

**Disciplina: Segurança de Sistemas**

**Profa.: Rejane Cunha Freitas (**rejane.freitas@faculdadecdo.edu.br**)**

**Exercícios de revisão AP1**

1. Considere um sistema no qual existe um conjunto de informações disponíveis para um determinado grupo de usuários denominados "auditores". Após várias consultas com respostas corretas e imediatas, em um determinado momento, um usuário pertencente ao grupo "auditores" acessa o sistema em busca de uma informação já acessada anteriormente e não consegue mais acessá-la. Neste caso, houve uma falha na segurança da informação para este sistema na propriedade relacionada à:

a) Privacidade b) Integridade c) Consistência d) Irretratabilidade e) Disponibilidade

2. Considere um sistema no qual existe um conjunto de informações disponíveis para um determinado grupo de usuários denominados "auditores". Após várias consultas com respostas corretas, em um determinado momento, um usuário pertencente ao grupo "auditores" acessa o sistema em busca de uma informação e recebe, como resposta à sua consulta, uma informação completamente diferente da desejada. Neste caso, houve uma falha na segurança da informação para este sistema na propriedade relacionada à:

a) Confidencialidade b) Integridade c) Auditoria d) Disponibilidade e) Privacidade

3. Analise as seguintes afirmações relativas a conceitos de Segurança da Informação:

I. Política de Segurança é um conjunto de diretrizes que definem formalmente as regras e os direitos dos funcionários, prestadores de serviços e demais usuários, visando à proteção adequada dos ativos da informação.

II. Integridade é a condição na qual a informação ou os recursos da informação são protegidos contra modificações não autorizadas.

III. Disponibilidade é a propriedade de certas informações que não podem ser disponibilizadas ou divulgadas sem autorização prévia do seu dono.

IV. Uma boa política de segurança independe do treinamento aplicado aos funcionários.

Estão corretos os itens:

a) I e II b) II e III c) III e IV d) I e III e) II e IV

4. Todas as etapas relacionadas à análise, administração e manutenção das medidas de segurança para proteger as informações de uma empresa formam um ciclo que deve retornar ao seu ponto de partida sempre que houver uma falha real ou uma falha em potencial na segurança da informação. Com relação e este ciclo é correto afirmar que:

a) entre as diversas formas de se implementar uma política de segurança, aquela focada em ameaças tem como objetivo aumentar os riscos, para que estes sejam detectados pela análise de risco ou pelos sistemas de auditoria.

b) a perda de integridade, confidencialidade e disponibilidade não se relacionam com riscos do sistema.

c) as ameaças apresentam vulnerabilidades que podem causar perda de integridade.

d) não é recomendado, como medida de segurança a ser tomada por uma entidade, implementar uma política de segurança.

e) o objetivo da análise de risco é identificar vulnerabilidades e ameaças associadas às informações, identificar o impacto nos negócios em caso de sua ocorrência e sugerir planos de contingências.

5. Em uma das reuniões iniciais para a definição da Política de Segurança da Informação de uma empresa, os participantes estão discutindo afirmativas que foram feitas.

I - A política deve, sempre que possível, indicar alguma forma de punição para aqueles que a desrespeitarem ou, do contrário, ela simplesmente será ignorada. Por exemplo, as punições previstas para o não-cumprimento da política devem respeitar as leis de contrato de trabalho da organização, como a CLT, que prevê desde simples advertências até o desligamento por justa causa.

II - As pessoas, como ativos de informação, também possuem vulnerabilidades, entre as quais não conhecer as normas, não saber os limites, não saber o que é confidencial ou não, entre muitas outras. A política deve endereçar esse tipo de vulnerabilidade, diminuindo o risco de que ameaças consigam explorar as vulnerabilidades das pessoas.

III - A política regula o comportamento sobre o uso da informação em diversos níveis e meios. Sempre que for aplicável, ela deve apontar o responsável pela informação e a forma correta de uso, podendo estabelecer, por exemplo, que o sistema de correio eletrônico deve ser utilizado exclusivamente para fins profissionais relacionados com a empresa em questão.

IV - A classificação dos ativos de informação é uma etapa importante no processo de garantia de segurança da informação. Classificar envolve, por exemplo, inventariar, definir o grau de relevância e identificar esses ativos de informação. Esse processo, além de estruturar e permitir uma gestão mais eficiente dos ativos, contribui significativamente para a análise e tratamento de riscos de segurança da informação.

Com base nos aspectos relacionados à Política de Segurança da Informação em uma empresa estão corretos apenas os conjuntos de afirmativas:

a) I e III. b) II e III. c) I, II e IV. d) II, III e IV e) I, II, III e IV.

.

7. Ao passo que as informações são consideradas o principal patrimônio de uma organização, hoje em dia, estas estão sob constante risco, fazendo com que a segurança da informação tenha se tornado crucial para a sobrevivência das organizações. **Assinale V ou F, para as alternativas a seguir**:

a) (V) a definição técnica de ameaça concretizada é a consequência de uma vulnerabilidade do sistema ter sido explorada.

b) (F) a observação e conhecimento de informações armazenadas em sistemas ou a análise do tráfego de uma rede são considerados ataques ativos.

c) (V) são classificadas como informações confidenciais aquelas cujo acesso interno ou externo de pessoas não autorizadas é crítico para a empresa, sendo imprescindível um número restrito de pessoas autorizadas e o controle total sobre o uso das informações.

d) (V) a autenticação é como os usuários informam à infraestrutura de rede quem são eles.

e) (F) a política de segurança deve ser flexível e viável a longo prazo. Todavia, não pode ser definida de modo independente de software e hardware específicos.

f) (V) a auditoria da Segurança da Informação faz parte da auditoria da Tecnologia da Informação e engloba a avaliação da política de segurança, de controles de aspectos de segurança institucional globais (lógico, físico e ambiental) e de planos de contingência e continuidade dos serviços.

g) (F) controle de acesso é aplicado após a implementação da política de segurança para garantir que todos os itens da política estão sendo cumpridos.

8. Quais são as diferenças entre transmitir a mensagem secretamente e manter a integridade da mensagem? Podemos ter uma sem a outra? Justifique a sua resposta.

Eu posso transmitir uma mensagem secretamente, mantendo a integridade, por meio da utilização da criptografia. Uma mensagem secreta é uma mensagem que somente as partes endereçadas irão receber, enquanto a integridade da mensagem é quando uma mensagem chega sem alteração.

9. Qual é a diferença entre um intruso ativo e um passivo?

Um intruso ativo é aquele que aproveita as vulnerabilidades de um sistema realiza modificações nas informações acessadas e/ou instala um software para captar todas as informações disponíveis, enquanto o passivo somente observa e cria conhecimento de informações armazenadas em sistemas.

10. Explique o conceito de ameaças à segurança da informação e caracterize as ameaças externas e internas.

Ameaça à segurança é qualquer fator ou ação capaz de interferir e causar danos à integridade, à confidencialidade e à disponibilidade de dados e informações da empresa. Internas: colaboradores, fornecedores. Externos: hackers (White hats e Black hats), cyber ativismo.