RNP Educação, Pesquisa e Inovação em Rede

Manual do Usuário - V1.0

CAFe - MFA - IDP

Painel de Segurança V2.2.3

1 Objetivo

Este documento consiste no manual de usuário da versão 2.2.3 do Painel de Segurança MFA (Múltiplos Fatores de Autenticação), o qual inclui o suporte a Passkey e melhorias de usabilidade.

2 Painel de Segurança MFA

2.1 Propósito do Serviço

O Painel de Segurança MFA é o ambiente onde você pode configurar múltiplos fatores de autenticação (MFA) e gerenciar os níveis de segurança da sua conta para realizar o login da sua instituição em diversos serviços por meio da rede CAFe (Comunidade Acadêmica Federada), da RNP (Rede Nacional de Pesquisa).

2.2 Público do Serviço

Usuários finais das instituições cujos IDPs (Provedor de Identidade) suportem o MFA. Este manual é direcionado para a versão 2.2.3 do Painel. Verifique a versão utilizada na sua instituição.

3 Visão geral

3.1 Conceitos Importantes

Esta seção apresenta conceitos importantes para a compreensão do manual.

1. **Fator de Autenticação:** um fator de autenticação é um método utilizado para verificar a identidade de um usuário ao acessar um sistema ou serviço digital. Ele garante que apenas pessoas autorizadas possam realizar login e acessar informações protegidas. Os fatores de autenticação podem ser classificados em três categorias principais:

    - **Algo que você sabe** – Como uma senha ou um PIN.
    - **Algo que você tem** – Como um código enviado por SMS, um token físico ou um aplicativo autenticador.
    - **Algo que você é** – Como biometria (impressão digital, reconhecimento facial ou de voz).

    Muitos sistemas utilizam a autenticação de dois ou mais fatores (MFA), combinando esses métodos para aumentar a segurança.

2. **IDP (Identity Provider ou Provedor de Identidade):** um IDP (Identity Provider ou Provedor de Identidade) é um serviço responsável por autenticar usuários e gerenciar suas credenciais de acesso a diferentes sistemas e aplicativos. Ele funciona como um intermediário entre o usuário e a aplicação que deseja acessar, garantindo que a identidade seja validada de forma segura.

3. **CAFe (Comunidade Acadêmica Federada):** a Comunidade Acadêmica Federada (CAFe) é uma infraestrutura de identidade digital mantida pela RNP (Rede Nacional de Ensino e Pesquisa). Ela permite que estudantes, professores, pesquisadores e servidores de instituições participantes utilizem uma única conta para acessar diversos serviços acadêmicos e científicos de forma segura.

3.2 Requisitos/Premissas

Para utilizar o Painel de Segurança MFA, é necessário atender aos seguintes requisitos e premissas:

- **Usuário vinculado a uma instituição participante:** o usuário deve estar vinculado a uma instituição que faça parte da CAFe e cujo IDP (Provedor de Identidade) suporte a configuração de múltiplos fatores de autenticação (MFA).
- **Credenciais de acesso válidas:** o usuário deve possuir um login institucional ativo para acessar o painel e gerenciar seus fatores de autenticação.
- **Dispositivo e sistema compatível:** para utilizar os fatores de autenticação disponíveis, é necessário ter um dispositivo (como um smartphone ou computador) com sistema operacional e navegador compatíveis com as tecnologias exigidas por cada método.

3.3 Públicos

O Painel de Segurança MFA é destinado a diversos perfis de usuários que fazem parte do ecossistema educacional e de pesquisa. Os públicos-alvo são:

- **Estudantes:** alunos de instituições de ensino superior, técnico ou pesquisa que utilizam a Rede CAFe para acessar serviços acadêmicos, como plataformas de aprendizado, bibliotecas digitais, repositórios de pesquisa, entre outros.
- **Professores e Docentes:** educadores e instrutores de instituições que acessam sistemas acadêmicos, materiais educacionais e outras plataformas colaborativas para ministrar aulas, acompanhar o progresso dos alunos e realizar outras atividades acadêmicas.
- **Pesquisadores:** profissionais que utilizam a infraestrutura da RNP e a Rede CAFe para acessar serviços de pesquisa, colaborar com outros pesquisadores e compartilhar dados acadêmicos e científicos de maneira segura.
- **Funcionários de Instituições de Ensino e Pesquisa:** profissionais administrativos e técnicos que tenham acesso a sistemas internos de gestão, como registros acadêmicos, dados financeiros, ou outras ferramentas necessárias para o gerenciamento das atividades da instituição.

4 Acesso ao Painel de Segurança MFA

4.1 Acesso a partir de um serviço

O acesso ao Painel de Segurança MFA pode ser realizado por meio dos seguintes passos:

1. Entre na tela de login de qualquer serviço integrado à CAFe. No exemplo deste manual, será utilizado o serviço de Emissão de Certificado Pessoal ICPEdu, conforme figura 1. Estando desconectado e na tela inicial do serviço, clique no botão Entrar[1] para ser direcionado à tela de seleção da instituição;

[1] Em alguns serviços, o botão pode apresentar textos diferentes, como, por exemplo, “Acesso Federado”.

Figura 1 – Serviço Emissão de Certificado Pessoal

2. Para prosseguir, realize a busca pelo nome ou sigla da sua instituição, conforme indicado na figura 2, e clique no botão "Prosseguir para login" que será direcionado para a tela de login junto à instituição selecionada;

Figura 2 – Seleção de instituição[2]

3. Na tela de login da instituição, clique no link "Painel de Segurança" abaixo do botão "Entrar", conforme destacado na figura 3, para ser direcionado a tela de login do Painel de Segurança MFA;

Figura 3 – Acesso pela instituição

[2] A tela pode ser diferente da ilustrada, uma vez que a interface do serviço de está em processo de atualização.

4. Na tela de login do Painel (ver figura 4), informe as suas credenciais da instituição e clique no botão "Entrar".

Figura 4 – Acesso Painel de Segurança

Atenção: se o sistema estiver exigindo um segundo fator, mas você não tem mais acesso ao fator utilizado e perdeu os códigos de emergência, solicite ao responsável com perfil de administrador que desative o MFA da sua conta ou entre em contato com o suporte da sua instituição.

5 Gerenciando seus Fatores e Acesso

5.1 Opções de Informações e acessibilidade

Na parte superior do Painel de Segurança, você encontrará opções informativas e de acessibilidade para facilitar a navegação e melhorar a experiência do usuário, conforme destacado na figura 5.

Figura 5 – Opções de Informações e acessibilidade

- **Sobre o Painel de Segurança MFA:** essa opção fornece informações detalhadas sobre o Painel de MFA, explicando como funciona a autenticação de múltiplos fatores para garantir maior proteção ao acesso.
- **Sobre a CAFe:** a Comunidade Acadêmica Federada (CAFe) permite o acesso seguro a diversos sistemas acadêmicos e científicos no Brasil. Essa opção traz mais informações sobre o funcionamento da CAFe e sua integração com o sistema de autenticação.
- **Sobre a RNP:** a Rede Nacional de Ensino e Pesquisa (RNP) fornece infraestrutura e soluções tecnológicas para instituições acadêmicas e de pesquisa. Aqui, você encontra mais detalhes sobre a RNP e seu papel na segurança digital.

- **Opções de Acessibilidade:** para melhorar a usabilidade do sistema, o cabeçalho também oferece opções de acessibilidade:
    - Zoom + : aumenta o tamanho da interface para facilitar a leitura.
    - Zoom - : reduz o tamanho da interface para visualizar mais informações na tela.
    - Alto Contraste: ativa um modo de alto contraste, alterando as cores do sistema para facilitar a leitura, conforme ilustrado na figura 6. Nesse modo:
        - O fundo da tela fica **preto**.
        - Os textos aparecem em **branco** para melhor visibilidade.
        - Os títulos são destacados na cor **amarela** para diferenciação.

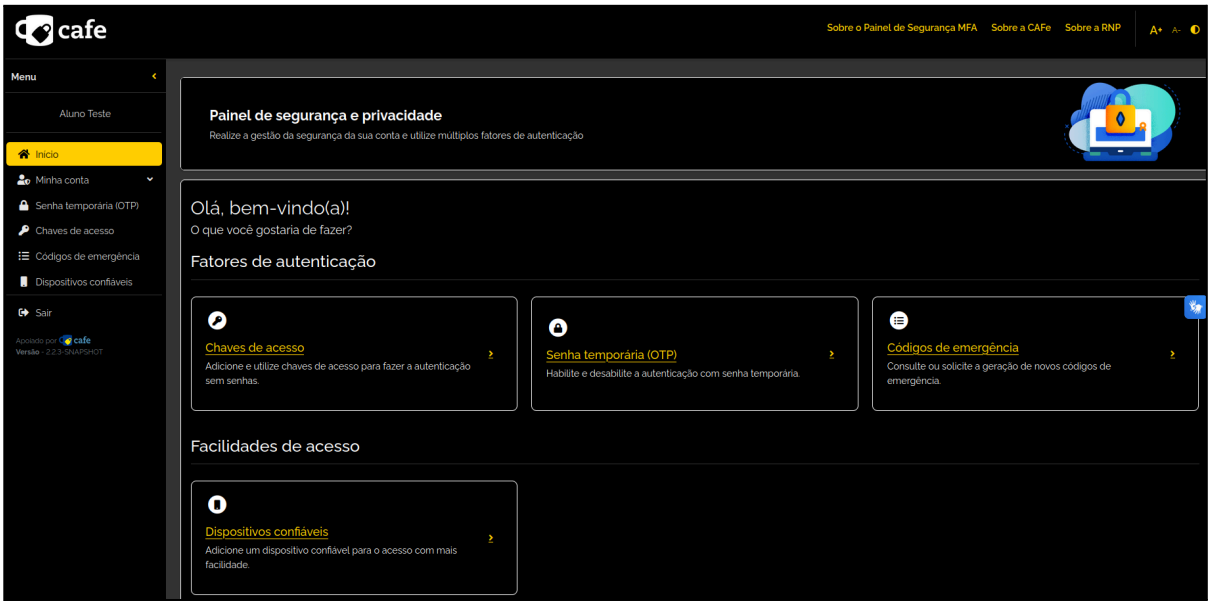

Figura 6 – Auto Contraste ativo

5.2 Tela Inicial

Na parte central da tela inicial, você verá a mensagem de boas-vindas: "Olá, bem-vindo. O que você gostaria de fazer?". Abaixo dessa mensagem, há cartões que organizam as configurações em duas categorias principais, conforme apresentado na figura 7. Cada item elencado a seguir será detalhado nos capítulos seguintes.

1. Fatores de Autenticação:
    a. **Chave de acesso:** registre as chaves de acesso para login mais seguro nos serviços;
    b. **Senha temporária (OTP)**: configure a geração de senhas temporárias;
    c. **Código de emergência:** obtenha códigos para acesso em situações de emergência.
2. Facilidades de Acesso:
    a. **Dispositivos confiáveis:** gerencie os dispositivos em que você já fez login e marcou como seguros.

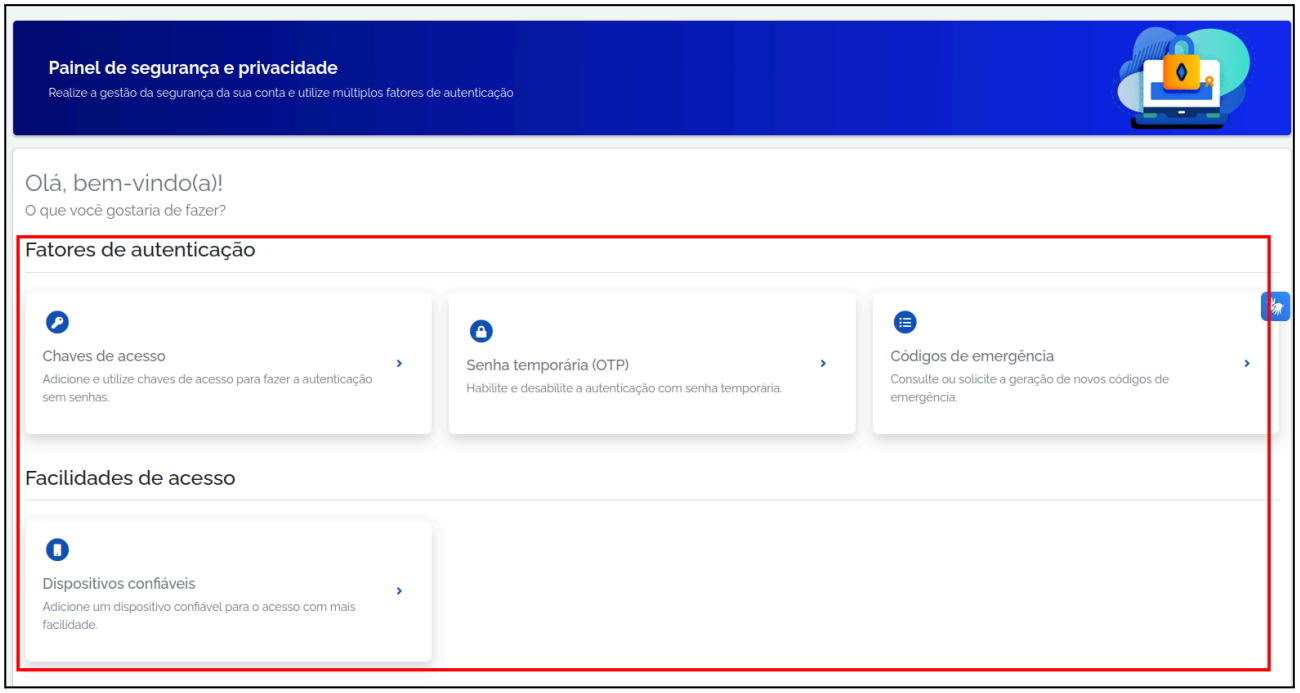

Figura 7 – Tela Inicial

5.3 Menu Lateral

No menu lateral esquerdo (destacado na figura 8), você encontrará as mesmas opções do item anterior, organizadas de forma compacta para acesso rápido. Além disso, encontrará a opção para sair do sistema.

Para configurar qualquer um desses itens, clique no botão correspondente e siga as instruções na tela.

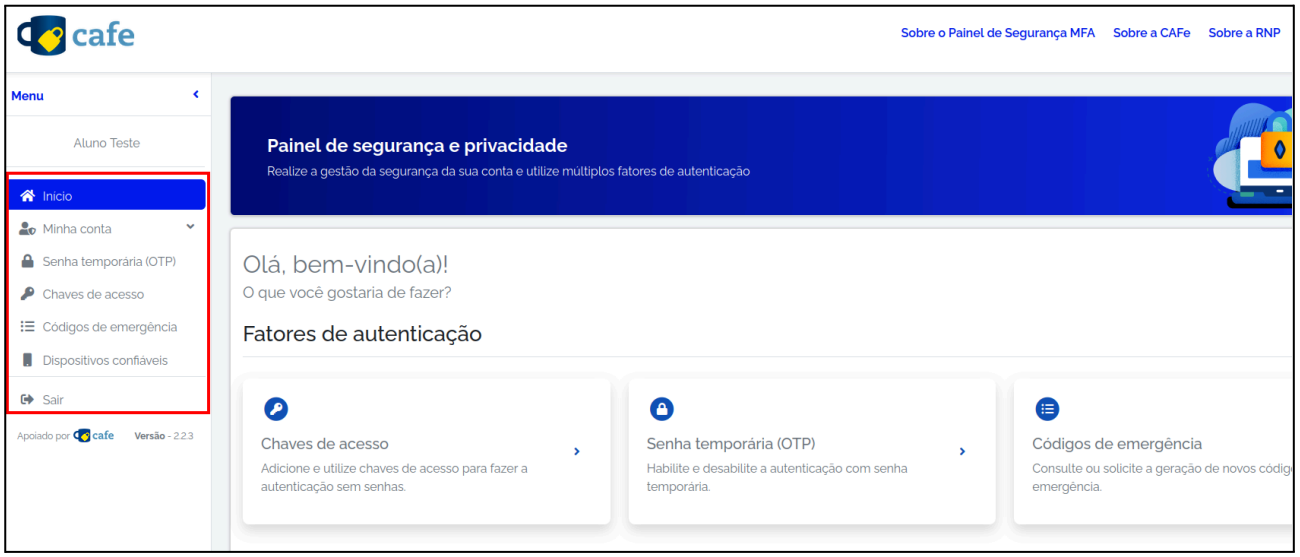

Figura 8– Menus à esquerda

6 Senha Temporária (OTP)

O One Time Password (OTP), ou Senha Temporária (OTP), é um código de autenticação único e temporário, válido por um curto período e utilizado somente uma vez. Ele reforça a segurança ao impedir múltiplas utilizações de uma mesma informação, reduzindo riscos como roubo de credenciais.

Gerado por aplicativos autenticadores, o OTP é amplamente usado na Autenticação Multifator (MFA), adicionando uma camada extra de proteção contra acessos não autorizados.

6.1 Configurar o OTP

Para habilitar o OTP como segundo fator de autenticação, acesse a opção "Senha temporária (OTP)" no menu lateral ou nos cartões centrais da tela inicial do Painel. Na tela seguinte, clique no botão "Configurar senha temporária (OTP)", conforme destacado na figura 9, que será direcionado para a tela de ativação da senha temporária.

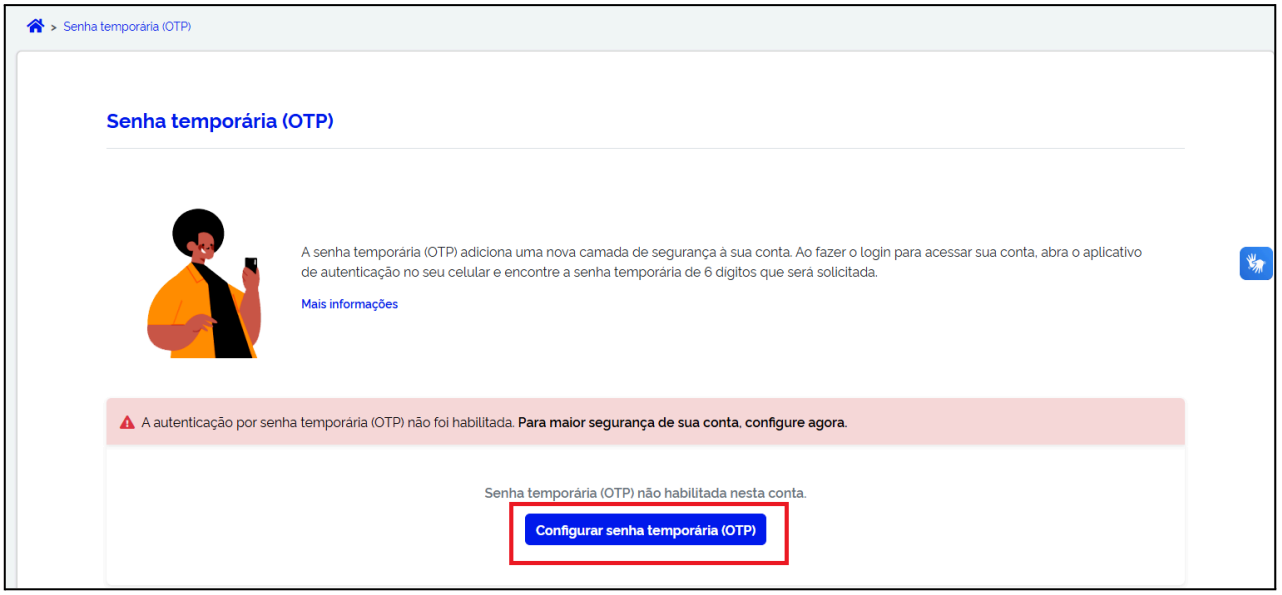

Figura 9 – Ativar senha temporária (OTP)

Na tela de ativação do OTP, é exibido um alerta (veja figura 10) sobre a necessidade de completar todos os passos detalhados na página para completar a configuração do OTP como segundo fator de autenticação.

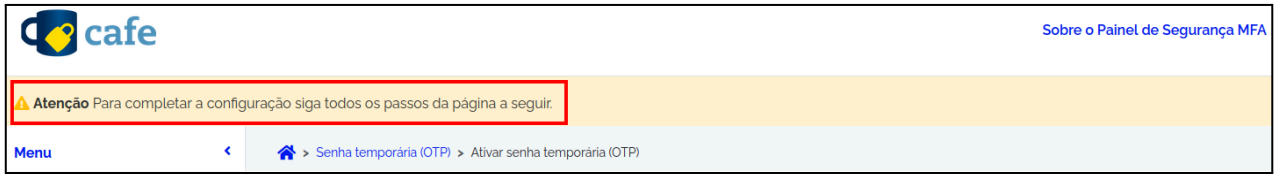

Figura 10 – Mensagem de Alerta

Importante: se você sair da página antes de concluir todos os passos, o OTP não será ativado corretamente e será necessário reiniciar o processo.

Os seguintes passos detalhados na tela de ativação no Painel e resumidos a seguir são necessários para configuração completa da Senha Temporária (OTP):

1. Abra seu aplicativo de autenticação favorito. Caso ainda não tenha um aplicativo no seu dispositivo, baixe um aplicativo autenticador[3];

2. No seu dispositivo, adicione a conta clicando no ícone de + presente em alguns aplicativos ou na opção correspondente;

3. Localize a opção de leitura do QR Code e aponte a câmera do seu celular para o QR Code apresentado no passo 3 da tela de ativação no Painel. Caso esteja realizando o procedimento por meio do seu smartphone, alguns aplicativos permitem a inserção do código correspondente ao QR Code para adicionar a conta. Para isso, clique no botão "Copiar" abaixo do QR Code (veja exemplo na figura 11) para copiar o código e adicionar no aplicativo;

Figura 11 – QR Code gerado (alterado)

4. Após a execução com sucesso do passo 3, o aplicativo apresentará a Senha Temporária válida para um período de tempo. Informe os 6 dígitos da senha nos campos indicados no passo 4 da tela de ativação no Painel e clique no botão "Ativar senha temporária (OTP)" (veja exemplo na figura 12) para validar e finalizar a configuração;

Figura 12 – Inserir código e botão de ativar

Obs.: A execução dos passos a seguir só serão necessários caso seja o primeiro fator que você esteja configurando.

5. O sistema apresentará um pop-up com a mensagem "Fator de autenticação ativado com sucesso". Clique no botão "Continuar";

6. O sistema apresentará um novo pop-up com a mensagem "Você não possui códigos de emergência válidos. Novos códigos serão gerados automaticamente.". Clique novamente no botão "Continuar" para ser redirecionado a tela de códigos de emergência;

7. Siga as orientações para salvar os códigos que são exibidos uma única vez e podem ser usados caso você perca o acesso ao aplicativo autenticador ou não consiga gerar um código OTP temporário. Veja mais informações sobre os Códigos de Emergência no Capítulo 8.

[3]https://ajuda.rnp.br/cafe/idp-cafe/perguntas-frequentes/coleta-verificacao-de-atributos/painel-de-seguranca-mfa-cafe/senhas-descartaveis-mfa

Após a execução dos passos anteriores, você pode confirmar a configuração, acessando o menu "Senha temporária (OTP)" e na tela seguinte (veja figura 13) observar as informações exibidas, como: data e hora que o OTP foi configurado.

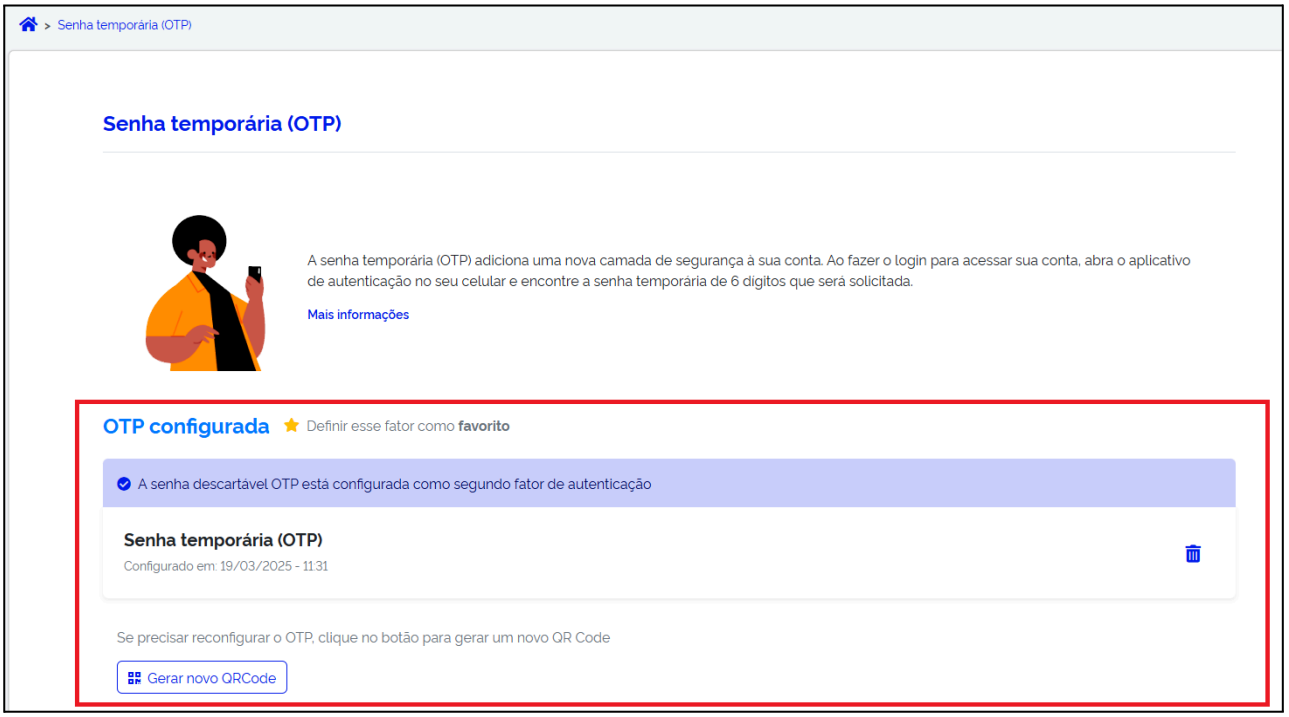

Figura 13 - OTP configurada

6.2 Gerar Novo QR Code para OTP

Se você precisar reconfigurar o OTP, execute os seguintes passos:

1. Acesse o menu "Senha temporária (OTP)" e clique no botão para gerar um novo QR Code, conforme indicado na figura 14;

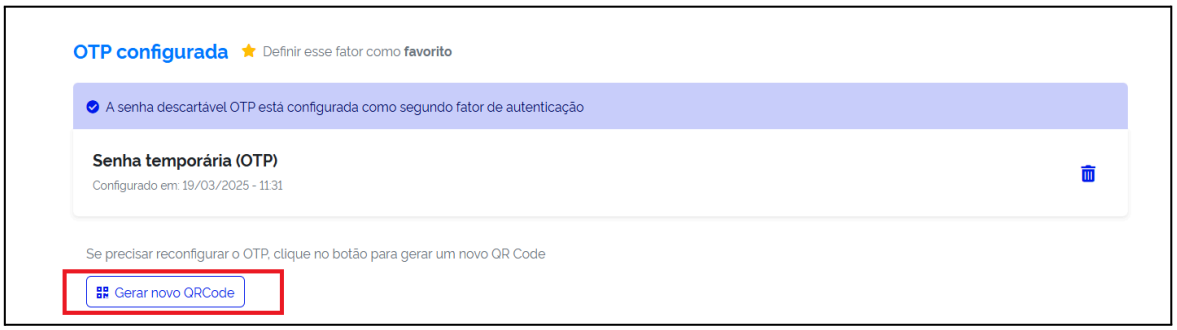

Figura 14 - Gerar novo QR Code

2. Na sequência, o sistema apresentará um pop-up para ser confirmada a ação, conforme ilustrado na figura 15. Clique no botão "Sim, gerar novo QR Code" para confirmar e ser redirecionado para a tela de ativação do OTP. Execute novamente os passos de configuração do OTP, conforme descrito na seção 6.1

Figura 15 - Confirmação para Gerar novo QR Code

Atenção: Ao confirmar a geração de um novo QR Code, a configuração do OTP atual será invalidada e removida do Painel. No entanto, vale ressaltar que a configuração cadastrada no seu aplicativo autenticador **não será excluída automaticamente**. Ou seja, você precisará **remover manualmente a configuração antiga** do aplicativo autenticador para evitar qualquer conflito ou duplicidade de códigos.

6.3 Definir o OTP como fator Favorito

Se houver mais de um fator de autenticação configurado na sua conta, você pode definir um deles como favorito para ser apresentado como primeira opção de segundo fator durante o processo de login para acesso aos serviços.

Para definir o fator OTP como favorito, acesse o menu "Senha temporária (OTP)" e execute os seguintes passos:

1. Na tela seguinte, selecione o ícone de estrela com o texto "Definir esse fator como favorito" logo acima da configuração do OTP, conforme figura 16;

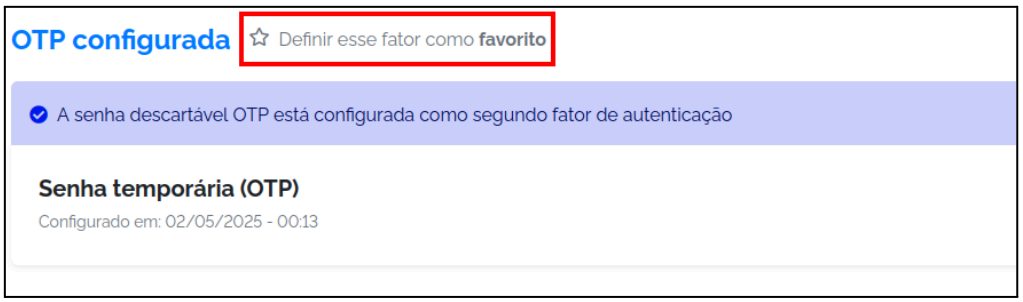

Figura 16 – Definir OTP como fator favorito

2. O sistema apresentará um pop-up para confirmação de alteração do fator favorito. Clique no botão "Sim, prosseguir", conforme apresentado na figura 17, para concluir o procedimento.

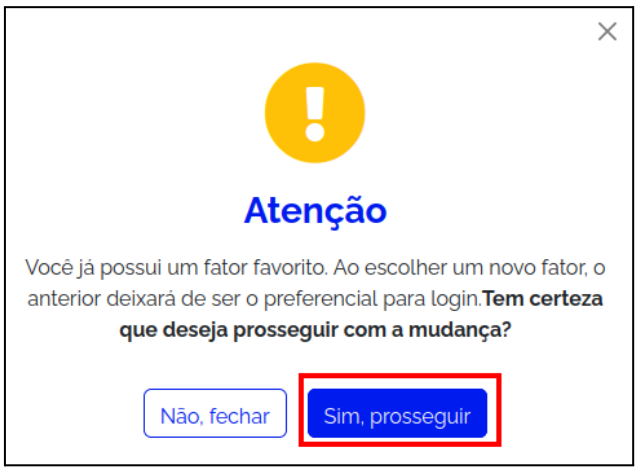

Figura 17 – Confirmar OTP como fator favorito

6.4 Excluir OTP

Caso deseje excluir o OTP, execute os seguintes passos:

1. Acesse o menu "Senha temporária (OTP)" e clique no ícone de lixeira, conforme destacado na figura 18;

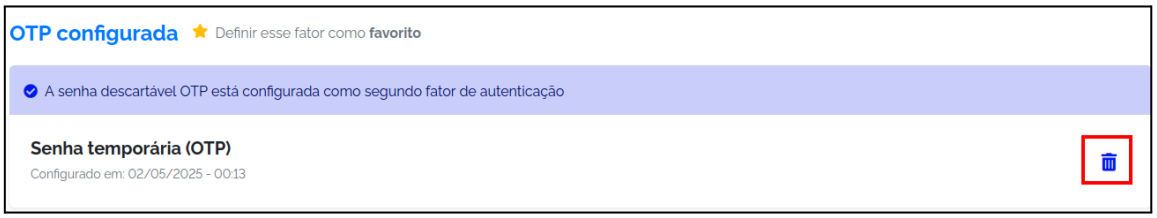

Figura 18 - Excluir OTP

2. Na sequência, o sistema apresentará um pop-up com a mensagem "Você tem certeza que deseja remover esse fator?". Clique no botão "Sim, excluir" para invalidar e remover a configuração de Senha Temporária (OTP) do Painel.

Atenção: ao excluir o OTP, os códigos OTP gerados pelo seu aplicativo não poderão mais ser utilizados nos próximos logins. Como consequência, caso seja seu único fator configurado, sua conta não possuirá mais um segundo fator de autenticação. Isso implica na remoção da camada extra de segurança que o OTP proporciona, deixando sua conta vulnerável a acessos não autorizados caso outras medidas de segurança não sejam adotadas.

Além disso, igualmente ao que acontece ao gerar novo QR Code, **a configuração OTP cadastrada no seu aplicativo autenticador não será excluída automaticamente**. Será necessário **remover manualmente** a configuração antiga do aplicativo para evitar qualquer conflito ou duplicidade de códigos em cadastros futuros.

6.5 Realizar Login utilizando o OTP como segundo fator

Após a configuração do OTP, você poderá utilizar as senhas temporárias geradas pelo aplicativo como segundo fator de autenticação nos próximos logins para acesso aos serviços. Depois da validação das credenciais (usuário e senha) inseridas numa primeira etapa do login, o sistema apresentará a tela de segundo fator e a Senha Temporária (OTP) poderá ser utilizada conforme os cenários A ou B descritos a seguir.

A) Se o OTP estiver definido como fator favorito (veja seção 6.3), depois da validação das credenciais (usuário e senha), o sistema apresentará a tela para login com Senha Temporária (OTP), conforme exemplo da figura 19. Para se autenticar, execute os seguintes passos:

1. Acesse o aplicativo Autenticador do seu dispositivo, digite o código temporário OTP gerado nos campos indicados;

2. Clique no botão "Entrar" para completar o login.

Figura 19 – Login utilizando Senha Temporária (OTP)

B) Caso possua mais de um fator configurado na sua conta e o OTP não esteja definido como fator favorito (veja seção 6.3), a tela apresentada após validação das credenciais será a do fator que foi definido como favorito. Para utilizar o OTP como segundo fator, execute os passos a seguir:

1. Na tela do outro fator apresentada pelo sistema, clique no link "Outras formas de autenticação" abaixo do botão "Entrar", conforme apresentado na figura 20;

Figura 20 – Outras formas de autenticação

2. O sistema apresentará um pop-up para escolha de outro fator de autenticação. Selecione a opção "Senha Temporária (OTP)", conforme indicado na figura 21;

Figura 21 – Selecionar OTP como segundo fator

3. Após a seleção do fator OTP no passo 2, execute os passos descritos no cenário A para completar o login.

7 Chaves de Acesso (passkeys)

As chaves de acesso (passkeys) são uma solução inovadora para autenticação, oferecendo uma alternativa mais segura e prática às senhas tradicionais e aos códigos temporários (OTP). Em vez de digitar senhas ou códigos, o usuário valida sua identidade por meio de um dispositivo autorizado, como um celular ou computador, com suporte ao recurso.

Utilizada como segundo fator de autenticação, a chave de acesso reforça a segurança ao eliminar riscos como o uso de senhas fracas, reutilizadas ou códigos que podem ser interceptados.

7.1 Adicionar Chaves de Acesso

Para adicionar uma chave de acesso como segundo fator de autenticação, acesse a opção "Chaves de acesso" no menu lateral ou nos cartões centrais da tela inicial do Painel. Na tela seguinte, execute os seguintes passos:

1. Clique no botão "Adicionar chave de acesso" conforme apresentado na figura 22;

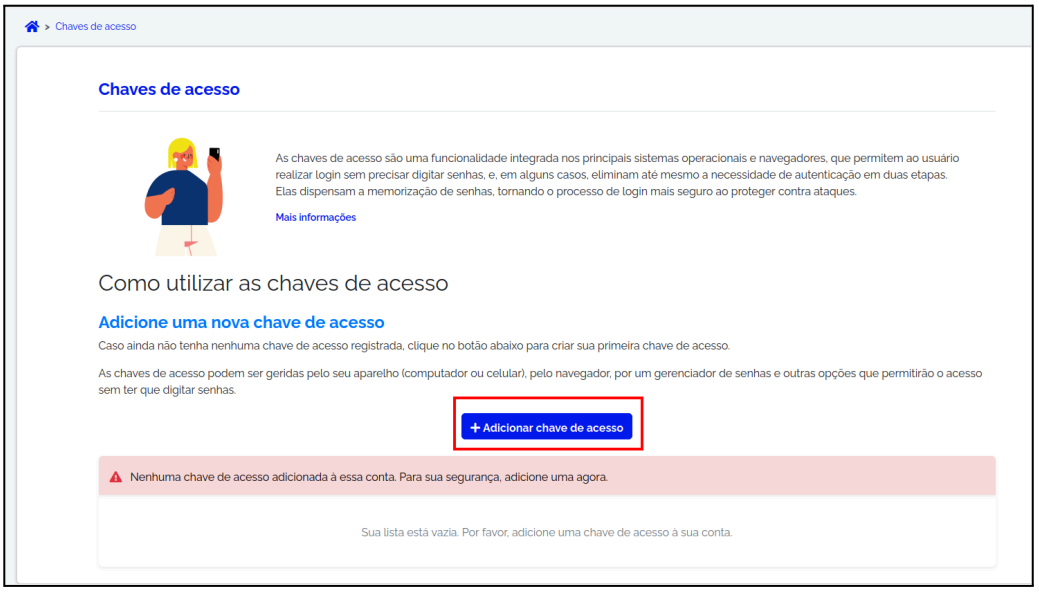

Figura 22 – Adicionar chave de acesso

2. Na sequência, o sistema apresentará um pop-up para que você digite um nome que ajude a identificar a chave (exemplo: "Meu Celular" ou "Meu Notebook");

3. Após digitar o nome para chave, clique no botão "Adicionar" para prosseguir, conforme indicado na figura 23;

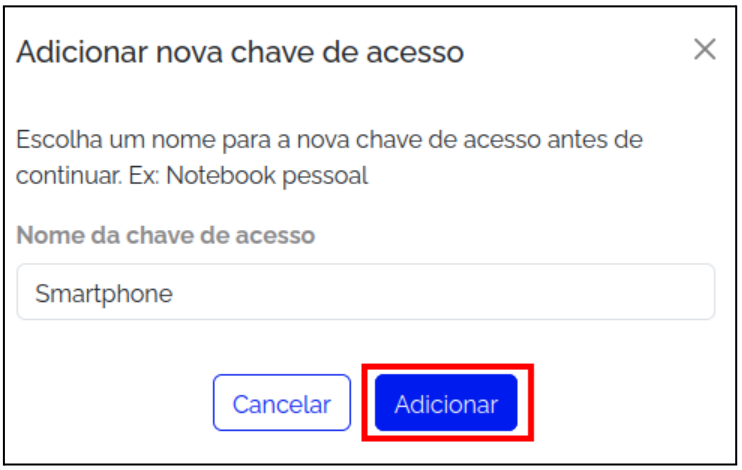

Figura 23 – Nome da chave de acesso

4. Na sequência, o sistema operacional ou navegador exibirá as opções disponíveis de chaves de acesso. Para o exemplo deste manual, os itens indicados na figura 24 foram apresentados e será utilizado o "QR Code via smartphone" como opção. Selecione a alternativa desejada para continuar;

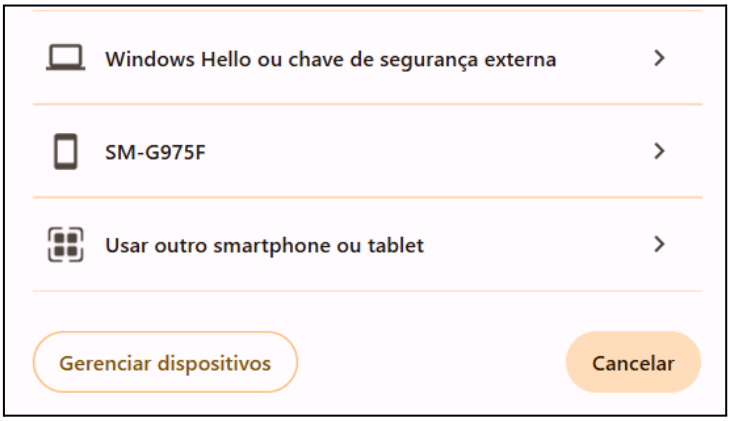

Figura 24 – Opções de Chaves de Acesso

ATENÇÃO: as opções que serão apresentadas vão depender do sistema operacional, navegador e/ou dispositivo utilizado. Além disso, é importante ficar claro que pode ser que seu sistema operacional, navegador e/ou dispositivo **NÃO suporte,** ou **suporte PARCIALMENTE** o uso de Chaves de Acesso. Outro ponto importante é que, caso utilize um dispositivo externo como Chave de Acesso (que é o caso exemplificado neste manual), é necessário que seu dispositivo esteja com o Bluetooth ativo.

5. Após selecionar a opção "Usar outro smartphone ou tablet", um QR Code será exibido na tela (veja exemplo na figura 25). Utilize a câmera ou o aplicativo leitor de QR Code do seu smartphone para escanear o código e siga as instruções exibidas no dispositivo para concluir o processo de adição de chave de acesso;

Figura 25 – QR Code para adicionar Chaves de Acesso

6. Se todos os passos forem seguidos corretamente, a nova chave de acesso será adicionada com sucesso e poderá ser utilizada como segundo fator de autenticação nos próximos logins para acesso aos serviços, tornando o processo mais seguro e prático;

Obs.: a execução dos passos a seguir só será necessária caso seja o primeiro fator que você esteja configurando.

7. O sistema apresentará um pop-up com a mensagem “Fator de autenticação ativado com sucesso”. Clique no botão “Continuar”;

8. O sistema apresentará um novo pop-up com a mensagem “Você não possui códigos de emergência válidos. Novos códigos serão gerados automaticamente”. Clique novamente no botão “Continuar” para ser redirecionado a tela de códigos de emergência;

8. Siga as orientações para salvar os códigos que são exibidos uma única vez e podem ser usados caso você perca o acesso à chave de acesso adicionada. Veja mais informações sobre os Códigos de Emergência no Capítulo 8.

7.2 Editar Chaves de Acesso

Para renomear uma chave de acesso adicionada à sua conta, acesse o menu "Chaves de Acesso" e execute os seguintes passos:

1. Na tela apresentada, clique no ícone de edição na coluna de Ações ao lado do nome da chave que deseja alterar o nome, conforme destacado na figura 26;

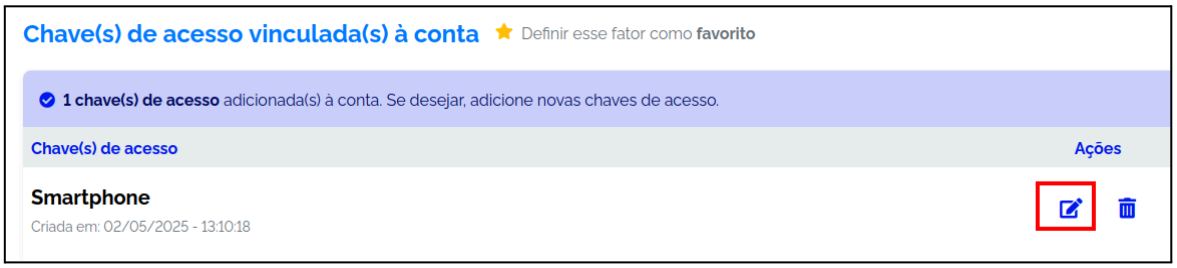

Figura 26 – Editar nome da Chave de Acesso

2. O sistema apresentará um pop-up contendo um campo preenchido com o nome atual. Altere o nome da chave para o que desejar e clique no botão "Salvar" para confirmar a alteração, conforme indicado na figura 27.

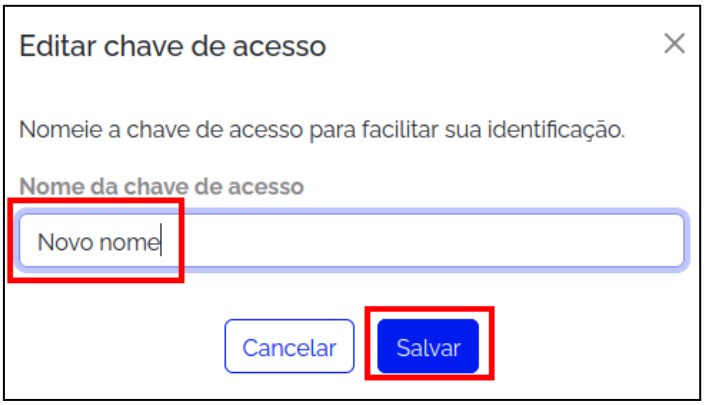

Figura 27 – Renomear Chave de Acesso

7.3 Definir a Chave de Acesso como fator Favorito

Se houver mais de um fator de autenticação configurado na sua conta, você pode definir um deles como favorito para ser apresentado como primeira opção de segundo fator durante o processo de login para acesso aos serviços.

Para definir o fator Chave de Acesso como favorito, acesse o menu "Chaves de Acesso" e execute os seguintes passos:

1. Na tela seguinte, selecione o ícone de estrela com o texto "Definir esse fator como favorito" logo acima da lista de Chaves de Acesso adicionadas, conforme indicado na figura 28;

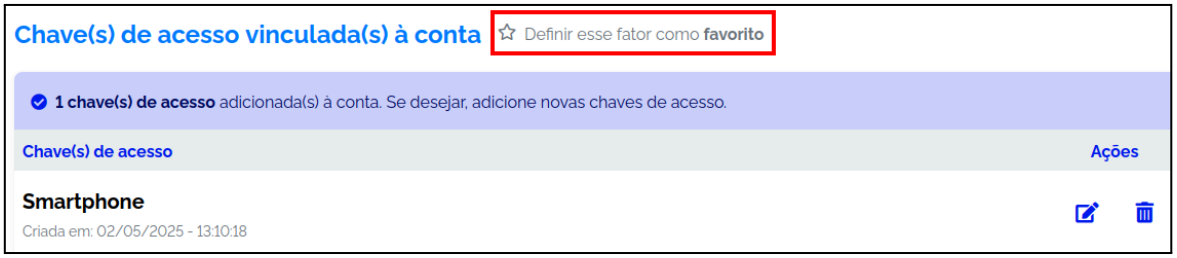

Figura 28 – Definir Chave de acesso como fator favorito

2. O sistema apresentará um pop-up para confirmação de alteração do fator favorito. Clique no botão "Sim, prosseguir", conforme apresentado na figura 29, para concluir o procedimento.

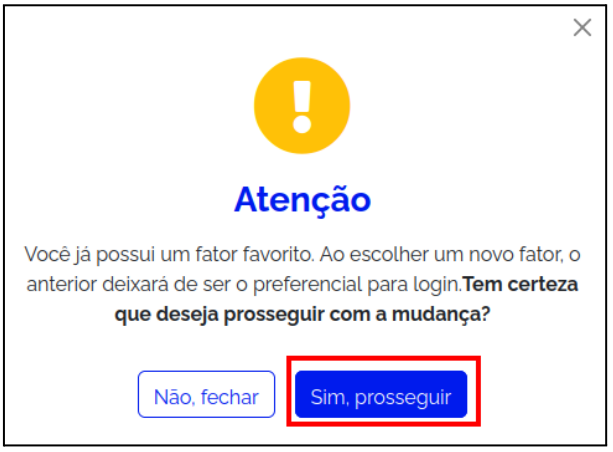

Figura 29 – Confirmar Chave de Acesso como fator favorito

7.4 Excluir Chave de Acesso

Para remover uma chave de acesso da sua conta, acesse o menu "Chaves de Acesso" e execute os seguintes passos:

1. Na tela apresentada, clique no ícone de lixeira na coluna de Ações ao lado do nome da chave que deseja excluir, conforme destacado na figura 30;

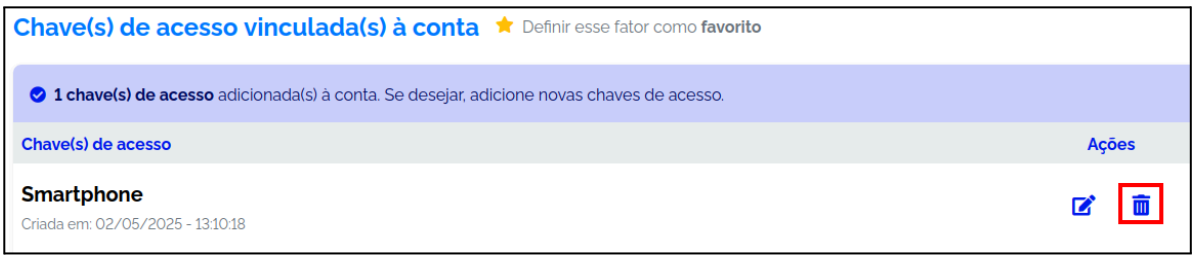

Figura 30 – Excluir Chave de Acesso

2. Na sequência, o sistema apresentará um pop-up com a mensagem "Você tem certeza que deseja excluir sua chave de acesso?". Clique no botão "Sim, excluir" para remover a chave de acesso do Painel.

Atenção: ao excluir uma chave de acesso, não será mais possível utilizá-la como segundo fator de autenticação durante o processo de login. Como consequência, caso não tenha outras chaves de acesso cadastradas e seja seu único fator configurado, sua conta não possuirá mais um segundo fator de autenticação. Isso implica na remoção da camada extra de segurança que as chaves de acesso proporcionam, deixando sua conta vulnerável a acessos não autorizados caso outras medidas de segurança não sejam adotadas. Se desejar, você pode adicionar uma nova chave de acesso a qualquer momento.

7.5 Realizar Login utilizando uma Chave de Acesso como segundo fator

Após adicionar uma ou mais Chaves de Acesso, você poderá utilizá-las como segundo fator de autenticação nos próximos logins para acesso aos serviços ou ao próprio Painel de Segurança MFA. Depois da validação das credenciais (usuário e senha) inseridas numa primeira etapa do login, o sistema apresentará a tela de segundo fator e a Chave de Acesso poderá ser utilizada conforme os cenários A ou B descritos a seguir.

A) Se fator Chave de Acesso estiver definido como fator favorito (veja seção 7.3), depois da validação das credenciais (usuário e senha), o sistema apresentará a tela para login com Chave de Acesso, conforme exemplo da figura 31. Para se autenticar, execute os seguintes passos:

Figura 31 – Realizar Login utilizando as Chaves de Acesso como segundo fator

1. Clique no botão Entrar para iniciar o processo de autenticação com Chave de Acesso;

2. Na sequência, o sistema operacional ou navegador exibirá as opções disponíveis de chaves de acesso. Para o exemplo deste manual, os itens indicados na figura 32 foram apresentados e será utilizado o "QR Code via smartphone" como opção. Selecione a alternativa desejada para continuar;

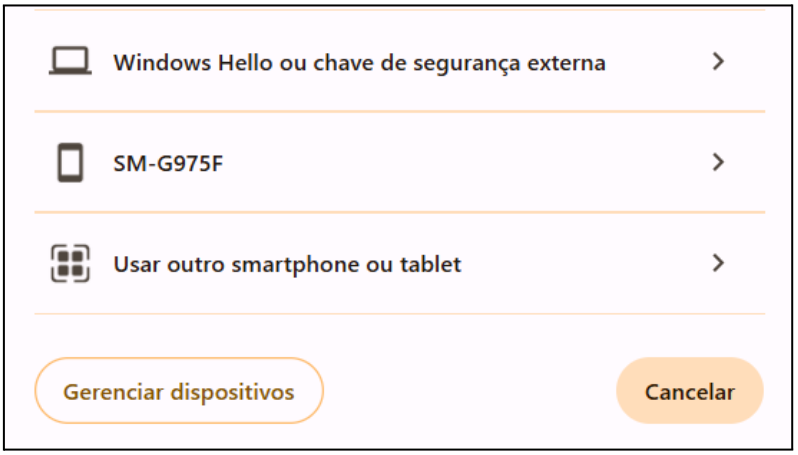

Figura 32 – Opções de Chaves de Acesso

ATENÇÃO: as opções que serão apresentadas vão depender do sistema operacional, navegador e/ou dispositivo utilizado. Além disso, é importante ficar claro que pode ser que seu sistema operacional, navegador e/ou dispositivo **NÃO suporte,** ou **suporte PARCIALMENTE** o uso de Chaves de Acesso. Outro ponto importante é que, caso utilize um dispositivo externo como Chave de Acesso (que é o caso exemplificado neste manual), é necessário que seu dispositivo esteja com o Bluetooth ativo.

3. Após selecionar a opção "Usar outro smartphone ou tablet", um QR Code será exibido na tela (veja exemplo na figura 33). Utilize a câmera ou o aplicativo leitor de QR Code do seu

smartphone para escanear o código e siga as instruções exibidas no dispositivo para concluir o processo de autenticação com chave de acesso;

Figura 33 – QR Code para login com Chaves de Acesso

4. Se todos os passos forem seguidos corretamente, a autenticação será validada e o login será realizado, garantindo o acesso ao sistema.

B) Caso possua mais de um fator configurado na sua conta e o fator Chave de Acesso não esteja definido como fator favorito (veja seção 7.3), a tela apresentada após validação das credenciais será a do fator que foi definido como favorito. Para utilizar Chave de Acesso como segundo fator, execute os passos a seguir:

1. Na tela do outro fator apresentada pelo sistema, clique no link "Outras formas de autenticação" abaixo do botão "Entrar", conforme apresentado na figura 34;

Figura 34 – Outras formas de autenticação

2. O sistema apresentará um pop-up para escolha de outro fator de autenticação. Selecione a opção "Chave de Acesso", conforme indicado na figura 35;

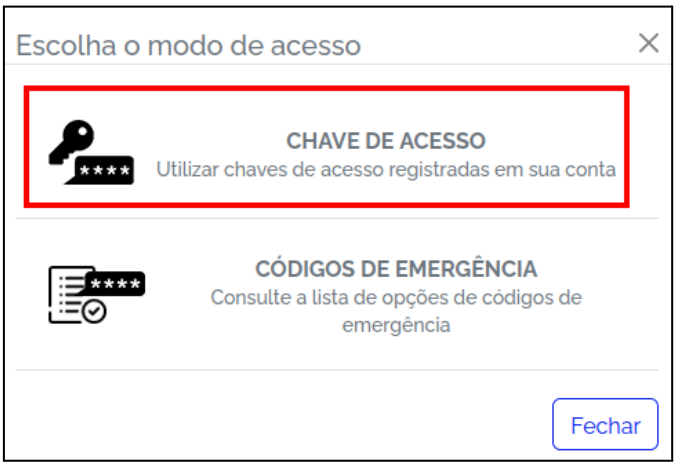

Figura 35 – Selecionar Chave de Acesso como segundo fator

3. Após a seleção do fator Chave de Acesso no passo 2, execute os passos descritos no cenário A para completar o login.

8 Códigos de emergência

Os Códigos de Emergência (também chamados de "Códigos de Backup", "Backup Code" ou "Senha de Emergência") são códigos fornecidos como uma alternativa para acessar sua conta caso você não consiga usar os fatores de autenticação que estejam ativos. Esses códigos atuam como um fator de autenticação de backup, permitindo que você recupere o acesso à sua conta sem depender exclusivamente dos demais fatores ativos.

8.1 Códigos de Emergência gerados automaticamente

Os Códigos de Emergência são gerados automaticamente após a ativação de um primeiro fator de autenticação, como Senhas Temporárias - OTP (veja seção 6.1) ou Chaves de Acesso (veja seção 7.1), e podem ser usados caso você perca o acesso ao aplicativo autenticador configurado ou a chave de acesso adicionada na sua conta.

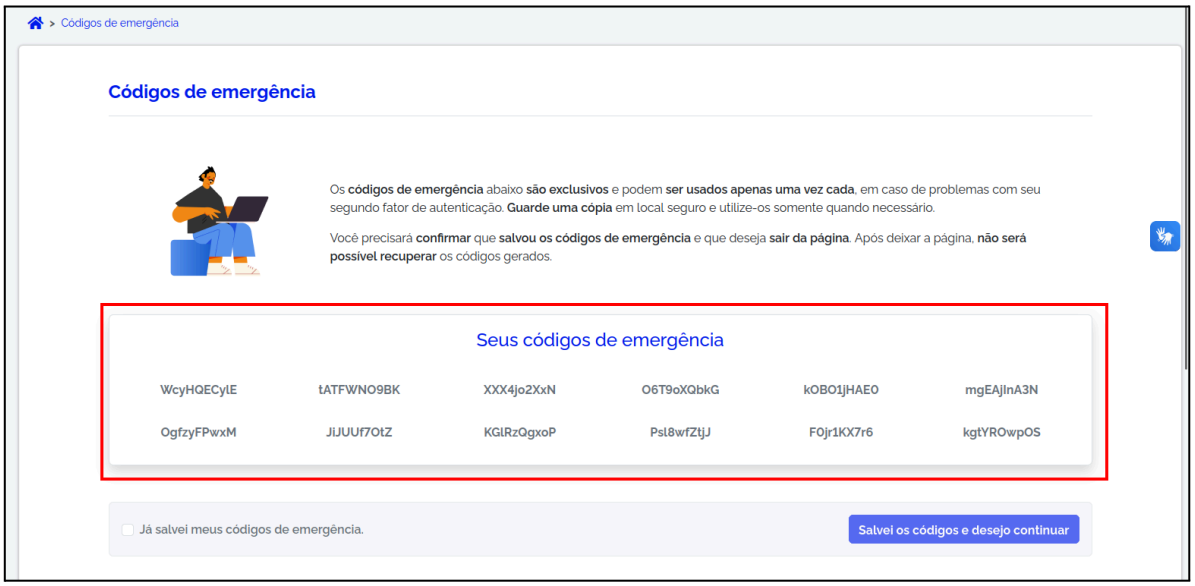

Figura 36 – Códigos de emergência gerados automaticamente

Após o sistema gerar os códigos automaticamente, conforme apresentado na figura 36, escolha como deseja armazená-los (veja figura 37):

- Imprimir os códigos
  - Gera uma versão para impressão;
  - Ideal para quem prefere manter uma cópia física em um local seguro.
- Salvar em PDF
  - Cria um arquivo digital com os códigos;
  - Recomendado para armazenamento em dispositivos protegidos.
- Copiar para a área de transferência
  - Permite colar os códigos em outro local, como um gerenciador de senhas;
  - Rápido e prático para quem deseja salvar os códigos imediatamente.

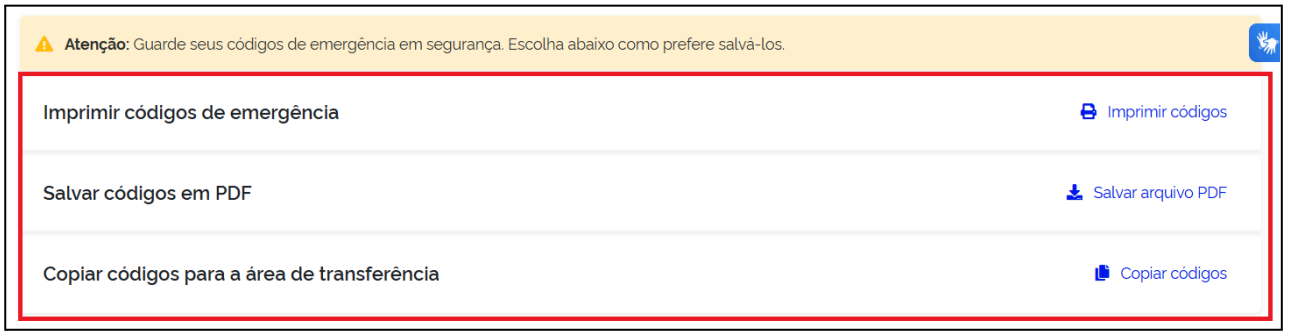

Figura 37 – Salvar Códigos de Emergência

Importante:

- Não compartilhe esses códigos com ninguém.
- Cada código pode ser utilizado somente uma vez.
- Toda vez que um primeiro fator de autenticação é configurado, novos códigos de emergência são gerados.
- Ao gerar novos códigos de emergência, os anteriores são invalidados.
- NÃO existe forma de visualizar os códigos gerados após sair da tela representada pelas figuras 36 e 37. Por isso, **você precisará confirmar que salvou os códigos de emergência** e que **deseja sair da página**, selecionando a opção "Já salvei meus códigos de emergência" e clicando no botão "Salvei os códigos e desejo continuar", conforme ilustrado na figura 38.

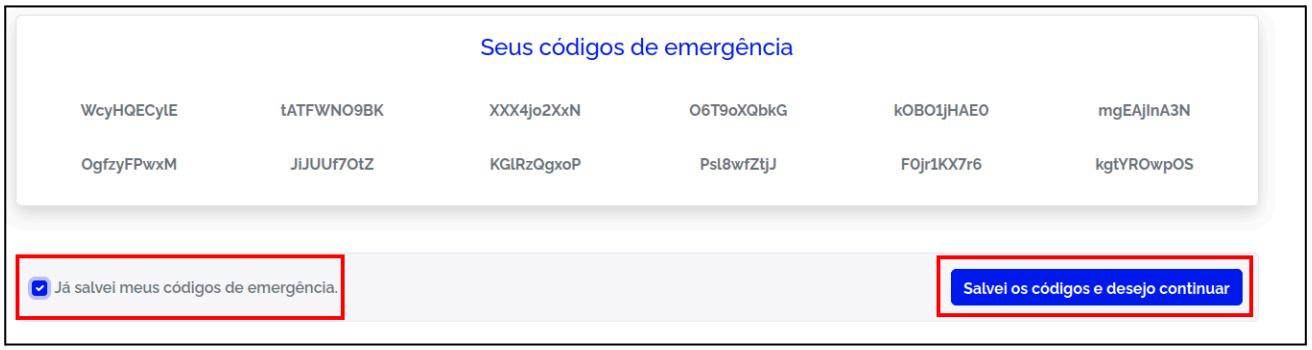

Figura 38 – Confirmação para sair da página

8.2 Gerar novos Códigos de Emergência

Para confirmar a quantidade de códigos de emergência disponíveis, acesse a opção "Códigos de Emergência" no menu lateral ou nos cartões centrais da tela inicial do Painel .

Você verá as seguintes informações na tela seguinte, conforme apresentado na figura 38:

- Data e horário da última geração de códigos.
- Quantidade de códigos ainda válidos.
- Um botão para gerar novos códigos, caso necessário.

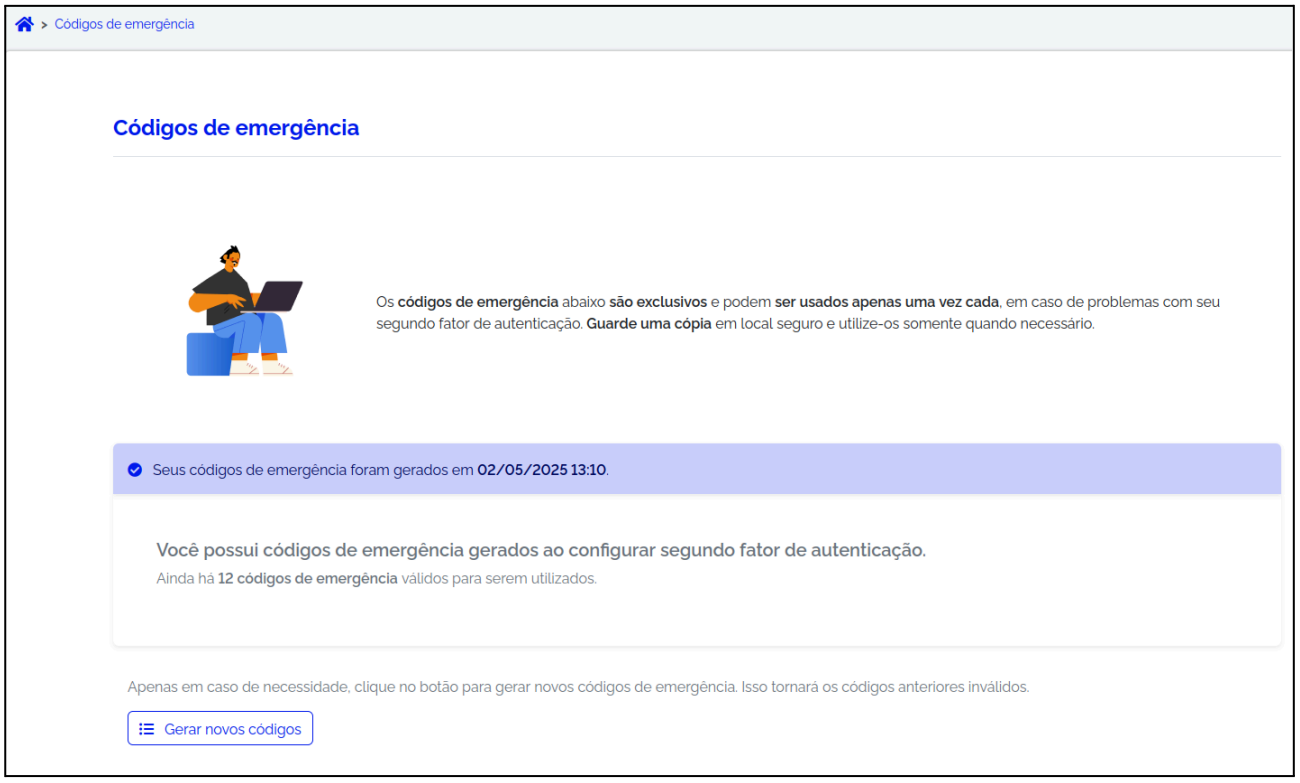

Figura 38 – Gestão de Códigos de Emergência

Se os códigos atuais ainda estiverem válidos e se você ainda possui acesso a eles, recomenda-se utilizá-los antes de gerar novos. Para gerar novos códigos, execute os seguintes passos:

1. No menu de "Códigos de Emergência", clique no botão "Gerar novos códigos" (veja figura 38);

2. O sistema apresentará um pop-up para confirmar a geração de novos códigos. Clique no botão "Sim, gerar novos códigos de emergência", conforme indicado na figura 39, para gerar um novo conjunto de códigos de emergência e invalidar imediatamente os códigos anteriores que ainda estejam válidos.

Figura 39 – Confirmar a geração de novos Códigos de Emergência

8.3 Realizar Login utilizando os Códigos de Emergência

Se você já possuir algum fator configurado em sua conta, poderá utilizar os Códigos de Emergência como um segundo fator provisório (recomendado) de autenticação para acesso aos serviços. Essa ação é recomendada principalmente para recuperar o acesso ao próprio Painel de Segurança MFA, quando você tem um ou mais fatores (OTP e/ou Chave de acesso) configurados na sua conta e não possui acesso a nenhum deles.

Depois da validação das credenciais (usuário e senha) inseridas numa primeira etapa do login, o sistema apresentará a tela de segundo fator e o Código de Emergência poderá ser utilizado. Para isso, execute os seguintes passos:

1. Na tela do segundo fator (neste exemplo foi utilizado o OTP) apresentada pelo sistema, clique no link "Outras formas de autenticação" abaixo do botão "Entrar", conforme apresentado na figura 40;

Figura 40 – Outras formas de autenticação

2. O sistema apresentará um pop-up para escolha de outro fator de autenticação. Selecione a opção "Códigos de Emergência", conforme indicado na figura 41;

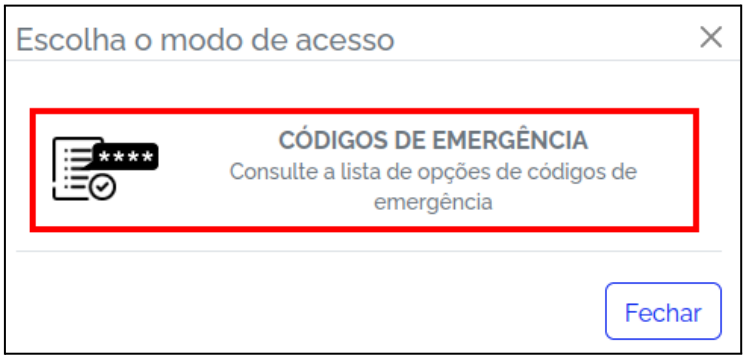

Figura 41 – Login utilizando os Códigos de Emergência

3. O sistema apresentará a tela para login com Códigos de Emergência. Localize um dos seus códigos de emergência válidos, digite-o no campo correspondente, conforme mostrado na figura 42. Certifique-se de que o código inserido esteja correto e, em seguida, clique no botão "Entrar" para concluir a autenticação.

Figura 42 – Login utilizando os Códigos de Emergência

9 Dispositivos Confiáveis

São dispositivos que permitem que o usuário acesse sua conta sem a necessidade de autenticação adicional (usando um segundo fator) em acessos futuros. Ao marcar um dispositivo como confiável, você facilita o processo de login, eliminando a necessidade de inserir códigos ou passar por autenticação de dois fatores toda vez que acessar os serviços desejados a partir desse dispositivo específico. Isso oferece uma experiência mais ágil, mas é importante garantir que o dispositivo confiável seja seguro e usado regularmente, para evitar possíveis riscos de segurança.

9.1 Cadastrar Dispositivo Confiável

Para adicionar um dispositivo como confiável, acesse a opção “Dispositivos Confiáveis” no menu lateral ou nos cartões centrais da tela inicial do Painel. Na tela seguinte, execute os seguintes passos:

1. Clique no botão “Sim, adicionar dispositivo”, conforme indicado na figura 43;

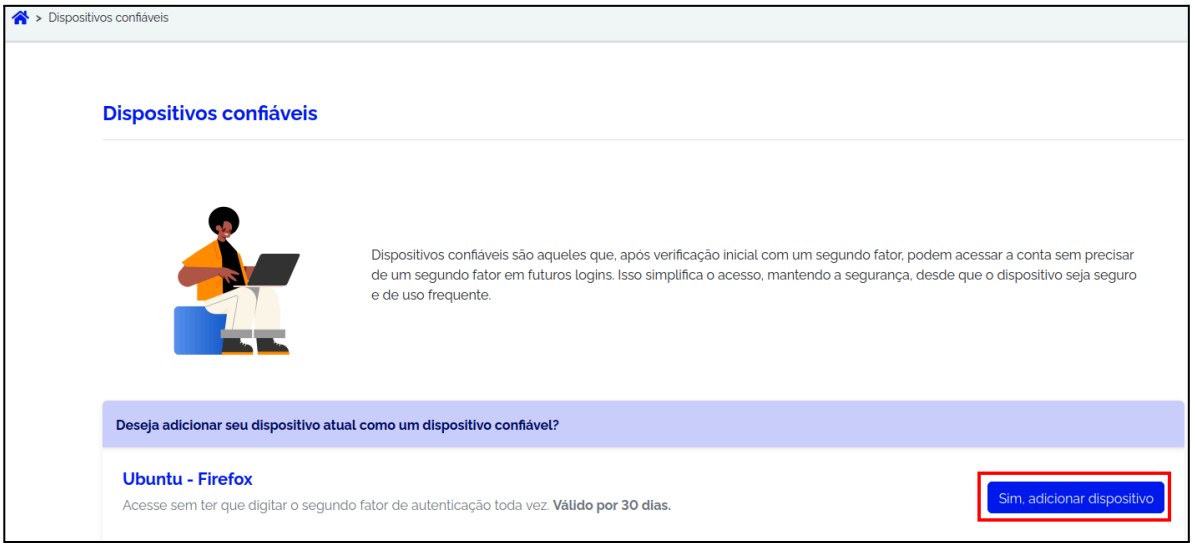

Figura 43 – Adicionar Dispositivos Confiáveis

2. O sistema apresentará um pop-up para que você forneça uma identificação para o dispositivo, a qual pode ser um nome personalizado. Digite o nome desejado e clique no botão “Salvar” para concluir o cadastro, conforme indicado na figura 44.

Figura 44 – Adicionar nome para o Dispositivo Confiável

Atenção:

- Não é possível manter dois dispositivos confiáveis ativos para o mesmo Sistema/Navegador. Uma vez que um dispositivo seja adicionado à lista de dispositivos confiáveis, ele será único, e não poderá ser registrado novamente enquanto estiver ativo. Caso o dispositivo seja removido ou tenha seu prazo de validade expirado, o botão "Sim, adicionar dispositivo" será exibido, permitindo que ele seja adicionado novamente.

- Com o Dispositivo Confiável cadastrado, você simplifica seu acesso aos serviços, dispensando a necessidade de inserir o segundo fator de autenticação a cada login. Esta **opção ficará ativa por 30 dias**, mas pode ser reativada a qualquer momento. Após esse período, será necessário realizar novamente a autenticação de segundo fator.

- Os 30 dias são configurados por um usuário com perfil de administrador. Portanto, se o prazo exibido em seu acesso for diferente do mencionado neste manual, significa que o administrador da sua instituição fez uma configuração personalizada.
- O acesso ao Painel de Segurança MFA **SEMPRE** exigirá o segundo fator de autenticação, caso esta funcionalidade esteja ativa, mesmo quando o dispositivo for confiável. Isso significa que, independentemente do dispositivo, se o OTP ou a Chave de Acesso estiverem configurados como segundo fator, será necessário fornecê-los para completar o login e garantir a segurança da sua conta.

- Dispositivos confiáveis **configurados em uma guia anônima não funcionarão**, uma vez que, ao encerrar a sessão nessa modalidade, todos os cookies e dados temporários associados à navegação são automaticamente apagados, impossibilitando a manutenção da configuração de confiança.

9.2 Visualizar listagem de Dispositivos Confiáveis

Você pode visualizar a lista dos dispositivos confiáveis adicionados à sua conta acessando o menu "Dispositivos confiáveis". Cada dispositivo terá as seguintes informações (veja figura 45):

- **Nome do Dispositivo:** identificação do dispositivo confiável (exemplo: "IOS - Chrome" ou "Windows - Chrome");
- **Informações:** detalhes sobre o dispositivo, como o navegador utilizado e o sistema operacional;
- **Data de Configuração:** a data e hora em que o dispositivo foi adicionado como confiável;
- **Validade:** a data de expiração do dispositivo confiável. Quando a data de expiração está próxima de sua validade, a data ficará na cor vermelha, conforme destacado na figura 45;
- **Destaque de dispositivo:** é exibido um destaque mostrando que o dispositivo atual está configurado e indicando qual é o dispositivo da listagem.

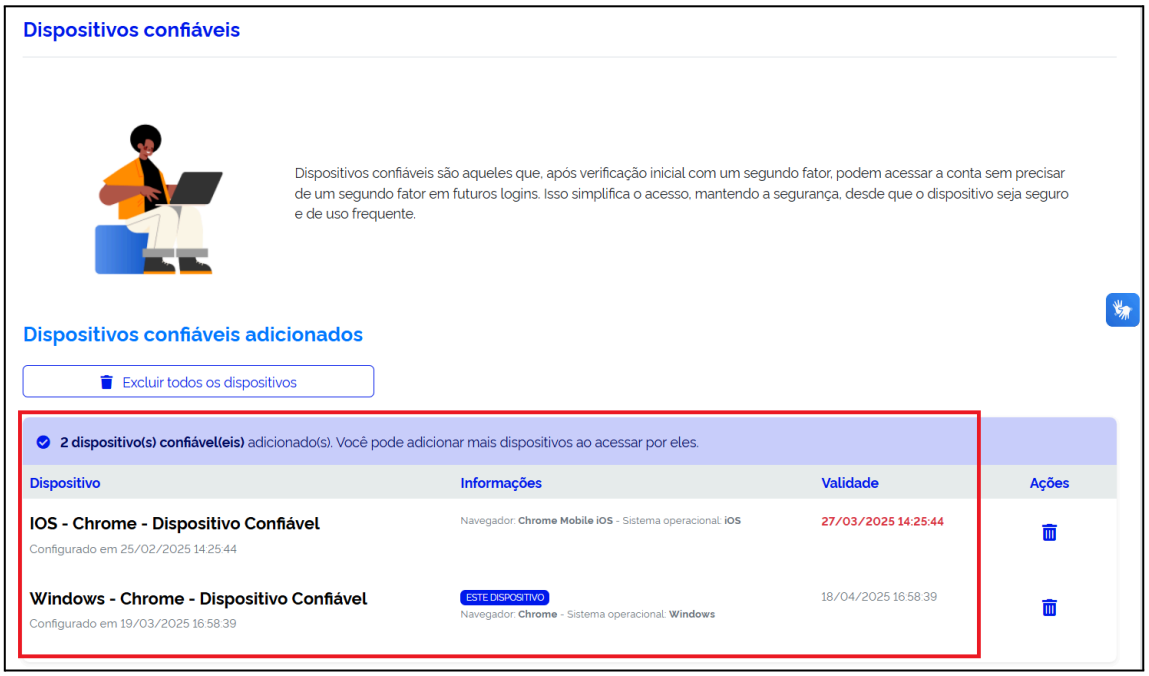

Figura 45 – Visualizar listagem de Dispositivos Confiáveis

9.3 Excluir Dispositivo Confiável

Para excluir um dispositivo confiável individualmente, execute os seguintes passos:

1. Acesse o menu “Dispositivos Confiáveis e clique no ícone de lixeira, da coluna “Ações”, relativo ao dispositivo que deseja excluir, conforme indicado na figura 46;

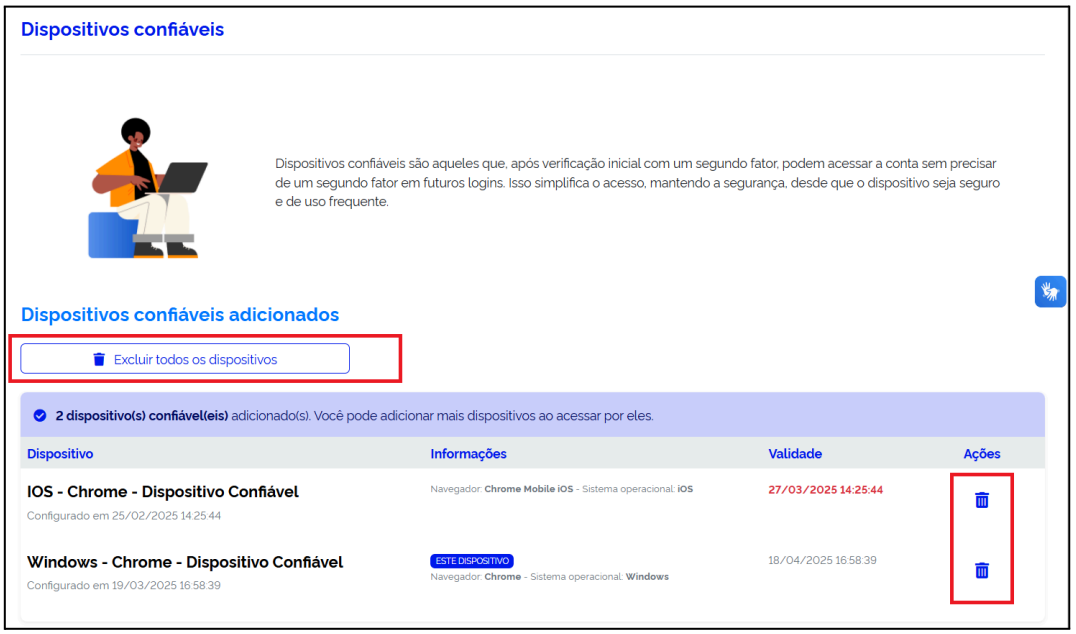

Figura 46 – Excluir Dispositivos Confiáveis

2. O sistema apresentará um pop-up para confirmação de exclusão do dispositivo. Clique no botão “Sim, excluir” para concluir a ação, conforme apresentado na figura 47.

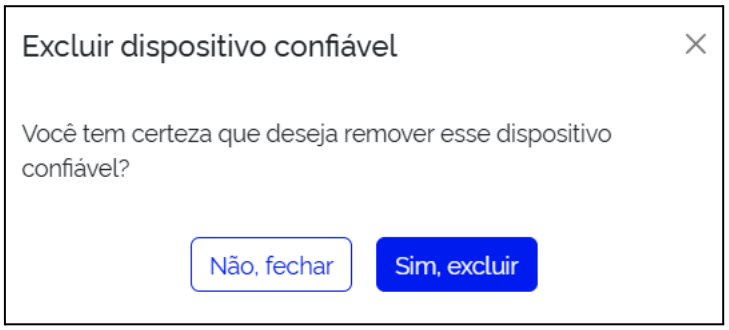

Figura 47 – Confirmar exclusão de Dispositivo Confiável individual

Se desejar excluir todos os dispositivos confiáveis de uma vez, execute os seguintes passos:

1. Acesse o menu “Dispositivos Confiáveis” e clique no botão "Excluir todos os dispositivos", veja figura 46;

2. O sistema apresentará um pop-up para confirmação da exclusão de todos os dispositivos. Clique no botão “Sim, excluir todos” para concluir a ação, conforme apresentado na figura 48.

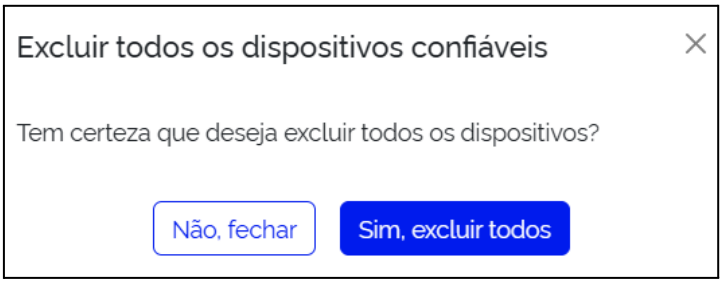

Figura 48 – Confirmar exclusão de todos os Dispositivos Confiáveis

10 Considerações

A Autenticação Multifatorial (MFA) é um recurso essencial para proteger suas credenciais e garantir a segurança de sua conta. O processo envolve várias camadas de proteção, tornando o acesso mais seguro e confiável.

A Senha Temporária (OTP) oferece uma camada adicional de segurança, gerando códigos temporários que expiram rapidamente. A utilização de um aplicativo autenticador para gerar essas senhas dificulta o comprometimento das informações, reforçando a proteção da conta contra acessos não autorizados.

As Chaves de Acesso simplificam o login, permitindo que o dispositivo autorizado prove a identidade do usuário de forma segura. Com as chaves, o usuário não precisa inserir senhas ou códigos constantemente, o que torna o processo mais ágil e reduz a chance de informações serem esquecidas ou roubadas.

Os Códigos de Emergência oferecem uma solução de backup em casos onde o acesso aos fatores de autenticação convencionais é perdido. Esses códigos devem ser armazenados de forma segura, pois são um recurso crucial para restaurar o acesso à conta em situações imprevistas. A segurança e o controle sobre os códigos são fundamentais para proteger sua conta.

Por fim, a funcionalidade de Dispositivos Confiáveis facilita o acesso à conta, permitindo que dispositivos registrados sejam reconhecidos automaticamente, dispensando a necessidade de autenticação adicional em acessos futuros. No entanto, é fundamental garantir que esses dispositivos sejam seguros, já que a perda ou roubo de um dispositivo confiável pode representar riscos para a conta.

Ao adotar essas soluções de MFA, você fortalece a segurança de sua conta e mantém o controle sobre o acesso, garantindo um processo de login mais seguro e ágil.