Questão 37

Uma empresa de tecnologia desenvolveu um sistema interno para gerenciar projetos. No sistema, administradores podem criar e excluir projetos, gerentes podem adicionar membros às equipes e visualizar relatórios, enquanto funcionários só acessam as próprias tarefas. Durante os testes, um funcionário relatou que conseguiu visualizar projetos de outras equipes, o que representa um risco de segurança. A equipe de desenvolvimento precisa corrigir essa falha.

Qual é a melhor solução para garantir que esse risco de segurança não ocorra?

A Implementar uma abordagem de acesso dinâmico, permitindo que usuários solicitem permissões temporárias conforme a necessidade de suas tarefas.

B Criar um sistema de múltiplos níveis de autorização, permitindo que cada usuário tenha acesso personalizado com base em permissões individuais.

C É a correta
Aplicar um modelo de autorização baseado em funções, associando cada usuário a um papel predefinido que determina seus acessos.

D Adotar um sistema baseado em listas de controle de acesso, configurando permissões específicas para cada recurso e usuário no sistema.

E Limitar o acesso a determinadas funções apenas pelo bloqueio visual de elementos no front-end, impedindo que usuários não autorizados vejam determinadas opções.

Resposta comentada	Feedback do professor
O item avalia se o estudante compreende a importância do modelo de autorização baseado em funções e sua aplicabilidade em sistemas organizacionais. A alternativa correta é a letra C, pois esse modelo estrutura as permissões com base no papel do usuário, garantindo uma gestão eficiente e segura do controle de acesso.	GABARITO: C) Esse modelo define grupos de permissões atribuídas a papéis específicos, reduzindo erros e garantindo que cada usuário tenha apenas os acessos necessários. DISTRATORES: A) Embora possa ser útil em certos cenários, essa abordagem exige monitoramento constante e pode comprometer a segurança ao conceder permissões temporárias sem um controle rígido. B) Esse modelo torna a administração das permissões complexa e difícil de gerenciar em sistemas grandes, aumentando o risco de configurações inconsistentes. D) As listas de controle de acesso podem ser eficazes, mas exigem um gerenciamento minucioso para cada recurso, tornando a implementação menos escalável em comparação ao modelo baseado em funções. E) Apenas esconder elementos no front-end não impede acessos indevidos, pois usuários podem manipular requisições para visualizar dados restritos.