REVISÃO II

1. Dada a natureza crítica dos dados em um hospital, onde a integridade e a confidencialidade são vitais, a auditoria de sistemas desempenha um papel crucial. Qual é o principal objetivo da auditoria de sistemas em tal ambiente?

   a) Maximizar a eficiência operacional

   b) Assegurar a conformidade com as políticas de segurança da informação

   c) Reduzir custos através da automação

   d) Promover o uso de tecnologias emergentes

2. Em uma instituição financeira, a gestão de riscos de TI é uma prioridade para proteger contra perdas financeiras e preservar a confiança do cliente. Que tipo de auditoria é especialmente importante em instituições financeiras para assegurar visões externas objetivas?

   a) Auditoria Interna

   b) Autoauditoria

   c) Auditoria Externa

   d) Auditoria Informal

3. Uma empresa de software desenvolve produtos com alto risco de vulnerabilidades de segurança devido à complexidade do código. Quais etapas da auditoria são cruciais para identificar e mitigar essas vulnerabilidades antes que elas afetem os clientes?

   a) Planejamento e Acompanhamento

   b) Execução e Relatório

   c) Relatório e Planejamento

   d) Acompanhamento e Execução

4. Na era digital, as ameaças à segurança cibernética estão em constante evolução, exigindo que as empresas se adaptem rapidamente. Qual é a diferença fundamental entre vírus e worms?

   a) Worms precisam de interação humana para se espalhar.

   b) Vírus replicam-se automaticamente sem intervenção humana.

   c) Worms não podem transportar payloads.

   d) Vírus precisam de interação humana para se espalhar.

5. O phishing continua sendo uma ameaça significativa devido à sua evolução e à sofisticação crescente. Como as organizações podem efetivamente prevenir ataques de phishing?

   a) Limitando o acesso à internet

   b) Educando os funcionários sobre segurança

   c) Usando apenas software licenciado

d) Proibindo o uso de emails

6. A engenharia social explora as fraquezas humanas para acessar sistemas protegidos. Qual técnica de engenharia social é especialmente focada em executivos de alto nível?

   a) Pharming

   b) Baiting

   c) Whaling

   d) Spear Phishing

7. Ransomware é um tipo de malware que criptografa dados críticos e exige resgate para sua liberação. Como o ransomware moderno utiliza IA para aprimorar seus ataques?

   a) Priorizando dados críticos automaticamente

   b) Corrompendo bancos de dados de IA

   c) Criando cópias de segurança falsas

   d) Enviando alertas falsos de segurança

8. Com a crescente integração das cadeias de suprimentos globais, as vulnerabilidades podem ter ramificações extensas. Que tipo de ataque cibernético explora especificamente as cadeias de suprimento?

   a) Ataques de negação de serviço

   b) Infiltração de malware em atualizações de software

   c) Ataques via dispositivos IoT comprometidos

   d) Phishing direcionado a fornecedores

9. Na segurança de TI, é crucial diferenciar ameaças humanas de não humanas para desenvolver estratégias de mitigação eficazes. O que caracteriza uma ameaça não humana?

   a) Phishing por funcionários descontentes

   b) Desastres naturais como inundações e terremotos

   c) Ataques deliberados de hackers

   d) Erros de programação em software

10. A privacidade dos dados tornou-se uma preocupação central com o aumento do volume de dados pessoais processados online. Qual regulamento procura proteger a privacidade dos dados na União Europeia?

    a) COPPA

    b) GDPR

    c) CCPA

    d) PIPEDA

11. O aumento dos ataques de negação de serviço (DoS) requer que as organizações reforcem suas medidas de mitigação. Qual estratégia é eficaz na mitigação de ataques DDoS?

    a) Uso de firewalls básicos

    b) Implementação de redes de distribuição de conteúdo (CDN)

    c) Restrições estritas de senha

    d) Vigilância constante manual

12. Manter a integridade dos sistemas de informação exige uma compreensão clara dos riscos associados. O que descreve melhor uma "vulnerabilidade" em segurança da informação?

    a) Um ataque que pode resultar em perda de dados

    b) Uma fraqueza que pode ser explorada por uma ameaça

    c) Uma política de segurança eficaz

    d) Um software sem atualizações de segurança

13. A proteção de servidores é fundamental para manter a integridade e disponibilidade dos serviços de TI. Que tipo de servidor é primariamente usado para armazenar e gerenciar grandes volumes de dados?

    a) Servidor Web b) Servidor de Email c) Servidor de Arquivos d) Servidor de Banco de Dados

14. A adoção de tecnologia na nuvem trouxe novos desafios de segurança para as organizações. Qual é um desafio específico de segurança enfrentado em ambientes de nuvem?

    a) Manutenção de hardware físico

    b) Detecção de acessos não autorizados

    c) Instalação de software local

    d) Gestão de energia eficiente

15. A conscientização em segurança é crucial para prevenir incidentes e fortalecer a cultura de segurança de uma organização. Qual é o papel principal da educação e conscientização em segurança?

    a) Treinar funcionários sobre práticas seguras e reconhecimento de ameaças

    b) Instalar softwares de segurança

    c) Monitorar o tráfego de rede

    d) Criar políticas de segurança complexas