Instituto Federal de Santa Catarina – Campus Gaspar
Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas
Disciplina.: Segurança da Informação
Prof. Fabio César Schuartz

Nome.: _____ Data.:

Segurança da Informação - Primeira Avaliação

a) Coloque seu nome e data a caneta;
b) Utilize caneta, provas a lápis não são elegíveis a revisão;
c) Evite rasuras nas questões objetivas, questões assinaladas em mais de uma letra são consideradas erradas;

1. (1,0) Cite três condições genéricas que podem aumentar o risco das informações de uma empresa a serem comprometidas.

2. (1,0) Cite e descreva as três propriedades principais da informação que devemos proteger.

3. (1,0) Os momentos vividos pela informação que a colocam em risco durante o seu ciclo de vida são:

a) Criação, manuseio, transporte e validação.
b) Criação, armazenamento, validação e descarte.
c) Preparação, manuseio, validação e armazenamento.
d) Manuseio, armazenamento, transporte e descarte.
e) Preparação, transporte, validação e armazenamento.

4. (1,0) Analise as sentenças abaixo e assinale a alternativa correta.

I - Vulnerabilidade são fraquezas presentes nos ativos de informação, que podem causar, apenas de maneira intencional, a quebra de um ou mais dos três princípios de segurança da informação.
II - Ameaça é um agente externo ao ativo de informação que poderá quebrar um ou mais dos três princípios de segurança da informação suportada ou utilizada por este ativo.
III - A probabilidade é a chance de uma falha de segurança ocorrer levando-se em conta o grau das vulnerabilidades presentes nos ativos que sustentam o negócio e o grau das ameaças que possam explorar estas vulnerabilidades.

a) Somente a sentença I está correta.
b) Todas as sentenças estão corretas.
c) As sentenças I e III estão corretas.
d) As sentenças II e III estão corretas.
e) Nenhuma das sentenças está correta.

5. (1,0) Ao fazer uma análise referente ao risco, descreva quais são as ações que podem ser tomadas em relação a ele.

6. (1,0) Considere os quatro métodos para se comprometer a segurança de sistemas de informação: (a) Interceptação da entrada; (b) Técnicas de engenharia social; (c) Força-bruta e (d) Criptoanálise. Para os seguintes tipos de ataques, caracterizar cada um deles com um método.

a) Sequestro de navegador:
b) Dicionários:
c) Sniffing:
d) Phishing:
e) Sequestro de sessão:
f) Man-in-the-middle:
g) Keyloggers:
h) Tabelas Rainbow:

7. (1,0) O que são controles físicos e controles lógicos? Dê 2 exemplos de cada tipo de controle.

8. (1,0) Assinale (V) para verdadeiro ou (F) para falso, a respeito das seguintes afirmações:

( ) Para que um sistema comece a ser considerado seguro, ele precisa submeter-se a uma auditoria de segurança independente.
( ) Existe proteção total contra código malicioso.
( ) Você não pode trocar chaves de criptografia com segurança sem uma informação compartilhada.
( ) Algoritmos criptográficos secretos não são seguros.
( ) Segurança do lado do cliente não funciona.
( ) As senhas não podem ser armazenadas com segurança no cliente.

9. (1,0) Para responder esta questão, utilize o método da Cifra de Vigenère para descriptografar a seguinte mensagem:

bttjobmf upebt bt pqçõft bcbjyp

( ) Somente pelo período da manhã;
( ) Entre os períodos da manhã e da tarde;
( ) Entre os períodos da tarde e noite;
( ) Somente no período noturno;
( ) Em qualquer período.

10. (1,0) Qual a diferença entre criptografia simétrica e assimétrica?