ARA0064 - INTRO SEGURANÇA DA INFORMAÇÃO

Prof. Simone Gama

Parte I - Introdução e conceitos de Segurança da Informação

1. Conceitue Dados, Informação e Conhecimento. Conceitue os principais pontos do ciclo da informação.

2. Elencar os principais pontos sobre a avaliação da qualidade da informação.

3. Descreva sobre os principais Pilares da Segurança da Informação e elenque exemplos de T.I. sobre cada um deles.

4. Descreva sobre os principais pilares que compõe o Hexagrama Parkeriano.

5. Sejam as seguintes afirmações sobre os Pilares da Segurança da Informação e Análise de Riscos:

   I. O valor da informação sob o olhar da Confidencialidade da Análise de riscos está relacionado com a garantia de que a informação é exata e completa.

   II. A disponibilidade é uma propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

   III. A propriedade da Integridade garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação.

   IV. A legalidade é um princípio que garante o alinhamento das informações dentro das normas, portarias e leis.

   Estão **incorretas** apenas as afirmativas:

   a) I apenas;
   b) II e IV;
   c) I e II;
   d) III apenas;
   e) I e III apenas.

Parte II - Ameaças e Vulnerabilidades

6. Descreva as principais diferenças entre ativos tangíveis lógicos e físicos.

7. Correlacione corretamente as colunas de acordo com os tipos de ameaças da informação sob os aspectos dos pilares da segurança da informação:

   a) Disponibilidade ( ) Corrupção e/ou alteração de dados
   b) Confidencialidade ( ) Acesso não autorizado
   c) Integridade ( ) Ataques de Negação de Serviço

Estácio

ARA0064 - INTRO SEGURANÇA DA INFORMAÇÃO

Prof. Simone Gama

8. Descreva as principais diferenças entre Riscos, ameaças e Vulnerabilidades.

9. Descreva o conceito de ataques cibernéticos e exemplifique.

10. Marque V para Verdadeiro e F para Falso sobre os principais tipos de Software Maliciosos:

a. ( ) Os trojans, mais conhecidos como Cavalos de Tróia, são divididos em três partes, a saber: Mecanismo de Infecção, Mecanismo de Ativação e Carga Útil.

b. ( ) Os spyware's tem como principal objetivo espionar a máquina da vítima.

c. ( ) Os trojans, mais conhecidos como Cavalos de Tróia, simulam presentes inofensivos que, além de executar funções às quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário.

d. ( ) Os vírus costumam atacar sob três frentes: em forma de arquivos, de programas e no formato mutante.

e. ( ) Os keylooger's são um tipo de vírus de computador, muito semelhante aos Worms, que tem por objetivo destruir arquivos do tipo .doc do computador.

11. Marque V para Verdadeiro e F para Falso sobre Ataque de Negação de Serviços

a. ( ) O objetivo dos ataques de Negação de Serviço, ou *DoS* (*Denial of Service*), é interromper atividades legítimas de um servidor de web e o ataque procura tornar as páginas hospedadas indisponíveis na rede.

b. ( ) O *DDoS* ataca diretamente o pilar da confidencialidade da Segurança da Informação.

c. ( ) Em um ataque *DDoS*, um computador mestre denominado *master* pode ter sob seu comando até milhares de computadores zombies, literalmente zumbis.

d. ( ) Em um ataque *DDoS* volumérico, os atacantes direcionam solicitações legítimas para um servidor DNS por meio de um endereço IP falso.

e. ( ) Em um ataque *DDoS* por exploração, os atacantes direcionam os ataques a camada física do Modelo OSI, mais conhecida também como ataque do tipo 1.

ARA0064 - INTRO SEGURANÇA DA INFORMAÇÃO

Prof. Simone Gama

12. São consideradas vulnerabilidades e/ou ameaças a um sistema, exceto:

a. ( ) Acessos não autorizados ou perda de comunicação;

b. ( ) Instalações prediais, incluindo a presença de detectores de fumaça e outros recursos para combate a incêndio.

c. ( ) Erros na instalação ou na configuração de softwares.

d. ( ) Invasão e/ou monitoramento do sistema, mesmo sem alteração de informações.

13. É uma fraqueza de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças" (HINTZBERGEN, 2018). A definição apresentada refere-se ao conceito de:

a. ( ) Exposição

b. ( ) Salvaguarda

c. ( ) Vulnerabilidade

d. ( ) Risco

Observações - LEIA ATENTAMENTE:

- **Exercício Avaliativo p/ AV1, vale 3,0 pontos. A AVALIAÇÃO AV1 valerá 7,0 pontos.**
- A data de entrega é dia **14/04/2022**, até às 17hs, em formato .pdf, sem prorrogações e aceites fora do dia e horário estipulado, em respeito aos colegas que entregaram no prazo.
- A entrega será feita via ferramenta Teams e **somente** no espaço reservado para a entrega do exercício, não sendo aceito por outro meio, seja chat privado, email's, etc.
- Organização também faz parte do processo avaliativo, portanto, ao entregar, organize as questões e identifique seu exercício.
- As questões cobrem todo o assunto abordado em sala de aula, bem como assunto do conteúdo digital, que se encontra na sala de aula virtual da disciplina.