

CONSELHO NACIONAL DE JUSTIÇA (CNJ)

CARGO 8: TÉCNICO JUDICIÁRIO – ÁREA: APOIO ESPECIALIZADO ESPECIALIDADE: PROGRAMAÇÃO DE SISTEMAS

Prova Discursiva

Aplicação: 30/06/2024

PADRÃO DE RESPOSTA DEFINITIVO

1 As maneiras por meio das quais a autenticação multifator pode colaborar para a prevenção contra fraudes nos serviços *on-line* internos e externos do setor público brasileiro são as seguintes:

- proteção contra acesso não autorizado: com a autenticação multifator, mesmo que um invasor tenha obtido a senha de um usuário por meio de ataques de *phishing* ou engenharia social, ele ainda precisará de, pelo menos, um segundo fator de autenticação para acessar a conta. Isso reduz significativamente o risco de acesso não autorizado;
- prevenção contra roubo de identidade: a autenticação multifator dificulta o roubo de identidade, pois os fraudadores teriam que superar não apenas a senha, mas também, pelo menos, outro fator de autenticação. Isso torna o processo de falsificação de identidade muito mais complexo e menos provável de ser bem-sucedido;
- segurança em comunicações: a autenticação multifator também contribui para a segurança das comunicações dentro do serviço público. A validação de identidade antes do envio de informações sensíveis por *e-mail* ou mensagens eletrônicas ajuda a proteger contra vazamentos de dados e fraudes relacionadas à comunicação;
- prevenção contra ataques de engenharia social: a autenticação multifator dificulta a eficácia de ataques de engenharia social, nos quais fraudadores tentam obter acesso a sistemas, persuadindo os usuários a divulgar suas credenciais. Mesmo que uma senha seja comprometida, o segundo fator de autenticação será necessário para o acesso;
- monitoramento, rastreabilidade e auditoria: os sistemas de autenticação multifator geralmente possuem recursos de monitoramento e auditoria avançados, que registram as tentativas de autenticação, o que permite a detecção precoce de atividades suspeitas e ações de resposta imediata para prevenir fraudes; e
- cumprimento de regulamentações: a implementação da autenticação multifator também está alinhada com regulamentações de segurança de dados, como a Lei Geral de Proteção de Dados (LGPD).

2 Além da complexidade para os usuários, as desvantagens operacionais e(ou) técnicas da adoção de autenticação multifator são as seguintes:

- custos adicionais: alguns métodos de autenticação multifator, como *tokens* físicos ou soluções biométricas avançadas, podem gerar custos adicionais de implementação e manutenção, o que torna a solução mais dispendiosa;
- possíveis problemas de interoperabilidade: em ambientes complexos com diversos sistemas e aplicativos, pode haver desafios relacionados à interoperabilidade entre as soluções de autenticação multifator e as plataformas existentes, o que exige integrações cuidadosas;
- tempo e recursos para implementação: a adoção de autenticação multifator pode demandar tempo e recursos consideráveis durante a fase de implementação, incluindo treinamento para usuários e ajustes nos processos internos.
- possibilidade de bloqueios indevidos: em alguns casos, sistemas de autenticação multifator podem bloquear usuários legítimos devido a falhas de comunicação ou configurações inadequadas, causando frustração e interrupções no acesso aos sistemas; e
- vulnerabilidades específicas: certos métodos de autenticação multifator podem apresentar vulnerabilidades específicas, como ataques de *phishing* direcionados à obtenção dos fatores adicionais de autenticação, o que exige medidas adicionais de segurança e conscientização.

3 As medidas que podem ser adotadas para reduzir o impacto da complexidade para os usuários internos do uso de autenticação multifator, no contexto de uma organização pública, incluem:

- oferecer opções de autenticação que permitam que os usuários escolham entre diferentes métodos de autenticação multifator, como SMS, *e-mail*, aplicativos autenticadores, *tokens* físicos ou biometria, de acordo com sua familiaridade, suas preferências e sua conveniência, resguardados os padrões de segurança institucional;
- simplificar a experiência do usuário, projetando interfaces de usuário intuitivas e fáceis de usar para os processos de autenticação multifator, minimizando o número de etapas necessárias e fornecendo orientações claras durante o processo;

- fornecer treinamento e suporte adequados e eficazes aos usuários, explicando os benefícios da autenticação multifator, demonstrando como configurar e usar os métodos de autenticação e fornecendo assistência rápida em caso de problemas;
- implementar sistemas de autenticação adaptativa que avaliem o contexto de acesso, como dispositivo utilizado, localização geográfica e comportamento do usuário, para ajustar dinamicamente os requisitos de autenticação e reduzir a frequência de solicitações de autenticação multifator para situações de baixo risco;
- implementar soluções que minimizem a necessidade de autenticação multifator para atividades de rotina e em dispositivos confiáveis, quando apropriado e seguro, mantendo-se o alto padrão de segurança em situações de maior risco; e
- integrar a autenticação multifator com sistemas que utilizam tecnologias de SSO (*single sign-on*) para permitir que os usuários realizem o *login* uma vez e acessem vários aplicativos e serviços sem a necessidade de autenticação repetida.

QUESITOS AVALIADOS

QUESITO 2.1 Três maneiras por meio das quais a autenticação multifator pode colaborar para a prevenção contra fraudes nos serviços *on-line* internos e externos do setor público brasileiro

Conceito 0 – Não apresentou nem explicou corretamente nenhuma maneira por meio da qual a autenticação multifator pode colaborar para a prevenção contra fraudes nos serviços *on-line* internos e externos do setor público brasileiro.

Conceito 1 – ~~Apenas citou as maneiras~~ Citou pelo menos uma das três maneiras, sem explicá-la(s).

Conceito 2 – Apresentou e explicou corretamente apenas uma maneira.

Conceito 3 – Apresentou e explicou corretamente apenas duas das três maneiras.

Conceito 4 – Apresentou e explicou corretamente três maneiras.

QUESITO 2.2 Duas desvantagens operacionais e(ou) técnicas da adoção de autenticação multifator, excluída a complexidade para os usuários

Conceito 0 – Não indicou nem explicou corretamente nenhuma desvantagem operacional e(ou) técnica.

Conceito 1 – ~~Apenas indicou as desvantagens~~ Indicou pelo menos uma das duas desvantagens, sem explicá-las.

Conceito 2 – ~~Indicou e explicou apenas uma desvantagem operacional e(ou) técnica, excluída a complexidade para o usuário, mas o fez de forma parcialmente correta.~~ Indicou pelo menos uma desvantagem operacional e forneceu explicação parcial.

Conceito 3 – ~~Indicou e explicou corretamente apenas uma desvantagem operacional e(ou) técnica, excluída a complexidade para o usuário.~~ Indicou pelo menos uma desvantagem operacional e forneceu uma explicação completa ou duas explicações parciais.

Conceito 4 – ~~Indicou corretamente duas desvantagens operacionais e(ou) técnicas, mas explicou corretamente apenas uma delas.~~ Indicou pelo menos uma desvantagem operacional e forneceu uma explicação completa e uma explicação parcial.

Conceito 5 – Indicou e explicou corretamente duas desvantagens operacionais e(ou) técnicas.

QUESITO 2.3 Três medidas que possam ser adotadas para a redução do impacto da complexidade do uso de autenticação multifator para os usuários internos, no contexto de uma organização pública

Conceito 0 – Não citou corretamente nenhuma medida.

Conceito 1 – Citou corretamente apenas uma medida.

Conceito 2 – Citou corretamente apenas duas medidas.

Conceito 3 – Citou corretamente três medidas.