# Autenticação em 2 Fatores

## SISTEMA SEI

**Saiba como ativar!**

A autenticação em 2 fatores, ou 2FA, fornece segurança adicional, pois junta algo que você sabe (a sua senha) com algo que você possui (o seu smartphone). Somente com a combinação dos dois será possível efetuar o login. Após validar a senha, será preciso informar um código de 6 dígitos, que será gerado pelo aplicativo no smartphone. **Atenção a partir do dia 22/09, a realização da autenticação em 2 fatores será obrigatória.**

## 1. Instalação do Aplicativo de Autenticação

Instale em seu smartphone um aplicativo próprio para autenticação em duas etapas, como o Google Authenticator, Microsoft Authenticator, FreeOTP, Authy, etc. Os exemplos abaixo usam o Google Authenticator.

**Acesse a Apple Store ou o Google Play para instalar.**


## 2. Gerando um Código para Ativação

Na tela de login do sistema, após informar seu usuário e senha, **clique no link "Autenticação em dois fatores"**:


**Clique em Prosseguir** na tela de apresentação da autenticação em dois fatores:


A mensagem abaixo será exibida e, se você nunca fez este procedimento, apenas ignore:


## 3. Leitura do Código

**Abra o aplicativo** Google Authenticator encontre a opção para leitura de código. Pode ser necessário permitir que o aplicativo tenha acesso à câmera do smartphone:

**Aponte a câmera para o código QR** que está sendo exibido na tela e digite o código.


## 4. Finalização do Cadastro

**Informe um endereço de e-mail que não seja associado com a instituição.** Por exemplo, pode ser do gmail, hotmail, yahoo, etc. É imprescindível que a senha de acesso ao email seja diferente da senha de acesso ao sistema:


**Clique em "Enviar"** para que um link de ativação seja enviado para o endereço de e-mail fornecido. Somente após receber o e-mail e clicar no link é que o mecanismo de autenticação em 2 fatores estará ativado.

## 5. Login com a Autenticação em 2 Fatores

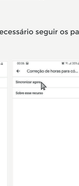
Se a autenticação em 2 fatores estiver ativada, então, após informar o usuário e senha, será exibida outra tela solicitando o código numérico. **Abra o aplicativo de autenticação** no seu smartphone e veja o código gerado. **Informe o valor no campo Código de Acesso** e clique em **Validar**:


De agora em diante, **sempre que fizer login**, será preciso consultar o seu smartphone, porque o código muda a cada 30 segundos. O sistema aceitará qualquer um dos códigos gerados nos últimos 90 segundos por isso é importante que o seu smartphone esteja com o horário correto.

## Saiba mais

### Configuração Manual do Código

Execute este passo apenas se você não consegue ler o código QR. Por exemplo, se estiver acessando esta página pelo smartphone ou se a câmera do seu celular não estiver funcionando. No aplicativo localize a opção "Entrada manual" ou "Inserir chave de configuração":




Clique sobre o código alfanumérico que está sendo exibido logo abaixo do código QR para copiá-lo. Em seguida, cole-o no aplicativo de autenticação e clique em "Adicionar":


### Liberando Dispositivos

Para dispositivos usados com frequência, pode ser conveniente liberá-los da validação a cada login. Para isso, na tela onde é solicitado o código numérico, marque a opção "Não usar 2FA neste dispositivo e navegador". Essa sinalização precisará ser realizada para cada navegador utilizado. O código poderá ser solicitado novamente se for feita a limpeza dos cookies do navegador ou se a liberação perder a validade de acordo com o período estabelecido pela instituição.

### Cancelando Dispositivos Liberados

Para cancelar as liberações, em todos os dispositivos, acesse o link "Autenticação em 2 fatores" disponível na tela inicial de login e clique no botão "Cancelar Dispositivos Liberados":


### Desativando a Autenticação em 2 Fatores

Se não conseguir validar o código por algum motivo (perda do aparelho, defeito, roubo, erro no aplicativo, etc.), é possível requisitar a desativação da autenticação em 2 fatores na mesma tela onde é solicitado o código numérico, ou então por meio do link "Autenticação em 2 fatores" disponível na tela inicial de login. Clique no botão "Desativar 2FA" para que um e-mail com o link de desativação seja enviado para o endereço que foi fornecido no momento da leitura do código QR. Somente após receber o e-mail e clicar no link é que o mecanismo de autenticação em 2 fatores será desativado.

### Solução de Problemas

Caso esteja recebendo a mensagem "Código inválido." ou "Código não reconhecido.", é possível que o horário no seu smartphone esteja desatualizado. Primeiro verifique se o aparelho está configurado para obter a hora automaticamente pela rede. Abaixo estão exemplos de como fazer isso em diferentes sistemas.


Após, apenas em dispositivos Android, também é necessário seguir os passos abaixo para sincronizar o horário no Google Authenticator:


**ATENÇÃO!**

A partir do dia **22/09**, a realização da **autenticação em 2 fatores será obrigatória**.

**Para saber mais**

**clique aqui**

Em caso de dúvidas sobre o MFA, contate o **Service Desk** - (11) 3324-7400

TRIBUNAL DE JUSTIÇA MILITAR DO ESTADO DE SÃO PAULO