# GUIA DO USUÁRIO



Este manual tem como objetivo fornecer orientações, diretrizes e critérios sobre às normas de segura da informações da Lei Geral de Proteção de Dados (LGPD), segurança de cibernética Duplo Fator de Segurança (MFA) para acesso aos portais de compra.

Além disso você encontrará informações sobre a Rede de Negócios Clicbusiness mostrando como se cadastrar em novos portais e participar de novos processos de compras.

# IMPLANTAÇÃO DO DUPLO FATOR DE AUTENTICAÇÃO MAF

## 1. O QUE MUDA?

A **Paradigma** trabalha constantemente buscando inovação, mas sempre com a atenção para a **Segurança da Informação**. E com o objetivo trazer mais uma camada de proteção, o acesso ao sistema da Paradigma exigirá **DUPLO FATOR DE AUTENTICAÇÃO**.

## 2. Como funciona?

A **autenticação** é uma medida de segurança para garantir que apenas pessoas autorizadas tenham acesso ao sistema. Ela precisa ser previamente cadastrada e informada corretamente sempre que for acessar o sistema.

O **segundo fator de autenticação**, é uma forma de aumentar a segurança do sistema e a proteção dos dados. Esse recurso é conhecido e amplamente utilizado em sistemas como Gmail, Facebook, Instagram, Whatsapp, Dropbox, Microsoft entre outros.

*É uma combinação entre usar algo que você sabe (senha) com um código gerado por um autenticador*.

## 3. Softwares recomendados

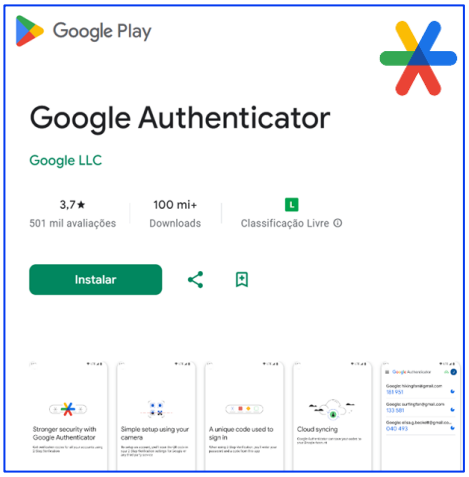
**Aplicativos de autenticação** → existirem diversos softwares que podem ser utilizados para o duplo fator, sugerimos o uso do aplicativo **Google Authenticator** e **Microsoft Authenticator**. Estes aplicativos estão disponíveis para Android e Iphone, gratuitamente, nas lojas oficiais Play Store e Apple Store.

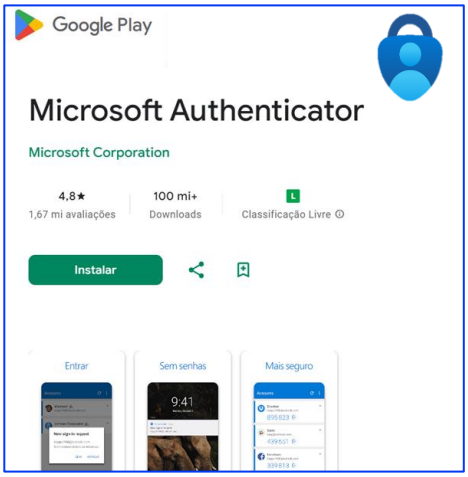
*Saiba mais nos links abaixo:*
https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=pt_BR
https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=pt_BR
https://apps.apple.com/br/app/google-authenticator/id388497605
https://apps.apple.com/br/app/microsoft-authenticator/id983156458

## 4. Como configurar o Duplo Fator de Autenticação?

Caso você não tenha um aplicativo de autenticação, é necessário fazer o download do Google ou Microsoft na Play Store ou Apple Store do seu celular.

### Download Aplicativo



## Como configurar o aplicativo

### Configurar o Google Authenticator

1. Em um dispositivo Android, acesse sua Conta do Google.
2. Na parte de cima da tela, toque na guia Segurança.
3. Se ela não aparecer, deslize por todas as guias até encontrar essa.
4. Em "Você pode adicionar mais opções de login", toque em Authenticator. Talvez seja necessário fazer login.
5. Toque em Configurar o autenticador.
6. Em alguns dispositivos, toque em Vamos começar.
7. Siga as etapas que aparecem na tela.

### Authenticator

1. Abra o Microsoft Authenticator **Configurar o Microsoft**.
2. Toque no botão "+" no canto superior direito.
3. Escaneie o código QR exibido na tela do seu computador ou siga as instruções fornecidas nas configurações da sua conta.
4. Verificação em Duas Etapas:
5. No seu computador, acesse o portal.office.com e faça login na sua conta do Office 365 para empresas.
6. Selecione "Configurar agora" e escolha "Aplicativo móvel" como método de verificação.
7. Certifique-se de que a opção "Receber notificações para verificações" esteja selecionada3.
8. Aprovação de Login:

# 5. Primeiro acesso após habilitar o duplo fator - MFA

***É necessário que tenha o aplicativo autenticador, configurado no seu celular.***

No seu primeiro acesso ao portal, após informar o usuário e senha, abrirá a tela do MFA (autenticação multifator) para escanear o QRCode, em 4 etapas:

## ETAPA 1

Preencha com o seu usuário e senha padrão

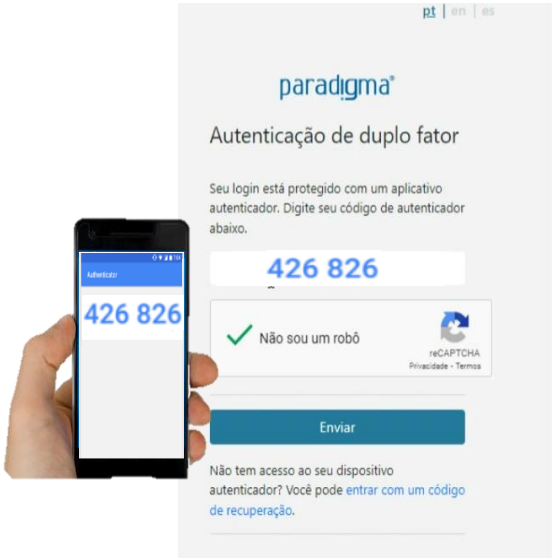
## ETAPA 2

Aponte a tela do celular com a opção de escanear QRCode do aplicativo aberta e escaneie o código que aparece na página

**Importante: O código de verificação do autenticador tem validade de 30 segundos para inserção e validação**


## ETAPA 3

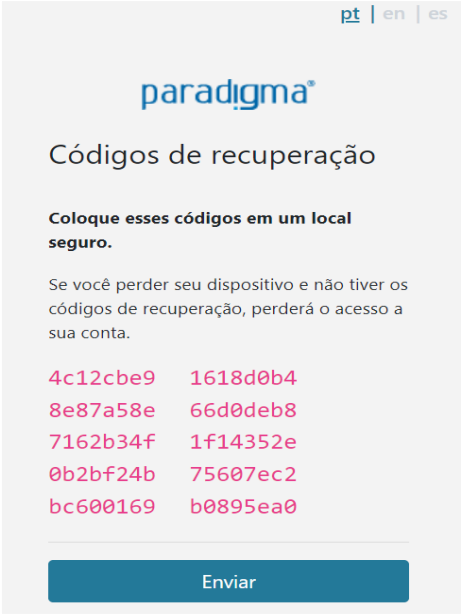
Informe o código gerado no aplicativo de autenticação e clique em “Não sou robô”



## ETAPA 4

O sistema irá gerar 10 códigos de recuperação de acesso.

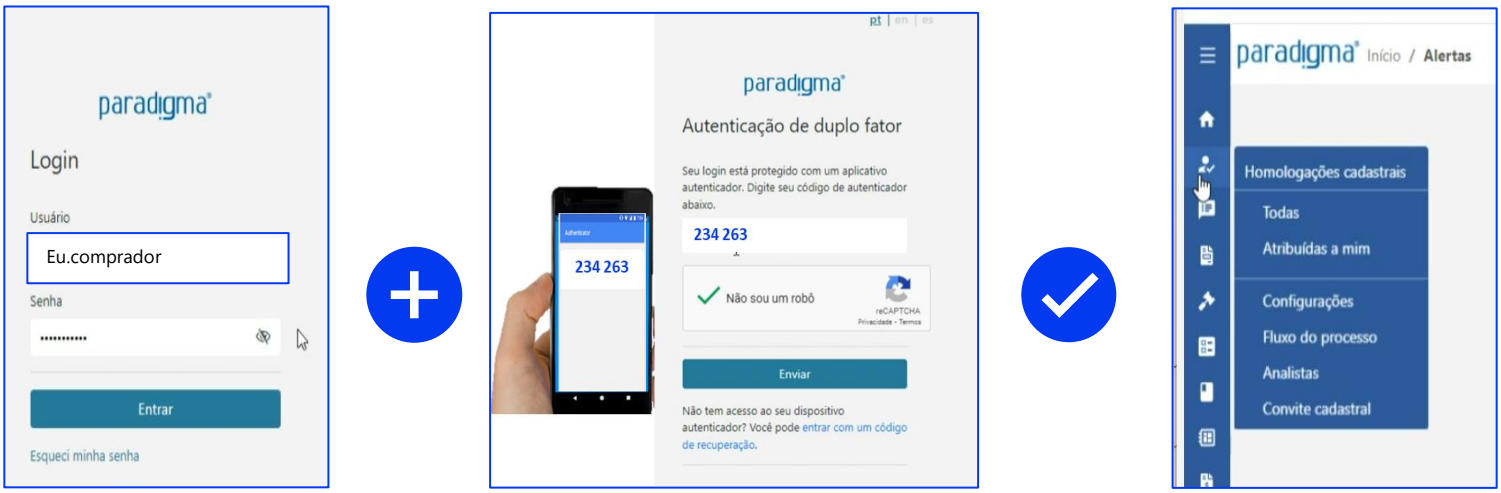
**Guarde-os em local seguro, diferente do dispositivo utilizado.**




# 6. Acesso após habilitar o duplo fator

***Sempre será solicitado o código do autenticador***

A partir de agora, sempre que **acessar o site com usuário** e senha, será solicitado o **código de autenticação do aplicativo** que foi ativado no passo anterior. E desta forma o seu acesso ocorrerá em 2 etapas



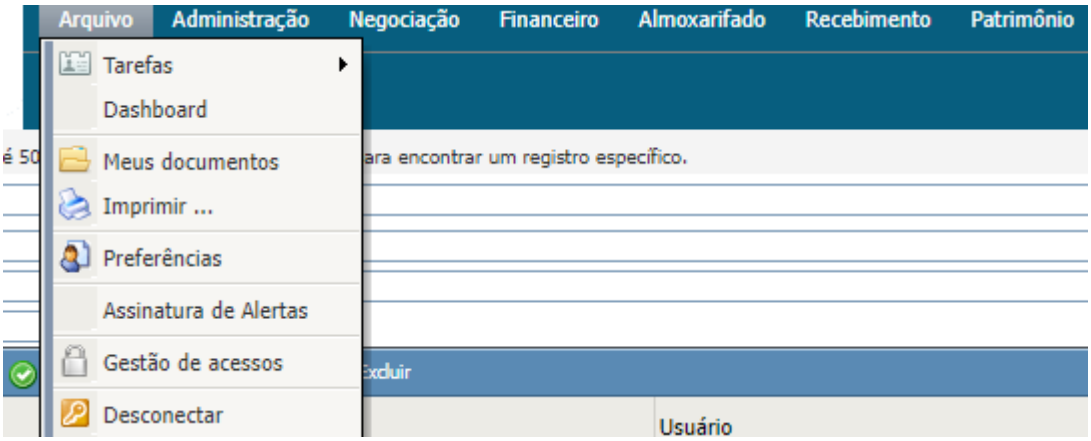

***Pronto! Eu acesso está liberado e seguro***

***Como reiniciar o autenticador de outro usuário (Somente para Administradores)***

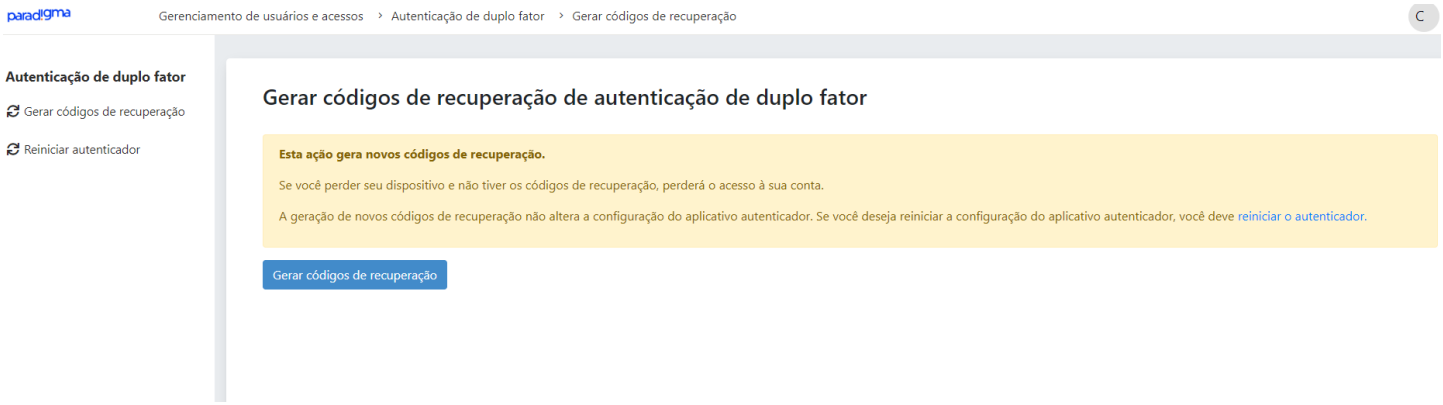
# 7. Perdeu o acesso ao autenticador ?

Se você perdeu o acesso ao autenticador, mas ainda consegue entrar no sistema utilizando seus códigos de recuperação, é possível reiniciar o autenticador ou gerar novos códigos de recuperação. Para isso, siga os passos abaixo:

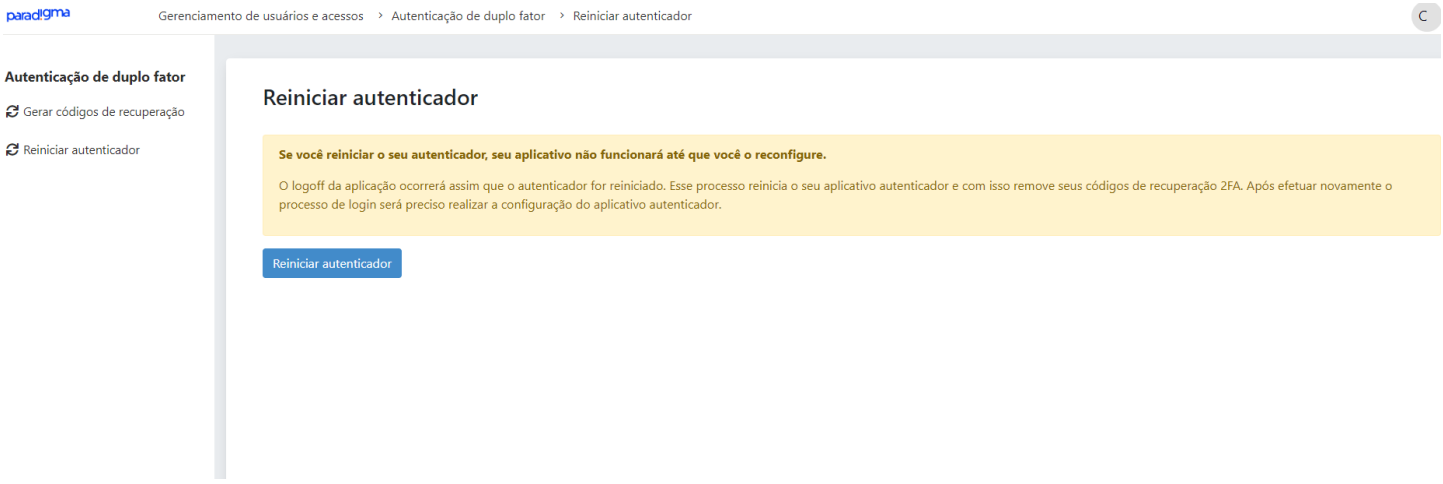
1. Acesse o menu “Gestão de acessos”:




2. A tela abaixo será aberta. Ao acessar o menu “Gerar códigos de recuperação” será permitido gerar 10 novos códigos clicando no botão abaixo:



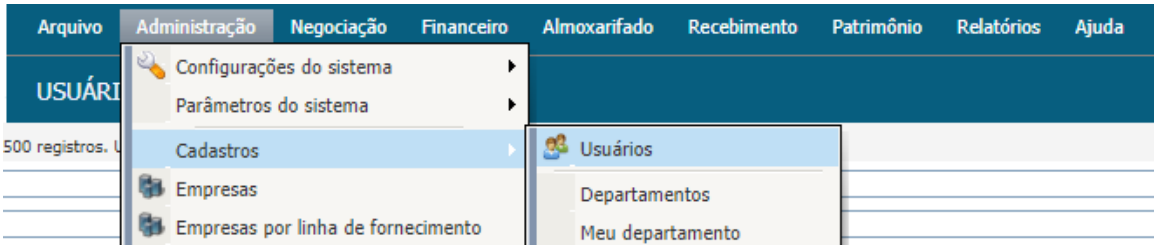

3. Ao acessar o menu “Reiniciar autenticador” será possível reiniciar o seu autenticador clicando no botão abaixo:



## Usuário administrador

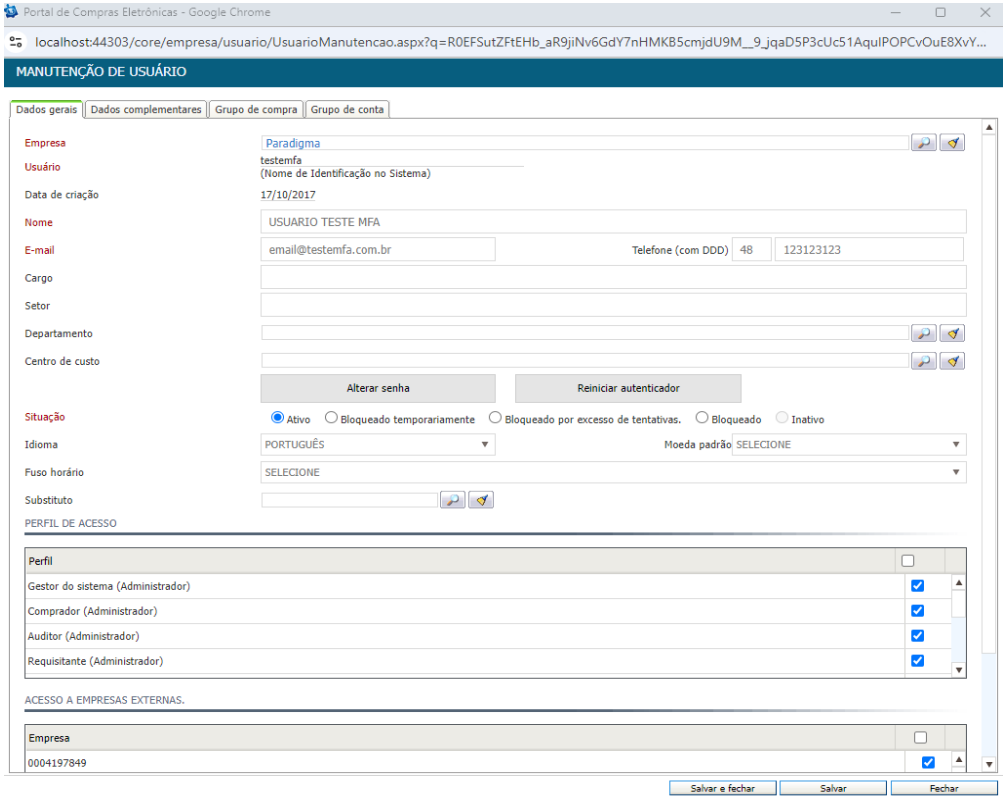
Se você é um usuário administrador, pode reiniciar o autenticador de qualquer usuário seguindo os passos abaixo:

1. Faça login com sua conta de administrador.
2. Navegue até a página de cadastro de usuários:




3. Selecione o usuário desejado:


4. Caso o usuário tenha um autenticador cadastrado o botão “Reiniciar autenticador” será exibido na tela:



5. Localize o botão "Reiniciar Autenticador". Ao clicar neste botão, o processo de autenticação de dois fatores será reiniciado para o usuário.
6. O usuário precisará reconfigurar seu aplicativo autenticador ao tentar fazer login novamente. Para isso ele deverá seguir os passos descritos na seção anterior (5. Primeiro acesso após habilitar o duplo fator – MFA).