# Questionário de Controlo de Acesso

P1: Qual é o objetivo principal do controlo de acesso em ambientes informáticos?

a. Garantir a confidencialidade e integridade dos dados.
b. Monitorizar e registar a atividade dos sistemas.
c. Permitir o acesso incondicional a todos os utilizadores.
d. Facilitar a comunicação entre diferentes sistemas operativos.

P2: No princípio do menor privilégio, o que é fundamental para a atribuição de acessos?

a. O nível hierárquico do utilizador na organização.
b. A quantidade de acessos previamente efetuados pelo utilizador.
c. Os privilégios exatamente necessários para realizar uma tarefa.
d. A preferência pessoal do utilizador por certos sistemas ou dados.

P3: Em que consiste o modelo de controlo de acesso baseado em listas de controlo de acesso (ACL)?

a. Atribuição de privilégios com base na função do utilizador.
b. Listagem de utilizadores autorizados a acessar cada objeto.
c. Definição de regras automáticas para todas as operações de acesso.
d. Organização de utilizadores em grupos com acessos predefinidos.

P4: O que caracteriza o Controlo de Acesso Discricionário (DAC)?

a. Política fixa de controlo de acesso imposta por um monitor de acesso.
b. Incapacidade dos sujeitos de ajustarem direitos de acesso.
c. Possibilidade de alguns sujeitos atualizarem direitos de acesso de outros.
d. Proibição de qualquer forma de transmissão de capacidades entre sujeitos.

P5: Que mecanismo de controlo de acesso permite ultrapassar as limitações de acesso estabelecidas

a. Controlo de Acesso Baseado em Regras (RBAC).
b. Controlo de Acesso Obrigatório (MAC).
c. Controlo de Acesso Discricionário (DAC).
d. Modelo de controlo de acesso 'Break-the-glass'.

P6: Qual o conceito associado à separação de deveres no contexto do controlo de acesso?

a. Prevenção de conflitos de interesse e fraude através da distribuição de privilégios.
b. Atribuição de todos os privilégios necessários a um único sujeito.
c. Centralização das tarefas de segurança em um administrador do sistema.
d. Acesso irrestrito a dados confidenciais para todos os sujeitos.

P7: No modelo Bell-LaPadula, qual das seguintes afirmações é verdadeira?

a. É permitido ler informação num nível inferior ao do sujeito (no read up).
b. É permitido escrever informação num nível superior ao do sujeito (no write up).
c. É permitido escrever informação num nível inferior ao do sujeito (no write down).
d. É permitido ler informação num nível superior ao do sujeito (no read down).

P8: Qual dos seguintes modelos de controlo de acesso utiliza etiquetas de integridade?

a. Modelo Bell-LaPadula.
b. Modelo Biba.
c. Controlo de Acesso Obrigatório (MAC).
d. Controlo de Acesso Baseado em Papéis (RBAC).

P9: No modelo de integridade de Biba, qual é a regra aplicável à escrita de dados?

a. Um sujeito pode escrever num objeto se tiver um nível de integridade superior.
b. Um sujeito pode escrever num objeto se tiver um nível de integridade inferior.
c. Um sujeito pode sempre escrever num objeto independentemente do nível de integridade.
d. Um sujeito não pode escrever num objeto para manter a integridade dos dados.

P10: Como é que o Controlo de Acesso Baseado em Atributos (ABAC) toma decisões de acesso?

a. Através do papel que o sujeito desempenha na organização.
b. Baseando-se na identificação e autenticação do sujeito.
c. Usando atributos associados às entidades relevantes.
d. Conforme as capacidades transmitidas entre sujeitos.