Questão 1

Em desenvolvimento de software seguro, para maior proteção dos acessos, é conveniente que o procedimento de log-on divulgue o mínimo de informações sobre o sistema, não fornecendo, assim, informações detalhadas a um usuário não autorizado.
A partir do contexto apresentado, analise as afirmativas I, II e III e assinale a alternativa que identifica de forma correta, procedimentos para um log-on eficiente:
I - Não ocultar senhas que estão sendo digitadas.
II - Não transmitir senhas com textos claros.
III - Mostrar um aviso de que a aplicação só pode ser acessada por pessoas autorizadas.

A. ○ Somente a afirmativa II está correta.

B. ○ Somente a afirmativa I está correta.

C. ● **Somente as afirmativas II e III estão corretas.**

D. ○ Somente a afirmativa III está correta.

Questão 2

Ano: 2020 Banca: IDECAN Órgão: IF-RR Prova: IDECAN - 2020 - IF-RR - Informática
A Internet promove uma série de facilidades, e o estilo de vida moderno passa pela sua utilização. Existe uma série de ataques que podem comprometer a segurança e a disponibilidade da informação que acontecem através da Internet. Um desses ataques consiste em inundar uma máquina com requisições falsas a um serviço, consumindo os recursos dessa máquina (processamento, memória e espaço em disco, etc.), provocando a interrupção do serviço. Marque a opção que indica o ataque descrito.

A. ○ Falsificação de e-mail (E-mail spoofing)

B. ○ Interceptação de tráfego (Sniffing)

C. ○ Força bruta (Brute force)

D. ○ Varredura em redes (Scan)

E. ● **Negação de serviço (DoS)**

Questão 3

Foi um termo originalmente criado para descrever o tipo de fraude que se dá através do envio, pela Internet, de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir o acesso a páginas fraudulentas (falsificadas), projetadas para furtar dados pessoais e financeiros de usuários.
O ataque definido é conhecido como:

A. DoS.

B. *Flood.*

C. *Botnet.*

D. ***Phishing.***

E. *Spoofing.*

Questão 4

Entre os controles que convêm ser realizados prioritariamente com o objetivo de proteger a integridade do software e da informação contra códigos maliciosos e códigos móveis no gerenciamento das operações de TI e das comunicações em uma empresa, inclui-se a ação de:

A. evitar a instalação de novos patches para não introduzir modificações no ambiente

B. **realizar procedimentos para a conscientização dos usuários contra métodos de engenharia social.**

C. colocar informações do sistema de emergência em local central na rede como endereços IP e regras para o firewall

D. garantir que a segurança da informação seja uma atividade restrita à área de TI.

E. estabelecer acordos de níveis de operação para responder a ameaças e vulnerabilidades na rede com eficiência.

Questão 5

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.
Possuímos diversas propriedades fundamentais na segurança da informação Qual delas NÃO é baseada em métodos de criptografia?

A. Irretratabilidade.

B. Integridade.

C. **Disponibilidade.**

D. Autenticidade.

E. Confidencialidade.

Questão 6

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.
De um modo geral, a manutenção da segurança dos ativos de informação deve cuidar da preservação da:

A. confidencialidade e disponibilidade, somente.

B. integridade, somente.

C. **confidencialidade, integridade e disponibilidade.**

D. confidencialidade e integridade, somente.

E. confidencialidade, somente.

Questão 7

Há diversas alternativas e elas refletem diretamente em como a segurança e privacidade deve ser tratada por sua empresa, principalmente quanto às responsabilidades.
_____que realiza os testes de segurança de uma forma interativada um teste de segurança conhecido como, combinando os testes estáticos e dinâmicos.
O que preenche corretamente a coluna é:

A. LDST ou Lógica dinâmica

B. SAST ou Análise estática

C. **IAST ou Forma interativa**

D. LAST ou Lógica estática

E. DAST ou Análise dinâmica

Questão 8

Conforme os padrões internacionais (ISO/IEC 17799) a Segurança da Informação possui atributos básicos associados a ela.
A propriedade que garante que a informação seja proveniente da fonte anunciada e que não seja alvo de mutações ao longo de um processo é a:

A. Repudio.

B. Integridade.

C. **Autenticidade.**

D. Disponibilidade.

E. Confidencialidade.

Questão 9

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 I

B. ● **I, II e III**

C. ○ Apenas I e II

D. ○ Apenas I e III

Questão 10

O objetivo e o escopo da auditoria podem estar relacionados com a conformidade com normas, padrões, frameworks, leis e requisitos de negócios.
Analise as técnicas e ferramentas que envolvem interação com pessoas, então assinale o que preenche corretamente a lacuna (BENETON, 2017) (ISACA, 2016) (ISACA, 2017) (KAMAL, 2020) (LIMA, 2020):
_____formulários a serem respondidos pelos profissionais de áreas-chave.

A. ○ **Pesquisas**

B. ○ **Entrevistas**

C. ○ **Dinâmicas em grupo**

D. ○ **Perguntas e observação**

E. ● **Questionários**

Questão 11

A gestão de riscos identifica, analisa, avalia, comunica e trata os riscos em um contexto determinado. _____tem como objetivo verificar e validar atividades, processos e sistemas das empresas de acordo com o que está estabelecido, incluindo aspectos legais e regulatórios, visando também a eficiência e eficácia.

A. **Controles de segurança** (selecionado)

B. Controladoria

C. Auditoria

D. Controles lógicos

E. Controles físicos

Questão 12

Os controles têm objetivos diversos, como para o processo de aquisição, desenvolvimento e manutenção de sistemas, ou para o controle de acesso lógico e físico.
Quando nos referimos esses controles, o que completa corretamente a lacuna é:
Os controles _____ tem como exemplo o monitoramento de circuito fechado de TV.

A. Processuais

B. Lógicos

C. Físicos (selecionado)

D. Laboratoriais

E. Tecnológicos

Questão 13

Há diversas alternativas e elas refletem diretamente em como a segurança e privacidade deve ser tratada por sua empresa, principalmente quanto às responsabilidades.
_____deve ser aplicado no código-fonte, e é importante para remover as vulnerabilidades do código antes do software entrar em produção.
O que preenche corretamente a coluna é:

A. **SAST ou Análise estática**
B. IAST ou Forma interativa
C. LDST ou Lógica Dinâmica
D. LAST ou Lógica estática
E. DAST ou Análise dinâmica

Questão 14

A forma de executar a auditoria é importante, com o uso das técnicas e ferramentas mais adequadas para cada objetivo.
Analise as afirmativas sobre as técnicas de auditoria e assinale a alternativa correta:
I. Podem ir de entrevistas a testes técnicos
II. Com o uso de ferramentas para análise de logs e
III. Até mesmo de código-fonte.
Estão corretas as afirmativas:

A. **I, II e III**
B. Apenas I e II
C. Apenas I e III
D. Apenas II e III
E. Apenas I

Questão 15

O avanço dos ataques cibernéticos, que vitimam indivíduos, empresas e países, é motivado por uma série de fatores que tornam ainda mais desafiador o trabalho do profissional de segurança da informação.
Ano: 2017 Banca: CIEE Órgão: TJ-DFT Prova: CIEE - 2017 - TJ-DFT - (adaptada)
É um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate para restabelecer o acesso.

A. ○ **Cavalo de Troia**

B. ○ ***DDOS***

C. ○ ***Cookie***

D. ◉ ***Ransonware***

E. ○ ***Spam***

Questão 16

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. ○ F, F, V, V.

B. ◉ **V, F, V, F.**