1- Ao cifrar uma informação utilizando um algoritmo criptográfico e uma chave secreta, qual propriedade de segurança estará sendo garantida?

a) Autenticidade.

b) Disponibilidade.

c) Confidencialidade.

d) Irrefutabilidade.

e) Integridade

2- A biometria é uma técnica utilizada para garantir um princípio da segurança da informação. Esse princípio é conhecido como:

a) confidencialidade.

b) integridade.

c) autenticidade.

d) disponibilidade.

e) vulnerabilidade.

3- José utilizou uma ferramenta para criptografar uma informação a ser transmitida para Maria, com o objetivo de proteger a informação contra acesso não autorizado. O requisito básico de segurança da informação assegurado pela criptografia é a

a) autenticidade.

b) confidencialidade.

c) disponibilidade.

d) confiabilidade.

e) irretratabilidade.

4- Analise a afirmação abaixo e defina se é verdadeira ou falsa e justifique a escolha.

A principal diferença entre crackers e hackers refere-se ao modo como esses malfeitores da área de segurança da informação atacam: os crackers são mais experientes e realizam ataques sem utilizar softwares, ao passo que os hackers utilizam códigos maliciosos associados aos softwares para realizar ataques ao ciberespaço.

R: Falsa, ambos utilizam softwares, possuem o mesmo conhecimento, porem os crackers roubam dados de empresas para beneficio próprio, enquanto os hackers informas as vulnerabilidades para empresa invadida

5- A segurança de computadores se define como a proteção oferecida a um sistema de informação automatizado para atingir os objetivos apropriados de preservação da confidencialidade, integridade e disponibilidade (Tríade CID) de ativos de sistemas de informação (incluindo hardware, software, firmware, informações/dados e telecomunicações). Porém, ao longo do tempo, foram acrescentados outros elementos para fortalecer as políticas de proteção de dados. Posto isso, analise as afirmativas abaixo:

I - Integridade: defender contra a modificação ou destruição imprópria de informações.

II- Confidencialidade: preservar restrições autorizadas ao acesso e revelação de informações, incluindo meios para proteger a privacidade pessoal e as informações proprietárias.

III - Disponibilidade: assegurar que o acesso e o uso das informações seja confiável e realizado no tempo adequado.

IV - Irretratabilidade (não repúdio): protege contra a confirmação, por parte do remetente ou destinatário, da autenticidade ou recebimento de dados, assegurando que eles possam recusar sua participação ou autoria, se desejarem.

V - Ameaça: tentativa de violação da segurança do sistema.

VI - Vulnerabilidade: falha, defeito ou fraqueza no projeto, implementação ou operação e gerenciamento de um sistema que poderia ser explorado para violar a política de segurança do sistema.

VII - Risco: expectativa de perda de segurança expressa como a probabilidade de que uma ameaça particular explore uma vulnerabilidade particular com resultado danoso particular.

VIll - Ataque: um potencial para violação de segurança que existe quando há circunstância, capacidade, ação ou evento que poderia infringir a segurança e causar dano.

Estão corretas:

A - I, II, IV, V, VI, VII, apenas.

B - I, III, VI, VII, VIII, apenas.

C - I, II, III, IV, V, VII, apenas.

D - I, II, III, VI, VII, apenas.

E - Todas as afirmações estão corretas.

6- Sobre o Princípio da Integridade, é correto afirmar que:

A) a informação deverá estar disponível sempre que um usuário autorizado queira acessá-la.

B) garante o sigilo da informação, impedindo que ela seja acessada por pessoas não autorizadas.

C) impossibilita o emissor negar a autoria de determinada mensagem ou transação.

D) assegura que a informação não sofra qualquer alteração por usuário não autorizado. Além de garantir entrega, recebimento ou armazenamento do conteúdo completo sem qualquer perda.

E) garante que o autor da informação é realmente quem ele diz que é.

7) O objetivo da Gestão de Segurança de Informação é manter a qualidade das informações. Relacione a primeira coluna com a segunda, no que diz respeito aos conceitos sobre Gestão de Segurança da Informação.

Confidencialidade(1) (\_) propriedade de proteger a exatidão de ativos

Integridade(2) (\_) causa potencial de um incidente indesejado, o que pode resultar em danos para um sistema ou entidade

Gestão de risco(3) (\_) propriedade que garante que a informação não está disponível ou revelada a indivíduos não autorizados, entidades ou processos

Ameaça(4) (\_) atividades coordenadas para dirigir e controlar uma organização em relação a um determinado risco

A sequência CORRETA da segunda coluna é:

A) 1-2-3-4

B) 2-3-1-4

C) 2-4-1-3

D) 1-4-2-3