CENTRO UNIVERSITÁRIO DA GRANDE DOURADOS
PROVA
Protocolo: 659614

Exame

Curso: Tecnologia em Análise e Desenvolvimento de Sistemas
Disciplina: Segurança das Informações

Ano: 20221
Semestre: 5

RGM: _____ Aluno: _____

PROVA 01

Questão 1
Analise as afirmações abaixo tendo como base os conceitos de ameaças e assinale a opção correta.

i. Falta de energia elétrica não é uma ameaça involuntária a um servidor quando for provocada durante uma chuva com raios.
ii. Falta de energia elétrica sempre será classificada como ameaça involuntária a um servidor quando for provocada durante uma chuva com raios.
iii. Falta de energia elétrica sempre será classificada como ameaça involuntária a um servidor sem no-break quando for provocada durante uma chuva com raios.
iv. Falta de energia elétrica sempre poderá classificada como ameaça involuntária e voluntária a um servidor sem no-break quando for provocada por um funcionário.
v. Falta de energia elétrica sempre será classificada como ameaça voluntária a um servidor quando for provocada por um funcionário.

a) Estão corretas somente as afirmações i e v.
b) Estão corretas somente as afirmações i, ii e iii.
c) Estão corretas somente as afirmações i e iv.
d) Estão corretas somente as afirmações i, ii e iv.
e) Todas as afirmações são corretas.

Questão 2
As fases de Gestão de Risco da Segurança da Informação devem ser executadas na seguinte ordem:

a) Definição do Escopo, Identificação dos Riscos, Avaliação dos Riscos, Análise dos Riscos, Tratamento dos Riscos e Monitoração e Avaliação dos Resultados.
b) Definição do Escopo, Análise dos Riscos, Identificação dos Riscos, Avaliação dos Riscos, Tratamento dos Riscos e Monitoração e Avaliação dos Resultados.
c) Definição do Escopo, Identificação dos Riscos, Avaliação dos Riscos, Tratamento dos Riscos, Análise dos Riscos e Monitoração e Avaliação dos Resultados.
d) Definição do Escopo, Identificação dos Riscos, Análise dos Riscos, Avaliação dos Riscos, Tratamento dos Riscos e Monitoração e Avaliação dos Resultados.

Questão 3
O objetivo da segurança organizacional em relação a segurança da informação (SI) é:

a) Implantar a Segurança da Informação na empresa.
b) Implantar e Avaliar a Segurança da Informação na empresa.
c) Definir papéis, funções e responsabilidades em relação a Segurança da Informação
d) Planejar, avaliar, implantar e corrigir a SI dentro da empresa.

Questão 4
Com relação aos algoritmos criptográficos listados abaixo, assinale a alternativa correta.
i. 3-DES
ii. BLOWFISH
iii. RC2
iv. RSA
v. DSS

a) Os algoritmos listados nos itens i, ii e iii são utilizados na criptografia assimétrica
b) Os algoritmos listados nos itens i, ii e iv são utilizados na criptografia simétrica
c) Os algoritmos listados nos itens ii e v são utilizados na criptografia assimétrica
d) Os algoritmos listados nos itens ii, iii e iv são utilizados na criptografia simétrica
e) Os algoritmos listados nos itens iv e v são utilizados na criptografia assimétrica

Questão 5
Abaixo estão listadas cinco ações. Tendo como base as fases da gestão da segurança da informação assinale a opção correta.
i. Criar a equipe de segurança da informação bem como a sua estrutura hierárquica
ii. Inventariar os processos de negócios críticos da empresa
iii. Relizar o treinamento de funcionários e conscientização dos mesmos sobre a importância da segurança da informação para o negócio da empresa.
iv. Realizar simulações de ataques para medir a eficácia das medidas de segurança.

a) As ações listadas nos itens ii e iii são tomadas na fase de planejamento da gestão da Segurança da Informação.
b) As ações listadas nos itens i e iii são tomadas na fase de planejamento da gestão da Segurança da Informação.
c) As ações listadas nos itens iii e iv são tomadas na fase de planejamento da gestão da Segurança da Informação.
d) As ações listadas nos itens i e iv são tomadas na fase de planejamento da gestão da Segurança da Informação.
e) As ações listadas nos itens i e ii são tomadas na fase de planejamento da gestão da Segurança da Informação.

Questão 6
A técnica que aplica um polinômio associado com uma chave a um texto transformando o seu conteúdo em outro texto incompreensível. Somente quem conhecer a chave e o polinômio consegue transformar o texto incompreensível em sua forma original é chamado de:

a) Esteganografia simétrica.
b) Criptografia simétrica.
c) Criptografia assimétrica.
d) Esteganografia assimétrica.

Questão 7
Selecione opção correta que corresponda a um ativo de informação segundo a norma NBR ISO/IEC 17799:2005.

a) Serviços de computação e comunicação.
b) Aplicativos.
c) Planos de continuidade do negócio.

d) Pessoas e suas qualificações, habilidades e experiências

Questão 8
Analise as afirmações abaixo e seleciona a opção correta.

i. O requisito de confidencialidade é conseguido utilizando-se criptografia.
ii. No meio eletrônico a utilização de senhas garante a autenticidade.
iii. A disponibilidade é conseguida utilizando hardware redundantes.
iv. A confiabilidade é conseguida utilizando-se par de chaves criptográficas.

a) Estão corretas somente as afirmações i e iii
b) Estão corretas somente as afirmações i, ii e iii
c) Estão corretas somente as afirmações ii e iv
d) Estão corretas somente as afirmações i, ii e iv
e) Estão corretas somente as afirmações ii e iii

Questão 9
Assinale a opção que completa corretamente as lacunas do parágrafo abaixo:
O protocolo ____ garante a _____.

a) SSL / autenticidade e a integridade.
b) HTTP / autenticidade e a integridade.
c) POP / a autenticidade e a integridade.
d) SSL / confidencialidade, a autenticidade e a integridade.
e) HTTP / confidencialidade, a autenticidade e a integridade.

Questão 10
As afirmações são sobre alguns tipos de ataque, analise-as e assinale a opção correta.

i. O ataque de Port-Scannig é contra a disponibilidade.
ii. O ataque DoS é contra a autenticidade.
iii. O ataque de IP-Spoofing é contra a autenticidade.
iv. O ataque de Sniffing é contra a confidencialidade.

a) Estão corretas somente as afirmações i e iii.
b) Estão corretas somente as afirmações iii e iv.
c) Estão corretas somente as afirmações ii e iii.
d) Todas as afirmações são corretas.
e) Todas as afirmações são incorretas.

Questão 11
As informações que devem ser de conhecimento somente de um determinado departamento da empresa são classificadas como:

a) Confidenciais.
b) Restrita.
c) Pública.
d) Privada.

Questão 12
O ciclo de vida das informações é:

a) Produção, refinamento, distribuição, utilização e descarte.
b) Obtenção, refinamento, utilização, armazenamento e descarte.
c) Obtenção, refinamento, distribuição, utilização, armazenamento e descarte.
d) Obtenção, distribuição, armazenamento, utilização e descarte.
e) Produção, distribuição, utilização, descarte.

Questão 13
Assinale qual ação não faz parte da fase de planejamento da Segurança da Informação:

a) Inventariar os processos de negócios críticos da empresa.
b) Fazer a análise de cláusulas contratuais e da legislação a que a empresa deve atender.
c) Divulgação da política de segurança da informação.
d) Criar a equipe de segurança da informação bem como a sua estrutura hierárquica.
e) Inventariar os processos de negócios críticos da empresa.

Questão 14
Selecione a opção que completa corretamente as lacunas do texto abaixo.
O _____ é uma ferramenta que analisa os bytes de dados dos pacotes TCP ou UDP e compara com uma base de dados que contém os dados de pacotes de ataques conhecidos. Com isso ele consegue detectar se um ataque está ocorrendo. Já o _____ além de detectar a ocorrência de um ataque ele consegue impedir a continuidade desse ataque.

a) IPS/IDS
b) PROXY/IPS
c) IPS/PROXY
d) IDS/IPS
e) IDS/PROXY

Questão 15
Sobre política de segurança da informação (PSI) analise as afirmações listadas de i a iv abaixo e assinale a opção correta.
i. Sua elaboração deve ser realizada por consultores externos, com isso garante-se uma política muito mais eficiente.
ii. Para garantir o comprometimento a política deve ser aprovada pelos chefes de setores.
iii. A conformidade da PSI deve ser feita por pessoas não pertencentes ao setor auditado.
iv. A política de informação destina-se apenas aos funcionários de uma empresa.

a) Somente a afirmação III está incorreta.
b) Somente estão corretas as afirmações ii e iii.
c) Somente a afirmação iii está correta.
d) Todas as afirmações são corretas.
e) Somente estão incorretas as afirmações ii e iii.

Questão 16
Assinale a alternativa correta.

a) Falta de energia elétrica é somente uma vulnerabilidade voluntária.

b) Falta de energia elétrica é uma vulnerabilidade voluntária e involuntária.
c) Falta de energia elétrica pode ser uma ameaça involuntária e voluntária.
d) Falta de energia elétrica é somente uma ameaça involuntária.
e) Falta de energia elétrica é somente um ameaça voluntária.

Questão 17
Dada as características listadas nos itens de i a v assinale a alternativa correta.
i. Garantir a autenticidade.
ii. Garantir a integridade.
iii. Garantir a confidencialidade.
iv. Utilizar um par de chaves criptográficas.
v. Utilizar uma chave criptográfica.

a) São características da criptografia simétrica as apresentadas nos itens iii, iv e v
b) São características da criptografia simétrica as apresentadas nos itens iii e v
c) São características da criptografia simétrica as apresentadas nos itens iv e v
d) São características da criptografia simétrica as apresentadas nos itens iii e iv
e) São características da criptografia simétrica as apresentadas nos itens ii, iv e v

Questão 18
Assinale a opção que complete corretamente a frase abaixo.Segundo o seu conteúdo podemos classificar as informações como:

a) Pública, Restrita e Confidencial.
b) Sigilosa, privada e pública.
c) Informações pessoais, restritas e públicas
d) Informações pessoais, de segurança nacional e informações de negócio.

Questão 19
No armazenamento das informações, quais os requisitos básicos de SI devem ser observados. (assinale apenas uma opção)

a) Integridade, confiabilidade e autenticidade.
b) Confiabilidade e integridade.
c) Integridade, disponibilidade e confidencialidade.
d) Integridade e disponibilidade.
e) Disponibilidade e confiabilidade.

Questão 20
Em segurança da informação podemos definir risco como sendo:

a) A possibilidade de ocorrência de uma vulnerabilidade
b) A ocorrência de uma vulnerabilidade
c) A ocorrência de uma ameaça
d) A probabilidade de ocorrência de uma ameaça
e) A ocorrência de um ataque