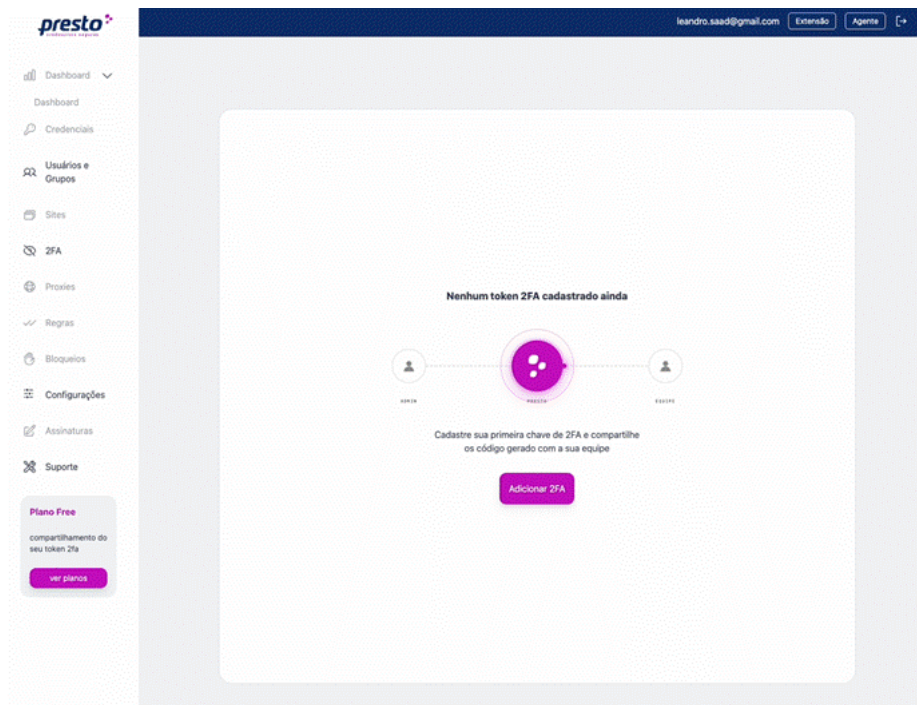


Figura 2 — Console após o cadastro, com o botão para adicionar o primeiro 2FA.

# Como cadastrar sua primeira chave 2FA

**Resumo** — Como cadastrar no *Presto Start* a chave secreta de 2FA de um portal, digitando-a ou importando por QR code, e conferir o código gerado.

## Pré-requisitos

- Conta no *Presto Start* criada
- A chave secreta do 2FA do portal (ou o QR code / o app Google Authenticator com a chave)

## 1. Primeiro acesso ao console

Após o cadastro, você chega ao console. O estado inicial está vazio e conduz direto para a próxima ação: cadastrar o primeiro 2FA.

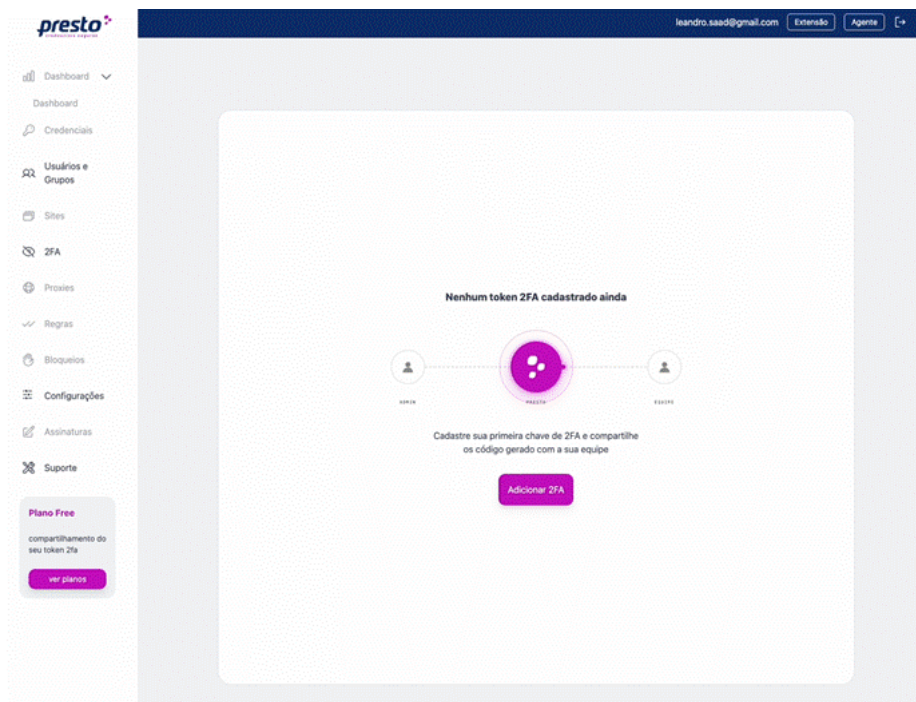
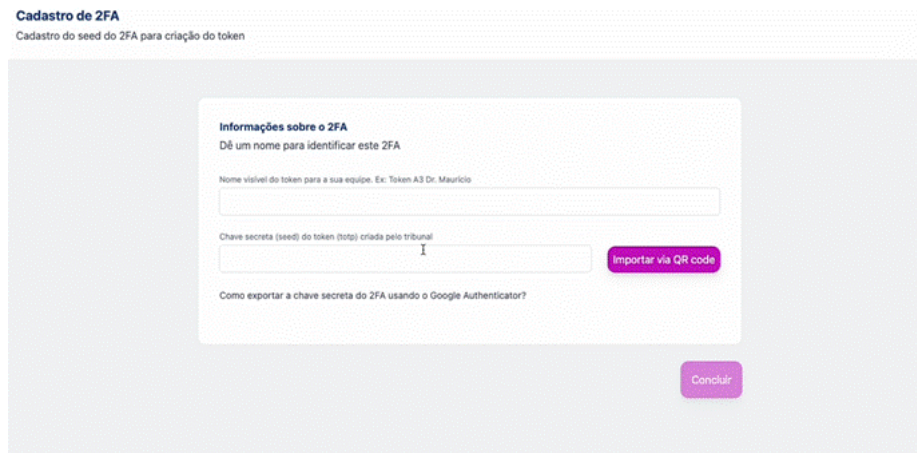


Figura 1 — Console após o cadastro, com o botão para adicionar o primeiro 2FA.

## 2. Abrir o cadastro de 2FA

No console, clique em **Adicionar 2FA**. Na tela **Informações sobre a 2FA**, dê um **nome** para identificar esse 2FA (por exemplo, o nome do portal e do usuário).



**Cadastro de 2FA**  
Cadastro do seed do 2FA para criação do token

**Informações sobre o 2FA**  
Dê um nome para identificar este 2FA

Nome visível do token para a sua equipe. Ex: Token A3 Dr. Maurício

Chave secreta (seed) do token (otp) criada pelo tribunal

Importar via QR code

Como exportar a chave secreta do 2FA usando o Google Authenticator?

Concluir

Figura 1 — Tela de cadastro de 2FA, com o campo da chave secreta e a opção de importar via QR code.

## 3. Informar a chave secreta

Você pode cadastrar a chave de duas formas:

- **Digitar a chave** secreta manualmente no campo indicado; ou
- Clicar em **Importar via QR code** e apontar a câmera para o QR code do portal.

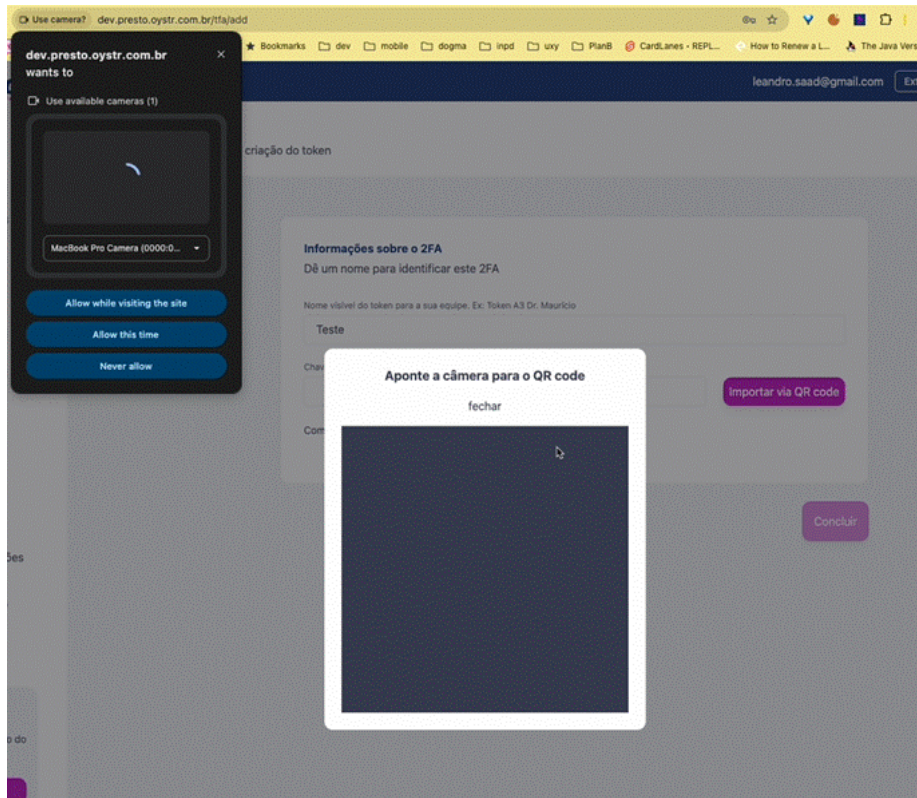


Figura 2 — Leitura da chave por QR code.

## 4. Conferir o código cadastrado

Ao salvar, o *Presto* exibe o **código TOTP** já gerado (campo **Código Cadastrado**). Confira se ele é igual ao código exibido no seu celular para garantir que a chave foi cadastrada corretamente.

### Informações sobre o 2FA

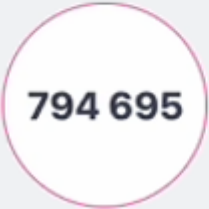
Dê um nome para identificar este 2FA

Nome visível do token para a sua equipe. Ex: Token A3 Dr. Maurício

Chave secreta (seed) do token (totp) criada pelo tribunal

[Importar via QR code](#)

Como exportar a chave secreta do 2FA usando o Google Authenticator?

794 695

### Código Cadastrado

Este é o código 2FA (totp) gerado pela chave acima. Este código se renova automaticamente a cada 30 segundos. Ele será compartilhado com os membros da sua equipe pela extensão do Presto

Figura 3 — Console após o cadastro, com o botão para adicionar o primeiro 2FA.

Se a chave que você quer cadastrar está no Google Authenticator, veja antes Como exportar a chave do Google Authenticator.

# Como exportar os códigos do Google Authenticator

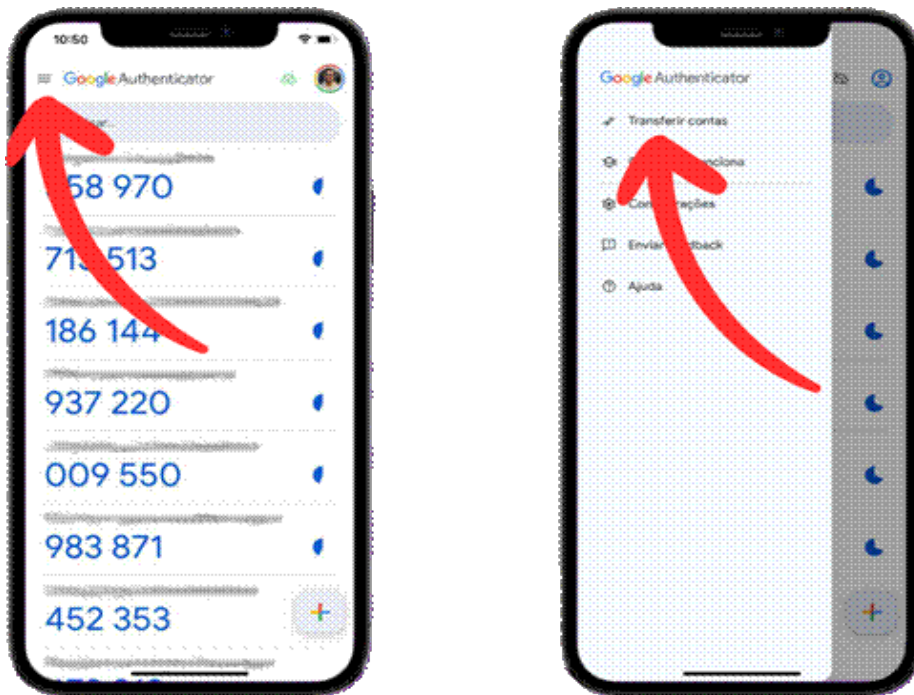
**Resumo** — Como retirar a chave secreta de um 2FA que já está no Google Authenticator e importá-la no *Presto*. Este é o passo que costuma gerar mais dúvida na ativação.

## Pré-requisitos

- App **Google Authenticator** no celular, com a conta de 2FA desejada
- Tela de cadastro de 2FA aberta no *Presto* (com a opção **Importar via QR code**)

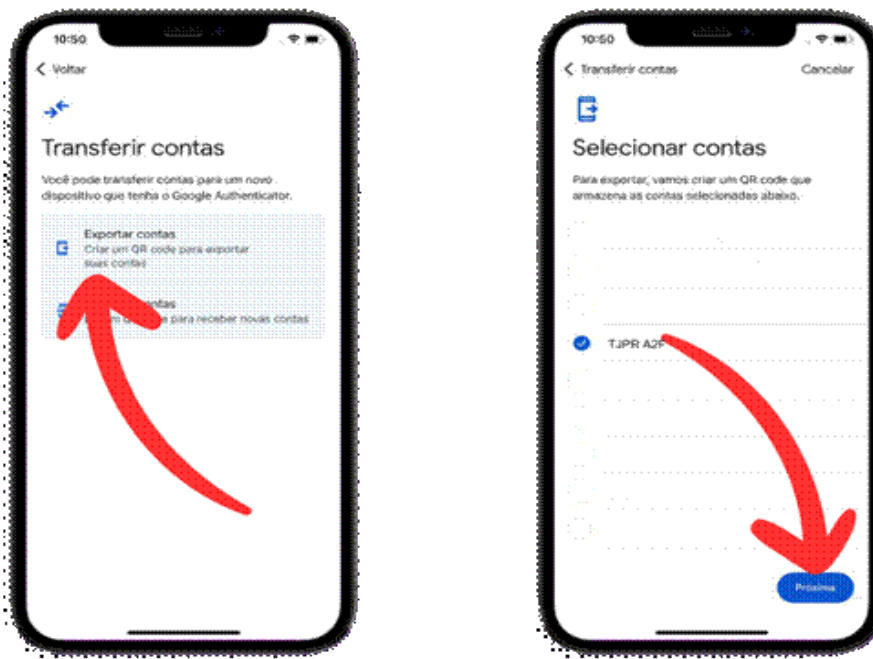
## Como transferir os códigos do Google Authenticator

1. Acesse a função "Transferir contas" do Google Authenticator.



Abra o Google Authenticator no celular "antigo" com a Conta Google logada. Toque no botão de três riscos, no canto superior esquerdo, e selecione a opção "Transferir contas".

## 2. Selecione "Exportar contas".



*Toque em "Exportar contas" e selecione o código do site que deseja transferir para o Presto. Depois, toque em "Próxima" para continuar.*

**Atenção:** exporte apenas o código do site que está cadastrando. Caso selecione mais de uma conta, o cadastro pode não funcionar corretamente.

## 3. Obtenha o QR Code gerado.



*O Google Authenticator irá gerar o QR code que deve ser lido na plataforma do Presto.*

# Erros Comuns / Troubleshooting

| Problema                                       | Causa provável                                                                        | Solução                                                              |
|------------------------------------------------|---------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| O <i>Presto</i> não importa a chave do QR code | Foram selecionadas várias contas na exportação, gerando um único QR com várias chaves | Exporte <b>uma conta por vez</b> e repita o processo para cada chave |

# Como convidar sua equipe e adicionar usuários

**Resumo** — Como dar acesso aos códigos 2FA para as pessoas do seu time. Os convidados passam a ver o código, mas nunca a chave secreta original.

## Pré-requisitos

- Pelo menos uma chave 2FA cadastrada
- E-mails das pessoas do time que terão acesso

## 1. Adicionar os e-mails do time

Na tela da chave (**Informações sobre a 2FA**), localize a seção **Compartilhe com seu time** e adicione o e-mail de cada pessoa que poderá usar aquele código. Em seguida, clique em **Concluir**.

A interface de configuração de 2FA é exibida em um container cinza claro. No topo, o título "Informações sobre o 2FA" é seguido por um campo de texto para "Dê um nome para identificar este 2FA" com o valor "Teste". Abaixo, há uma seção para a "Chave secreta (seed) do token (totp) criada pelo tribunal" com um campo de texto contendo pontos e um botão "Importar via QR code". Uma pergunta sobre exportar a chave secreta usando o Google Authenticator aparece abaixo. O centro da interface destaca o "Código Cadastrado" "794 695" em um círculo, com uma explicação de que se renova a cada 30 segundos. A seção "Compartilhe com seu time" contém um campo de texto para adicionar e-mails, com "leandro@oysttr.com.br" já adicionado. Um botão "Concluir" está no canto inferior direito.

Figura 1 — Código cadastrado e campo para compartilhar o 2FA com o time.

## 2. O convite por e-mail

Cada pessoa convidada recebe um **e-mail de convite**. Ao aceitar, ela passa a fazer parte da organização e a visualizar os códigos pela extensão do *Presto*.

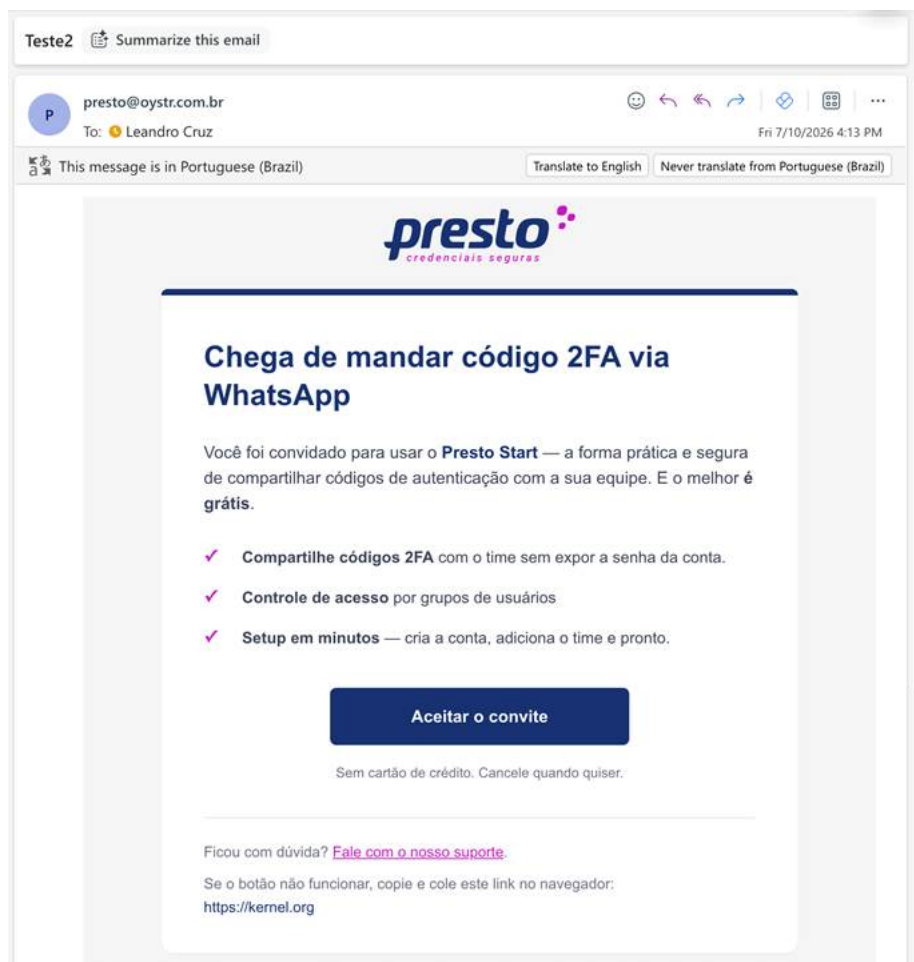


Figura 2 — E-mail de convite recebido pelo usuário.

**Adicionando usuários após o onboarding** — Para adicionar usuários posteriormente você deverá ir em **Usuários e Grupos > Lista de Usuários > Adicionar novo usuário**

# Como cadastrar a chave de 2FA depois do primeiro acesso

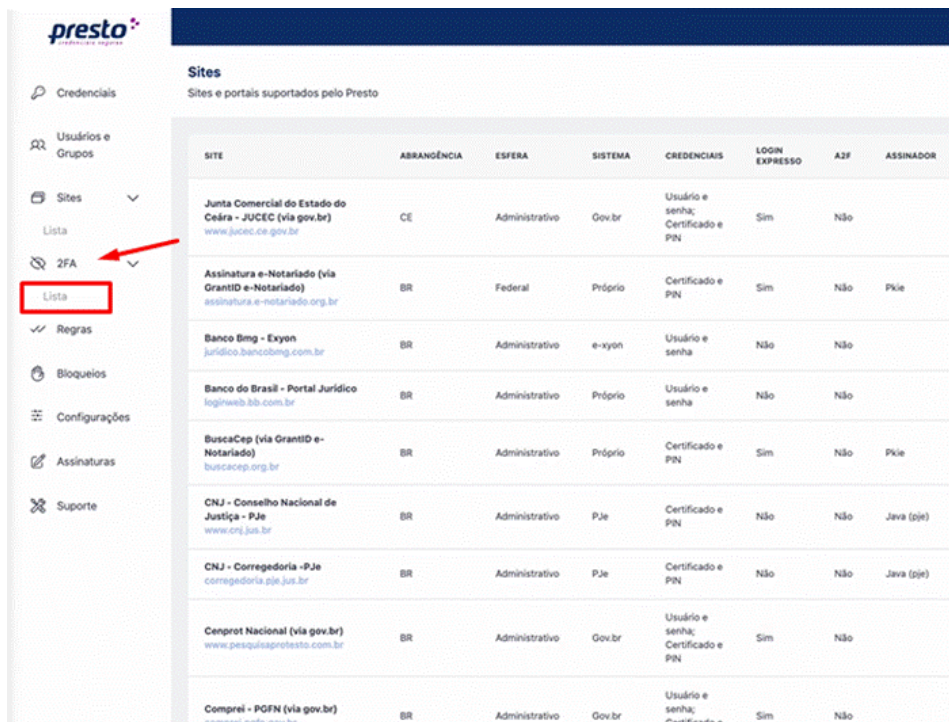
Nesta seção, você aprenderá a configurar a autenticação de dois fatores (2FA) no nosso Console. Iremos guiá-lo no processo de ativar a autenticação e vinculá-la à sua conta de forma segura.

Para iniciar, é importante que você já tenha em mãos a chave ou o QR code para exportar para o Console do PRESTO. Abaixo, apresentamos um passo a passo para obter essa informação.

Caso não saiba como exportar a chave do Google Authenticator acesse esse guia [Como exportar os códigos de 2FA do Google Authenticator | Oystripedia](#)

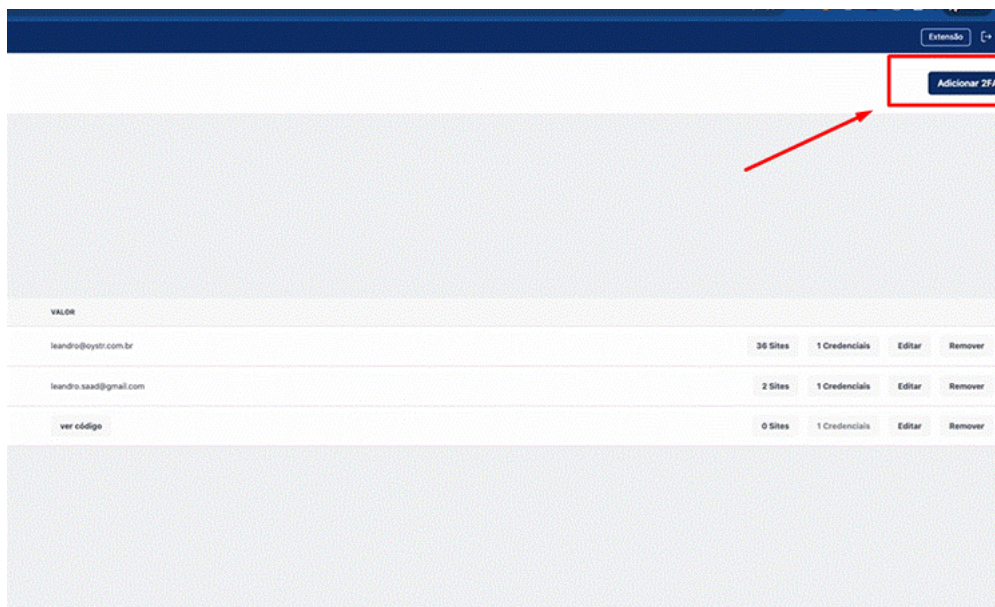
## **Como cadastrar a chave de 2FA no PRESTO**

1. Para inserir a chave de autenticação de dois fatores no **Console do PRESTO**, localize no menu principal, no canto esquerdo da página, a opção **"2FA"** e, em seguida, **"Lista"**.



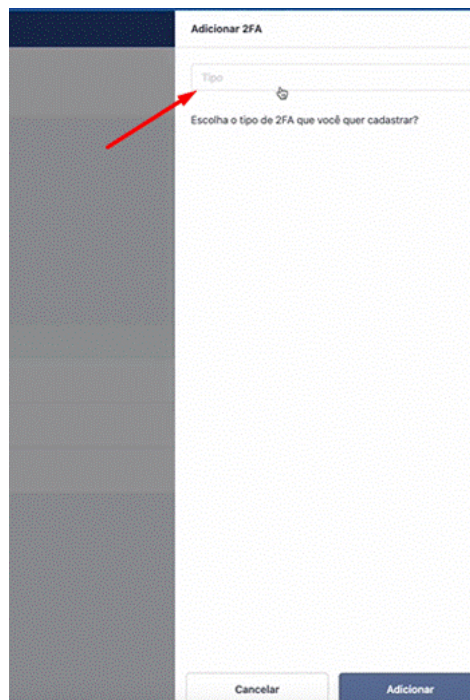
Menu "2FA" > "Lista" no Console do Presto.

2. Clique no botão **"Adicionar 2FA"**.



Botão "Adicionar 2FA".

3. Selecione o tipo de 2FA que deseja adicionar (E-mail ou Token Baseado em tempo).

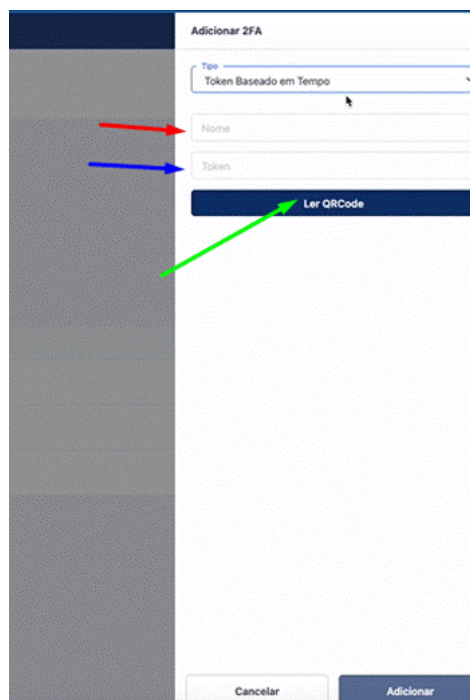


The screenshot shows a mobile application interface for adding 2FA. The title bar at the top is dark blue with the text 'Adicionar 2FA'. Below the title bar is a dropdown menu labeled 'Tipo' with a downward arrow. Below the dropdown is the text 'Escolha o tipo de 2FA que você quer cadastrar?'. At the bottom of the screen are two buttons: 'Cancelar' (light gray) and 'Adicionar' (dark blue).

*Seleção do tipo de 2FA.*

4. Selecionando o Token Baseado em tempo, preencha os campos indicados na tela, conforme a legenda abaixo:

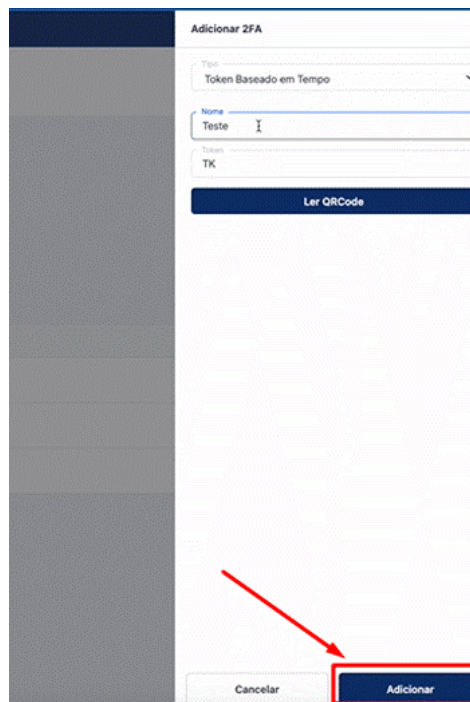
- **Vermelho:** Nome do 2FA — para que você possa localizar na lista de 2FA cadastradas.
- **Azul:** Token — caso prefira inserir o código token em vez de ler o QR code.
- **Verde:** Ler QR code — para leitura do QR code em vez de digitar o código Token.



The screenshot shows the same mobile application interface as before, but with the 'Tipo' dropdown menu set to 'Token Baseado em Tempo'. Below the dropdown are two input fields: 'Nome' and 'Token'. Below these fields is a dark blue button labeled 'Ler QRCode'. At the bottom of the screen are two buttons: 'Cancelar' (light gray) and 'Adicionar' (dark blue). Red and blue arrows point to the 'Nome' and 'Token' fields respectively. A green arrow points to the 'Ler QRCode' button.

*Campos de cadastro do token baseado em tempo.*

5. Após preencher esses campos, clique em **"Adicionar"**.



The screenshot shows a mobile application interface for adding a 2FA token. The form is titled "Adicionar 2FA" and contains the following fields:

- Tip:** A dropdown menu with "Token Baseado em Tempo" selected.
- Nome:** A text input field containing "Teste".
- Token:** A text input field containing "TK".

Below the "Token" field is a button labeled "Ler QRCode". At the bottom of the form are two buttons: "Cancelar" and "Adicionar". A red arrow points from the bottom left towards the "Adicionar" button, which is highlighted with a red rectangular border.

*Confirmação com o botão "Adicionar".*

# Como instalar a extensão do Presto no Chrome

**Resumo** — Como instalar a extensão do *Presto* no navegador, por onde os códigos 2FA são exibidos no momento do login.

## Pré-requisitos

- Navegador **Google Chrome** (a extensão funciona apenas no Chrome; Firefox e Safari ainda não são suportados)
- Convite aceito ou conta com acesso aos códigos

## Passo a passo

1. Abra a **Chrome Web Store**.
2. Localize a extensão **Presto** ou acesse em: **Presto - Chrome Web Store**

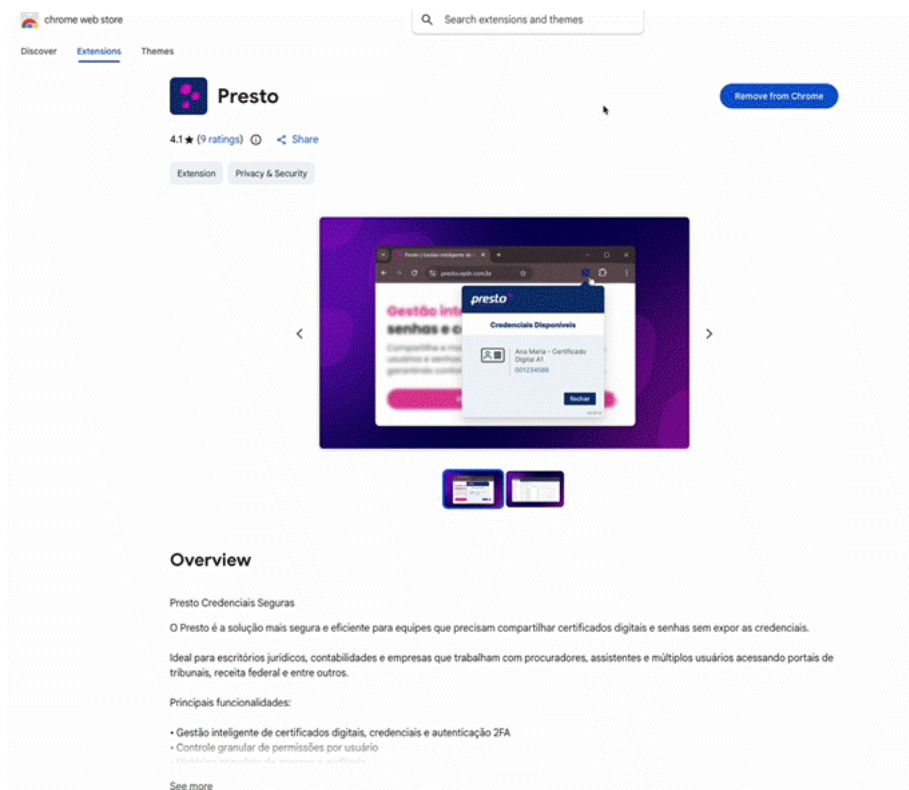


Figura 1 — Página da extensão Presto na Chrome Web Store.

1. Clique em **Adicionar ao Chrome** e **confirme as permissões**.
2. **Fixe** a extensão na barra do navegador para acesso rápido no dia a dia.

## Cadastro de 2FA

Cadastro do seed do 2FA para criação do token

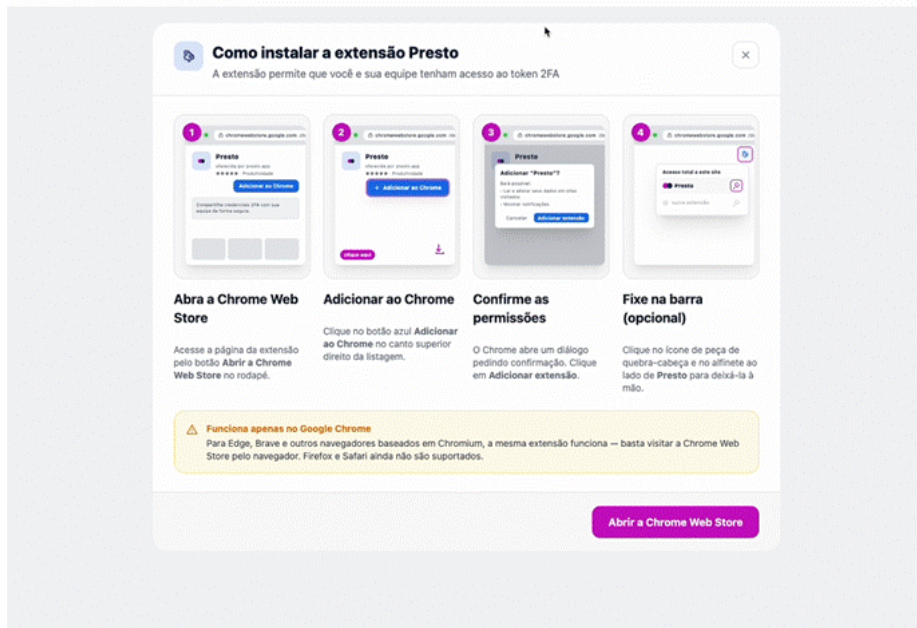


Figura 2 — Instalação da extensão em quatro passos.

**Resultado esperado:** o ícone do *Presto* aparece na barra do navegador, pronto para exibir os códigos 2FA.

# Como usar os códigos 2FA

**Resumo** — Como copiar o código 2FA pela extensão do *Presto* e concluir o login em um portal. É o uso do dia a dia, depois que a conta, as chaves e a extensão já estão configuradas.

## Pré-requisitos

- Extensão do *Presto* instalada e fixada no navegador
- Acesso a pelo menos uma chave 2FA (própria ou compartilhada com você)

## Passo a passo

1. Faça login no portal com **usuário e senha**, como de costume.
2. Quando o portal pedir o **código de verificação**, clique no ícone da extensão do *Presto*.
3. Na aba **2FA**, localize o código desejado. Use o campo **Filtro** para encontrar rapidamente pelo nome.

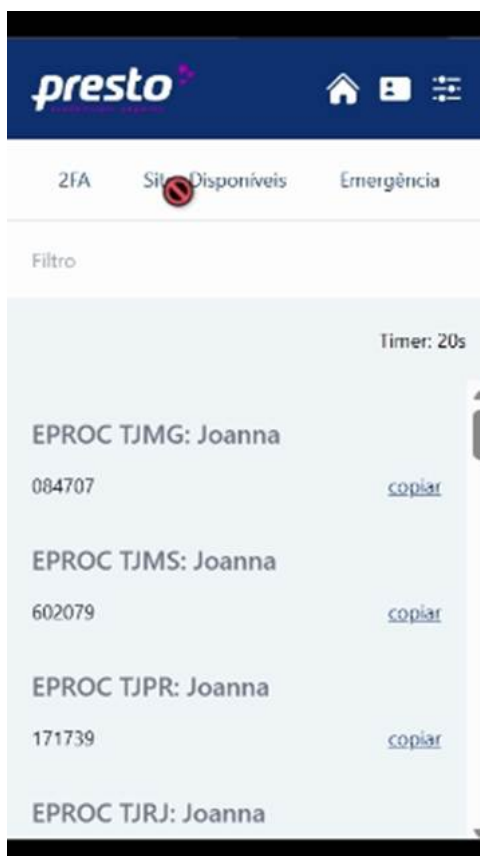


Figura 1 — Lista de códigos 2FA na extensão, com botão de copiar em cada item.

1. Clique em **copiar** ao lado do código.



Figura 2 — Uso do filtro para localizar rapidamente um código.

1. **Cole** o código no portal e conclua o login.

O código é temporário: um **timer** indica o tempo restante. Se ele expirar antes de você colar, copie novamente o código atualizado.

# Perguntas Frequentes (FAQ)

**Resumo** — Reúne as dúvidas mais comuns sobre o *Presto Start*: o que é, como funciona o cadastro, as chaves 2FA, o convite da equipe, a extensão e a segurança. Consulte esta página para respostas rápidas; para os passos detalhados, use os artigos indicados em cada resposta.

## 1.Sobre o produto

### O que é o Presto Start?

O *Presto Start* é um **cofre compartilhável para as chaves de 2FA da equipe**. O administrador cadastra a chave secreta do 2FA uma única vez e a equipe passa a ver o **código de verificação (TOTP)** no momento do login, pela extensão do navegador — sem nunca ter acesso a chave secreta que gera o código de 2FA.

### O Presto Start é realmente gratuito? Preciso de cartão?

Sim, é gratuito até 5 chaves MFA e até 15 usuários. Não é necessário cartão de crédito nem contato comercial: o cadastro é aberto e **100% self-service**. Você lê e aceita os termos de uso e já começa a usar.

### Qual a diferença entre o Presto Start e o Presto completo?

O *Presto Start* cobre o compartilhamento de 2FA. O *Presto* completo acrescenta o cofre de credenciais, controles avançados e automações. Resumo:

| Recurso                                      | Presto Start · grátis | Presto · completo  |
|----------------------------------------------|-----------------------|--------------------|
| Compartilhamento de 2FA                      | Incluído              | Incluído           |
| Gestão de chaves de MFA                      | Incluído              | Incluído           |
| Acesso via extensão do Chrome                | Incluído              | Incluído           |
| Cofre de credenciais e certificados digitais | —                     | Incluído           |
| Controle granular por IP, horário e perfil   | —                     | Incluído           |
| Auditoria completa e dashboards              | —                     | Incluído           |
| SmartLogin e assinatura digital              | —                     | Incluído           |
| Suporte                                      | E-mail                | Chat em tempo real |

## Preciso falar com o time comercial para começar?

Não. Nenhuma etapa da ativação — cadastro, primeira chave, convite do time e extensão — depende do time da Oystre.

## 2. Conta e cadastro

### Como crio uma conta?

Pela landing page ([conteudo.oystre.com.br/presto-start](https://conteudo.oystre.com.br/presto-start)), que leva à página de registro. O passo a passo está em *Como criar sua conta no Presto Start*.

### Que dados preciso informar no cadastro?

Nome, empresa, CNPJ, e-mail e senha, além de aceitar os termos de uso. Recomendamos usar o **e-mail corporativo** da empresa.

## 3. Chaves 2FA

### O que é a "chave 2FA" e o "código TOTP"?

A **chave 2FA** é o segredo do autenticador de um portal (a mesma chave que hoje fica no app do celular). A partir dela, o *Presto* gera o **código TOTP** — o número temporário de verificação que você informa no login.

### Como cadastro uma chave 2FA?

Você pode digitar a chave secreta ou importá-la por QR code. Veja *Como cadastrar sua primeira chave 2FA*.

### Minha chave está no Google Authenticator. Como faço?

É possível exportá-la do app e importar no *Presto* por QR code. O passo a passo está em *Como exportar a chave do Google Authenticator*.

### Escaneei o QR code e o Presto não importou a chave. Por quê?

Provavelmente foram **selecionadas várias contas** ao exportar do Google Authenticator, o que gera um único QR com várias chaves — e o *Presto* não consegue importar assim. Exporte **uma conta por vez** e repita o processo para cada chave.

## Por quanto tempo o código é válido?

O código é temporário e **se renova automaticamente a cada 30 segundos**. Um *timer* na extensão indica o tempo restante; se ele expirar antes de você colar, copie o código atualizado.

## Quantas chaves posso cadastrar?

Você pode cadastrar **várias chaves** — uma para cada portal ou 2FA que precisar compartilhar com o time.

# 4. Equipe e acesso

## Como convido pessoas do meu time?

Na tela da chave, em **Compartilhe com seu time**, adicione os e-mails de quem terá acesso. Cada convidado recebe um e-mail de convite. Veja *Como convidar sua equipe*.

## Os convidados conseguem ver a chave secreta?

Não. Os convidados veem apenas o **código gerado**, nunca a chave secreta original.

## Posso escolher quem acessa cada chave?

Sim. O compartilhamento é **por chave**: você define os grupos que terão acesso a cada 2FA cadastrado.

## E se um colaborador sair da empresa?

Como o acesso é compartilhado pela organização e não fica preso ao celular de uma pessoa, o controle permanece **centralizado no administrador** — o time não perde o acesso quando alguém sai.

# 5. Extensão e uso no dia a dia

## Em qual navegador a extensão funciona?

Na extensão do **Google Chrome**. Ela também funciona em navegadores baseados em Chromium, como **Edge** e **Brave** (basta abrir a Chrome Web Store pelo próprio navegador). **Firefox** e **Safari** ainda não são suportados.

## Como instalo a extensão?

Pela Chrome Web Store, em poucos passos. Veja *Como instalar a extensão do Presto no Chrome*.

## É a mesma extensão do Presto completo?

Sim. É a extensão pública da Chrome Web Store, a mesma que atende os clientes da versão *Presto*, porém apenas com a funcionalidade do 2FA.

## Como uso o código no login de um portal?

Faça login normalmente; quando o portal pedir o código, abra a extensão, localize o 2FA (use o **Filtro**), clique em **copiar** e cole no portal. Veja *Como usar os códigos 2FA no login*.

# 6.Segurança

## A equipe consegue ver ou copiar minha credencial original?

Não. A equipe acessa os sistemas **sem ver, copiar ou guardar** a credencial original — apenas o código temporário é exibido.

## Onde a chave fica guardada?

Em um **cofre digital compartilhável**, e não no aparelho de uma única pessoa. Isso elimina a dependência de "quem está com o celular".

# 7.Suporte

## Onde consigo ajuda?

O suporte do *Presto Start* é feito por **e-mail**. Em caso de dúvidas não resolvidas por este FAQ ou pelos artigos de onboarding, entre em contato com a equipe de suporte Presto/Oystr por este [link](#).