Questão 1

Segurança da informação só é possível se todos da organização seguirem os mesmos princípios e realizarem suas tarefas do dia a dia com base em preocupações comuns de manutenção das propriedades da segurança da informação.
Complete a lacuna e assinale a alternativa correta.
Antes,a_____ tinha como objetivo a comunicação secreta, e atualmente foram acrescentados objetivos de autenticação de mensagens, assinatura digital, protocolos para troca de chaves secretas, protocolos de autenticação, leilões e eleições eletrônicas, dinheiro digital.

A. ○ Integridade

B. ○ Segurança da Informação

C. ○ Política da Segurança

D. ○ Disponibilidade

E. ● **Criptografia**

Questão 2

A Criptografia tem como definição que é a arte de escrever ou resolver códigos. A criptografia deriva de duas palavras gregas: *kryptos*, que significa oculto, e *graphien*, que significa escrever. Seu objetivo não é esconder a existência da mensagem, mas sim de apenas ocultar o seu significado.
Um certificado digital é um arquivo de dados contendo segmentos ou seções que possuem informações obrigatórias e adicionais armazenada em extensões. A utilização de certificados digitais permite que sejam agregados requisitos de segurança na tramitação de informações. Dentre esses requisitos, está a garantia da impossibilidade de que o autor recuse a autoria.
Esse é o requisito de:

A. ○ integridade.

B. ● **não-repúdio.**

C. ○ autenticidade.

D. ○ sigilo.

E. ○ privacidade.

Questão 3

Os testes de penetração ou pentests, são também conhecidos como testes de intrusão e ethical hacking, e são realizados a partir do ambiente externo.

O teste de _____ é o teste em que alguma informação é provida para o profissional, como uma credencial de acesso, enquanto outras informações têm que ser descobertas.

A. Yellow-Box

B. **Gray-Box.**

C. White-Box.

D. Red-Box

E. Black-Box.

Questão 4

A auditoria requer que o auditor busque evidências, avalie as forças e fraquezas de controles internos com base nas evidências coletadas, e prepare um relatório de auditoria que apresenta as fraquezas e recomendações para a remediação de uma forma objetiva para os atores envolvidos (ISACA, 2016).
Considerando as principais fases de um processo de auditoria, analise as afirmativas e assinale a alternativa correta:

I.Planejamento

II. Trabalho em campo

III. Relatórios

Estão corretas as afirmativas:

A. Apenas II e III

B. Apenas I e III

C. **I, II e III**

D. Apenas I e II

E. Apenas I

Questão 5

Para Nakamura.(2016), o termo *malware* vem do inglês malicious software, ou software malicioso, que causa, intencionalmente,danos à vítima.
Nakamura, Emílio Tissato. Segurança da Informação e redes. Londrina: Editora e Distribuidora Educacional S.A., 2016. 224 p.
Banca :IDECAN **Órgão:**PRODEB **Prova:**Assistente - Suporte **Analise as afirmativas sobre*softwares* maliciosos, marque V para as verdadeiras e F para as falsas.**
( )Para que o vírus se torne ativo e continue o processo de infecção, é necessário que o programa ou arquivo hospedeiro seja executado.
( )*Botnet* é o conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.
( )*Worm* é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.
( )Cavalo de Troia é um programa que permite o retorno de um invasor a um computador comprometido por meio da inclusão de serviços criados ou modificados para este fim.
A sequência está correta em:

A. V, V, F, F.

B. V, V, V, V.

C. F, V, F, V.

Questão 6

Assinale a alternativa que identifica de forma correta, somente princípios relacionados de forma direta ao contexto de segurança à interconexão dos sistemas.

A. Confiabilidade, integridade, disponibilidade, autenticação e não repúdio.

B. Confiabilidade, integridade, disponibilidade, autenticação e confidencialidade.

C. Confidencialidade, integridade, disponibilidade, programação e configuração.

D. Confiabilidade, integridade, disponibilidade, autenticação e repúdio.

E. Confidencialidade, integridade, disponibilidade, autenticação e configuração.

Questão 7

A forma de executar a auditoria é importante, com o uso das técnicas e ferramentas mais adequadas para cada objetivo.
O _____da ISACA é um framework de auditoria de TI que define padrões para as auditoria de TI relacionadas aos papéis e responsabilidades, ética, comportamento esperado e conhecimento e qualificação requeridas, além de termos e conceitos específicos ao assunto.
O que completa corretamente a definição é:

A. COBIT
B. SWOT
C. ITIL
D. **ITAF**
E. Ansoff

Questão 8

Engenharia social é uma técnica de ataque em segurança da informação.
Considere o recebimento de um e-mail que informa o usuário a respeito de uma suposta contaminação do computador dele por um vírus, sugerindo a instalação de uma ferramenta disponível em um site da Internet para eliminar a infecção. Entretanto, a real função dessa ferramenta é permitir que alguém tenha acesso ao computador do usuário e a todos os dados lá armazenados. Este método de ataque trata-se de:

A. Ransoware
B. Denial of Service.
C. Exploit.
D. Sniffer.
E. **Engenharia Social.**

Questão 9

A proteção de uma empresa é feita com o uso de mecanismos de segurança tecnológicos, físicos, processuais e regulatórios. É com a sua implementação que as finalidades de prevenção, detecção e resposta a incidentes são cumpridas.
É uma combinação de hardware e software que isola a rede interna de uma organização da internet em geral, permitindo que alguns pacotes passem e bloqueando outros, trata-se do:

A. link.

B. outlook.

C. plugin.

D. **firewall.**

E. browser.

Questão 10

A engenharia social é uma técnica de ataque utilizada para explorar a natureza Humana.
MITNICK, Kevin D.; SIMON, William M. A arte de enganar. São Paulo: Makron Books, 2003.
Aplicada em: 2017 **Banca:** IESES **Órgão:** IGP-SC **Prova:** Perito Criminal em Informática(adaptada)
Considerando as práticas do que se denomina 'Engenharia Social' no contexto da Segurança da Informação, é correto:

A. Algoritmos de 'força bruta' são um instrumento comumente utilizados para descoberta de informações.

B. A utilização de certificados digitais A3 é mais adequada que certificados A1.

C. Usa firewall.

D. A instalação de softwares detectores de 'phishing' é uma estratégia para evitar ataques de um engenheiro social.

E. **Um 'ataque' de engenharia social pode utilizar estratégias de relacionamento pessoal para obtenção de informações sigilosas.**

Questão 11

As ferramentas de segurança visam à prevenção, detecção e resposta a ataques, protegendo os ativos contra-ataques que comprometam uma das propriedades básicas de segurança da informação.
Aplicada em: 2017 **Banca:** IESES **Órgão:** IGP-SC **Prova:** Perito Criminal Geral
https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-seguranca-da-informacao/politicas-de-seguranca-de-informacao
Considere as afirmativas abaixo referentes aos três principais objetivos em se tratando de segurança da informação:
I. A confidencialidade garante que a informação não será conhecida por pessoas que não estejam autorizadas para tal.
II. A integridade garante que a informação armazenada ou transferida mantém suas características originais e é apresentada corretamente às entidades que tenham acesso a mesma.
III. A disponibilidade visa garantir a existência de qualquer entidade que tenha acesso à informação.
Estão corretas as afirmativas:

A. ○ **Apenas** I e II

B. ○ **Apenas** I e III

C. ○ **Apenas I**

D. ◉ **I, II e III**

Questão 12

Em relação a identificação do usuário para a garantia eficaz do gerenciamento de senhas.
A partir do contexto acima, analise as afirmativas I, II e III e assinale a alternativa correta.
I - Armazene e transmita senhas de forma segura.
II – Não armazene os arquivos de senhas separados dos dados do sistema de aplicação.
III - Mostre senhas na tela.

A. ◉ **Somente a afirmativa I está correta.**

B. ○ Somente a afirmativa III está correta.

C. ○ As afirmativas I, II e III estão INCORRETAS.

D. ○ As afirmativas I, II e III estão corretas.

E. ○ Somente a afirmativa II está correta.

Questão 13

As ferramentas de segurança visam à prevenção, detecção e resposta a ataques, protegendo os ativos contra ataques que comprometam uma das propriedades básicas de segurança da informação.
Prova: ESAF - CGU - Analista de Finanças e Controle - Tecnologia da Informação - Prova 3 Disciplina: Segurança da Informação | Assuntos: Auditoria de Sistemas;
Considere um sistema no qual existe um conjunto de informações disponível 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. ○ Privacidade

B. ● **Disponibilidade**

C. ○ Auditoria

D. ○ Integridade

E. ○ Confidencialidade

Questão 14

Segurança da informação só é possível se todos da organização seguirem os mesmos princípios e realizarem suas tarefas do dia a dia com base em preocupações comuns de manutenção das propriedades da segurança da informação.
Quando executamos o ataque :"Modificar imagens ou textos de um site ou substituí-los por informações ilegítimas". Estamos nos referindo ao ataque de:

A. ○ Fraude financeira.

B. ○ Vandalismo.

C. ○ Roubo de informações confidenciais.

D. ○ Ataque DoS (Denial of Service).

E. ● **Phishing.**

Questão 15

A segurança da informação só é possível se todos da organização seguirem os mesmos princípios e realizarem suas tarefas do dia a dia com base em preocupações comuns de manutenção das propriedades da segurança da informação

Banca: FCC, **Órgão:** MPE-RN **Prova:** Analista de Tecnologia da Informação - Redes-Segurança-Conectividade

Instrumento que define as normas a serem aplicadas na empresa e praticadas por seus funcionários, colaboradores, prestadores de serviço, clientes e fornecedores, com o objetivo de preservar os ativos de informação livres de risco, assegurando a continuidade dos negócios. É a definição de:

A. Gestão de Tecnologia da Informação.

B. Infraestrutura de Tecnologia da Informação.

C. Informação.

D. Política de Segurança da Informação.

E. Gerência de Relacionamento de Clientes.

Questão 16

Com o crescimento da internet e o uso de dispositivos móveis nas empresas é inevitável a ocorrência de problemas de segurança, é preciso muito planejamento e muito trabalho da equipe de TI para ligar com tudo isso. É importante criar normas rígidas e principalmente treinar toda a equipe interna e externa.
A NBR ISO/IEC 27005 define risco como a combinação das consequências advindas da ocorrência de um determinado evento indesejado com a probabilidade de ocorrência desse mesmo evento. A análise e a avaliação de riscos capacitam os gestores a priorizar os riscos. De acordo com essa norma, a atividade de análise de riscos inclui:

A. a avaliação e o tratamento de riscos.

B. a estimativa e o tratamento de riscos.

C. a comunicação e a avaliação de riscos.

D. o tratamento e a aceitação de riscos.

E. a identificação e a estimativa de riscos.