SEI:: Autenticação em 2 fatores

12/07/2025 01:06:55

Imprimir artigo da FAQ

Categoria:	STIC::Sistemas Administrativos::SEI - Sistema Eletrônico de Informações	**Votos:**	0
Estado:	público (todos)	**Resultado:**	0.00 %
Idioma:	pt_BR	**Última atualização:**	Qua 09 Jul 11:19:35 2025

Palavras-chave

sei, autenticação, 2 fatores, mfa

Sintoma (público)

Tendo em vista a Portaria Presidência nº 140, de 22/4/2024, do Conselho Nacional de Justiça, que estabelece a obrigatoriedade do Múltiplo Fator de Autenticação (MFA) para acesso aos sistemas judiciais sensíveis (Art. 1º), o Grupo Gestor Permanente do Sistema Eletrônico de Informações - SEI!, informou que a partir de 1º de agosto de 2025 será exigida a autenticação de dois fatores para acesso ao sistema SEI!, tanto aos usuários internos quanto externos.

Problema (público)

Solução (público)

Autenticação em 2 Fatores 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.
1. 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-a:

2. Instalação do Aplicativo de Autenticação Será gerado um código QR como este:

Para lê-lo, 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.

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 a câmera do smartphone:

Aponte a câmera para o código QR que está sendo exibido na tela e adicione a conta no aplicativo.

4. 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":

5. 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 e-mail 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 em2 fatores estará ativado.

6. 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.

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 2FAneste 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 2fatores" 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 2fatores" 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.