INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria de Tecnologia da Informação

OFÍCIO SEI CIRCULAR Nº 3/2023/DTI-INSS

Brasília, 19 de maio de 2023.

.

Às Unidades de Acordo de Cooperação Técnica na Administração Central, Superintendências Regionais e Gerências Executivas.

Assunto: Uso obrigatório de Múltiplo Fator de Autenticação (MFA) para acesso ao SEC.

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 35014.152395/2023-55

1. A Diretoria de Tecnologia da Informação - DTI, dando continuidade às medidas para incrementar as políticas de segurança da informação do INSS, de modo a preservar o valor que possuem para o Instituto e para a sociedade, divulga que, **a partir de 25 de maio de 2023, será obrigatório o uso de Múltiplos Fatores de Autenticação (MFA) para acesso ao sistema SEC**.

2. O uso da autenticação de múltiplos fatores (MFA) é fundamental, pois adiciona uma camada de segurança ao processo de autenticação, reduzindo significativamente o risco de invasões e violações de segurança.

3. A autenticação baseada apenas em senha pode ser facilmente comprometida por invasores que obtêm acesso às senhas por meio de técnicas como 'phishing, força bruta ou ataques de dicionário'. No entanto, com o uso da MFA, mesmo que um invasor obtenha acesso à senha, ele ainda precisará de, pelo menos, um segundo fator de autenticação, o que dificulta muito o processo de invasão.

4. Essa medida de segurança já foi aplicada com sucesso a outros sistemas corporativos do INSS e se faz necessária também no sistema SEC.

5. Os usuários do sistema SEC, para realizarem a autenticação a partir da data acima, precisarão cadastrar um *token OTP* por meio de aplicativo autenticador.

6. Existem três principais tipos de autenticação de múltiplos fatores (MFA):

- MFA baseado em conhecimento: este tipo de autenticação requer que o usuário forneça algo que apenas ele sabe, como uma senha ou PIN, juntamente com outro fator, como um código de verificação enviado por SMS ou e-mail;
- MFA baseado em posse: esse tipo de autenticação exige que o usuário apresente algo que ele possui, como um token de hardware, cartão inteligente ou telefone celular, além de um outro fator de

autenticação, como uma senha.

- MFA baseado em biometria: este tipo de autenticação usa as características físicas exclusivas do usuário, como impressão digital, reconhecimento facial ou voz, juntamente com outro fator de autenticação, como uma senha.

7. Cada tipo de autenticação de múltiplos fatores tem suas próprias vantagens e desvantagens, e a escolha dependerá do ambiente de segurança, requisitos regulatórios e níveis de risco associados ao acesso ao recurso protegido. Em geral, é recomendável utilizar dois ou mais tipos de fatores de autenticação para obter o máximo de proteção.

8. No Guia para utilização do MFA (11467400), fornecido pela DATAPREV, utiliza-se, preferencialmente o **"Google Authenticator", 'aplicativo de segurança gratuito** que viabiliza a autenticação em dois fatores ao gerar “chaves de acesso” para serem usadas neste processo'. Além disso, os sistemas de suporte já possuem expertise e know-how para atendimento de eventuais demandas nesse período de transição.

9. O Guia para utilização do MFA (11467400) segue anexo ao presente, e sugerimos que seja dada ampla divulgação da data de implantação do MFA bem como desse material junto às entidades conveniadas.

Atenciosamente,

AILTON NUNES DE MATOS JÚNIOR
Diretor de Tecnologia da Informação - Substituto

Anexos: I - Guia para utilização do duplo fator de autenticação (SEI nº 11467400).
II - Guia: Cartilha de Orientações do Suporte INSS (SEI nº 11503616).
III - Gui: Passo a Passo para Atendimento de Chamados (SEI nº 11503656).

Documento assinado eletronicamente por **AILTON NUNES DE MATOS JUNIOR**, **Diretor(a) de Tecnologia da Informação Substituto(a)**, em 19/05/2023, às 09:40, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **11497527** e o código CRC **F2D47547**.