# Lista 06 - Controles de Acesso

| | |
|---|---|
| *Professor:* | Fábio Engel de Camargo |
| *Disciplina:* | Segurança em Tecnologia da Informação |
| *Meio para entrega:* | Moodle |

1. Qual resposta descreve melhor o componente de autorização de controle de acesso?

   **a)** Autorização é o método que um sujeito utiliza para solicitar acesso a um sistema.

   **b)** Autorização é o processo de criar e manter as políticas e os procedimentos necessários para garantir que informação apropriada esteja disponível quando uma organização for auditada.

   **c)** Autorização é a validação ou prova de que o sujeito que recebeu o acesso foi o mesmo que o solicitou.

   **d)** Autorização é o processo de determinar quem está aprovado para acesso para quais recurso.

2. Qual resposta descreve melhor o comportamento de identificação de controle de acesso?

   **a)** Identificação é a validação ou prova de que o sujeito que recebeu o acesso foi o mesmo que o solicitou.

   **b)** Identificação é o método que um sujeito utiliza para solicitar acesso a um sistema.

   **c)** Identificação é o processo de determinar quem está aprovado para acesso e para quais recursos.

   **d)** Identificação é o processo de criar e manter as políticas e os procedimentos necessários para garantir que informação apropriada esteja disponível quando uma organização for auditada.

3. Qual resposta descreve melhor o componente de autenticação de controle de acesso?

   **a)** Autenticação é a validação ou prova de que o sujeito que recebeu o acesso foi o mesmo que o solicitou.

   **b)** Autenticação é o processo de criar e manter as políticas e os procedimentos necessários para garantir que informação apropriada esteja disponível quando uma organização for auditada.

   **c)** Autenticação é o processo de determinar quem está aprovado para acesso e para quais recursos.

   **d)** Autenticação é o método que um sujeito utiliza para solicitar acesso a um sistema.

4. Qual resposta descreve melhor o componente de responsabilização de controle de acesso?

   **a)** Responsabilização é a validação ou prova de que o sujeito que recebeu o acesso foi o mesmo que o solicitou.

   **b)** Responsabilização é o método que um sujeito utiliza para solicitar acesso a um sistema.

   **c)** Responsabilização é o processo de criar e manter as políticas e os procedimentos necessários para garantir que informação apropriada esteja disponível quando uma organização for auditada.

   **d)** Responsabilização é o processo de determinar quem está aprovado para acesso e para quais recursos.

5. Quando acessa uma rede, você recebe uma combinação de nome de usuário, senha, token, cartão inteligente ou biometria. Você, então, terá acesso autorizado ou negado pelo sistema. Este é um exemplo de _____.

   **a)** Controles de acesso físico.

   **b)** Controles de acesso lógico.

   **c)** Política de inclusão de grupo.

   **d)** Nenhuma das alternativas anteriores.

6. Acesso físico, contorno de segurança e interceptação são exemplos de como os controles de acesso podem ser _____.

   **a)** Roubados

   **b)** Comprometidos

   **c)** Auditados

   **d)** Autorizados

7. Desafios de controle de acesso incluem qual dos seguintes?

   **a)** Perda de laptop

   **b)** Exploração de hardware

   **c)** Interceptação

   **d)** Exploração de aplicativos

   **e)** Todas as alternativas anteriores

8. Analise:

   **I** Segurança física está associada à proteção de recursos através de controles como guardas, iluminação e detectores de movimento.

   **II** Controle de acesso através de usuário e senha específicos em um determinado software aplicativo pode ser caracterizado como um controle físico.

   **III** A segurança física está associada ao ambiente e a segurança lógica aos programas.

   **IV** A segurança lógica deve ocorrer após a segurança física, através de softwares e protocolos.

São corretas as afirmações:

**a)** somente I, II e III

**b)** somente I, II e IV

**c)** somente II, III e IV

**d)** somente I, III e IV

**e)** I, II, III e IVs

9. A respeito do controle de acesso a redes e aplicações, assinale, dentre as alternativas a seguir, a única que contém a ordem correta dos procedimentos lógicos atravessados por um usuário para acessar um recurso:

**a)** Autenticação, Identificação, Autorização e Auditoria.

**b)** Identificação, Autenticação, Autorização e Auditoria.

**c)** Autorização, Identificação, Autenticação e Auditoria.

**d)** Autorização, Autenticação, Identificação e Auditoria.

**e)** Bloqueio, Autenticação, Autorização e Auditoria.

10. A biometria se refere a várias técnicas de autenticação, para distinguir um indivíduo do outro, baseando-se nas características:

**a)** comportamentais, somente.

**b)** físicas e/ou lógicas.

**c)** físicas e/ou comportamentais.

**d)** físicas, somente.

**e)** lógicas, somente.

11. Obter confiança sobre a identidade de agentes ou integridade de dados em comunicação, baseando-se na posse de informação sigilosa (senha), dispositivos (smartcard), dado biométrico (impressão digital, retinal, etc) ou nas combinações destes elementos, trata-se do conceito de:

**a)** criptografia.

**b)** autenticação.

**c)** assinatura digital.

**d)** certificado digital.

**e)** função de hash.

12. Na ausência temporária do operador, o acesso ao computador por pessoa não autorizada pode ser evitado, de forma ideal, com a utilização de:

**a)** uma senha inserida na proteção de tela do Windows.

**b)** uma senha inserida no boot do computador.

**c)** uma senha inserida para acesso ao disco rígido.

**d)** desligamento do monitor, após alguns minutos de inatividade.

**e)** desligamento do computador, sempre que o operador se retirar.

13. Os métodos para implementação de um controle de acesso efetivo envolvem:

**a)** política de senhas, adoção de antivírus e firewall.

**b)** identificação, autenticação, autorização e auditoria.

**c)** assinatura digital, detecção de intrusão e criptografia.

**d)** política de senhas, plano de bloqueio e liberação.

**e)** processo de login e rotinas de backup.

14. Realize uma pesquisa sobre como o controle de acesso é implementado no Linux.

Os sistemas operacionais do mundo UNIX implementam um sistema de ACLs básico bastante rudimentar, no qual existem apenas três sujeitos: user (o dono do recurso), group (um grupo de usuários ao qual o recurso está associado) e others (todos os demais usuários do sistema). Para cada objeto existem três possibilidades de acesso: read, write e execute, cuja semântica depende do tipo de objeto (arquivo, diretório, socket de rede, área de memória compartilhada, etc.). Dessa forma, são necessários apenas 9 bits por arquivo para definir suas permissões básicas de acesso.
(Segurança Computacional - Carlos Maziero, 2019)