

Exercícios de Fixação Aulas 4 a 8

A decorative graphic consisting of several horizontal lines of varying lengths and colors (teal, light blue, and white) extending across the width of the slide.

Exercícios de Fixação - PSI

1. Dentre as opções abaixo, qual deles NÃO é um desafio para a implantação da política de segurança?

- A. Falta de profissionais capacitados
- B. Escopo muito abrangente
- C. Falta de conscientização dos funcionários
- D. **Orçamento liberado**

2. Como podemos definir a PSI (Política de Segurança da Informação)?

- A. Norma definida pela ISO para boas práticas em SI
- B. Conjunto de leis, normas, regras e procedimentos para a manutenção da SI na empresa**
- C. Conjunto de regras que trata exclusivamente do controle de acesso físico do data center
- D. Lei americana voltada para o mercado financeiro

3. Sobre a PSI, é correto afirmar que:

- A. É fácil de implantar em qualquer empresa
- B. Não depende em absolutamente nada dos usuários
- C. **Deve ser elaborada e colocada em prática antes de os problemas ocorrerem**
- D. Uma PSI pode ser usada em qualquer empresa, não havendo necessidade nenhuma de criar algo de acordo com o cenário da empresa

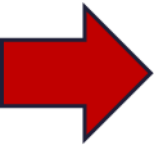
4. Qual camada da organização irá discutir e tomar decisões sobre diretrizes estratégicas e de negócio?

- A. Estratégica**
- B. Tática
- C. Operacional
- D. Braçal

Exercícios de Fixação - Classificação da informação/ Arquiteturas e Modelos de Segurança da Informação

1. Quem atribui os níveis de segurança que a informação demanda, classificando a mesma e definindo seus requisitos de proteção?

A. Custodiante da informação

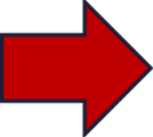


B. Usuário da informação

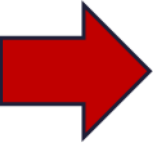
C. Proprietário da informação

D. Gestor da informação

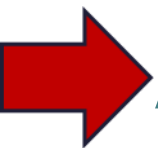
2. Com relação ao ciclo de vida de uma informação, qual é a etapa que a informação deixa um local e vai para outro (deixa seu local original)?

- A. Manuseio (informação manipulada)
- B. Armazenamento (informação guardada)
-  C. Transporte (informação enviada)
- D. Descarte (informação não será mais usada)

3. Quando pensamos em Segurança da Informação, seus pilares baseiam-se no CIDAL (confidencialidade, integridade, disponibilidade, autenticidade e legalidade). Como podemos definir o item integridade?

- A. Garantir que só pessoas autorizadas terão acesso a informação, garantindo a privacidade da informação
-  B. Garantir que as informações não serão alteradas de seu formato inicial, estando protegida contra alterações indevidas
- C. Garantir que a informação está disponível aos usuários quando essa for necessária na execução de suas tarefas
- D. Garantir que as normas da empresa e leis serão cumpridas
- E. Garantir que os usuários que estão acessando são de fato eles mesmos, validando o acesso

4. Quando pensamos na classificação das informações de uma empresa, qual rótulo de informação usado na classificação das informações diz respeito a informações cuja perda ou acesso por pessoas não autorizadas pode significar a paralisação dos processos da empresa?



A. Secreta

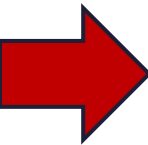
B. Confidencial

C. Restrita

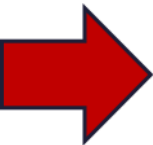
D. Interna

E. Pública

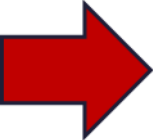
5. Qual é a essência da arquitetura de segurança?

- A. É uma coleção de medidas técnicas para proteger sistemas de ataques cibernéticos.
-  B. É uma coletânea de conceitos, processos e modelos de segurança que equilibram oportunidades e ameaças.
- C. É uma estratégia que busca eliminar completamente os riscos de segurança.
- D. É um plano que prioriza os objetivos financeiros da empresa em detrimento da segurança cibernética.

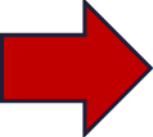
6. O que um arquiteto de segurança faz para criar uma estratégia adaptada aos objetivos da empresa?

- A. Ele implementa medidas de segurança padrão sem considerar os objetivos da empresa.
- B. Ele trabalha exclusivamente com a equipe de TI para definir os requisitos de segurança.
-  C. Ele fala com executivos, funcionários e outros para entender os objetivos da empresa e cria uma estratégia adaptada a esses objetivos.
- D. Ele foca apenas na mitigação de riscos sem considerar os objetivos de benefício da empresa.

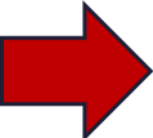
7. O que significa "Security By Default" no contexto do modelo SBSA (Security By Design, Security By Default, Security By Deployment, Security By Operation)?

- A. Refere-se a adicionar medidas de segurança após o desenvolvimento do sistema.
-  B. Significa que as configurações padrão de um sistema são seguras por natureza.
- C. É a fase de implantação do sistema em diferentes ambientes.
- D. Envolve a manutenção de medidas de segurança durante a operação contínua do sistema.

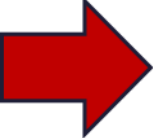
8. Qual é o principal objetivo do modelo SBSA em relação à segurança de sistemas e aplicativos?

- A. Priorizar a eficiência operacional em detrimento da segurança.
- B. Garantir que as medidas de segurança sejam adicionadas após o desenvolvimento do sistema.
-  C. Integrar a segurança em todos os estágios do ciclo de vida de um sistema ou aplicativo.
- D. Focar exclusivamente na detecção de ameaças cibernéticas após a implantação do sistema.

9. Qual é o objetivo principal do gerenciamento de riscos de segurança da informação?

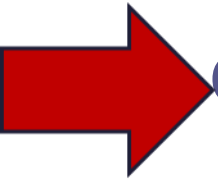
- A. Eliminar todos os riscos possíveis para garantir a segurança completa dos recursos de uma organização.
-  B. Reconhecer, analisar e responder a ameaças para proteger a confidencialidade, integridade e disponibilidade dos recursos da organização.
- C. Garantir que a arquitetura de segurança seja suficiente para proteger contra todas as ameaças possíveis.
- D. Ignorar os riscos e focar apenas nos objetivos empresariais, independentemente das incertezas.

10. Qual é a principal vantagem da implementação de um SGSI (Sistema de Gestão da Segurança da Informação)?

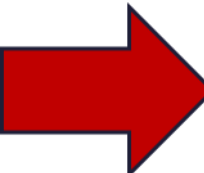
- A. Aumento da eficiência operacional da empresa.
-  B. Redução das violações de segurança.
- C. Maior compartilhamento de vulnerabilidades comuns.
- D. Priorização do desenvolvimento de estratégias de ataque.

Exercícios de Fixação – Segurança Física

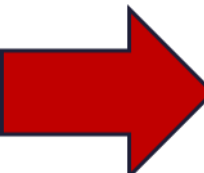
1. Sobre a segurança física, qual alternativa abaixo está correta?

- A. O piso elevado é um software modular, montada sobre uma estrutura de sistema, usado para organizar as aplicações.
- B. O piso elevado é um equipamento de placas modulares removíveis, sobre uma estrutura lógica, usado para organizar os encanamentos.
-  C. O piso elevado é um sistema de placas modulares removíveis, montada sobre uma estrutura, e deve ser usado para organizar e proteger fios e suportar equipamentos pesados sem vibração.
- D. O piso elevado é um sistema SO, para montar uma estrutura física, usado para organizar as aplicações.
- E. O piso elevado é um servidor de placas modulares, montada sobre uma área da rede.

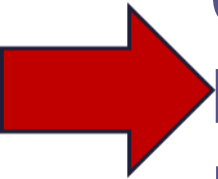
2. Considerando que o local onde estão os equipamentos de TI deve ser implantado em uma área que esteja livre de fatores de riscos físicos, qual opção abaixo deve ser evitada?

- A. Salas com piso elevado, cabeamento estruturado e aterramento.
-  B. Depósito de materiais combustíveis, proximidade de antenas de TV, tubulações de água e esgoto ou outros tipos de líquidos inflamáveis.
- C. Vizinhanças com escolas, supermercados, feiras e hospitais.
- D. Ambientes com gerador e nobreak.
- E. Ambiente com sistema que impeça pessoas não autorizadas de entrarem no ambiente além de câmeras de vigilância, seguranças e sistema de identificação.

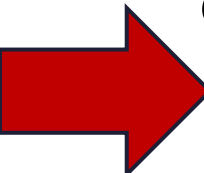
3. O emprego de controles apropriados para o acesso físico de pessoas a ambientes seguros de processamento de informações tem como principal finalidade:


- A. Organizar a emissão de identidades funcionais permanentes e credenciais temporárias para o público externo.
- B. Criar um banco de dados de clientes, com foco em relacionamento corporativo.
-  C. Assegurar que somente pessoas autorizadas tenham acesso permitido.
- D. Viabilizar e acelerar o acesso de fornecedores e prestadores de serviços em emergências.
- E. Estabelecer um histórico de todos os acessos, para fins logísticos e estatísticos.

4. É uma característica da Camada Física de Segurança da Informação:

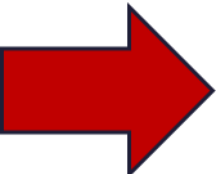
- A. Firewall para filtrar as informações que entram e saem.
- B. Sistema para detectar intrusão nos sistemas.
- C. Não instalar, nos computadores, programas suspeitos.
-  D. Controle de acesso a visitantes.
- E. Instalar e atualizar, constantemente, o sistema de firewall pessoal e de antivírus

5. Dentro de uma empresa existem diversos ativos envolvidos, tais como pessoas, materiais, pesquisas, equipamentos e informações sensíveis ou estratégicas. A segurança vai além do conceito restritivo de patrimônio considerado apenas como bens móveis e imóveis. Considerando o conceito amplo utilizado em segurança, um ativo: I. é todo e qualquer item que possa ser economicamente considerado, ao qual possa ser associada uma ideia de valor, ainda que minimamente expressivo; / II. é apenas um bem tangível; / III. é apenas um bem intangível. Dos itens, verifica-se que está(ão) correto(s) apenas:

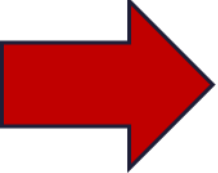
- 
- A. I.**
 - B. II.**
 - C. III.**
 - D. I e II.**
 - E. I e III.**


6. Qual é o objetivo principal da implementação de perímetros de proteção em segurança física e patrimonial?
- A. Isolar completamente os ativos patrimoniais, impedindo qualquer acesso externo.
 - B. Padronizar os controles de segurança em todos os perímetros, independentemente das necessidades.
 -  C. Adaptar os controles de segurança com maior rigor às áreas onde são mais necessários.
 - D. Reduzir a necessidade de segurança em todos os perímetros para economizar recursos.
 - E. Fornecer acesso livre a todas as áreas, eliminando a necessidade de controles de segurança.

7. Qual das seguintes classificações representa uma redundância completa em um Data Center?

- A. Data Center "N"
- B. Data Center "N+1"
- C. Data Center "N+2"
-  D. Data Center "2N"
- E. Data Center "2(N+1)"

8. Qual das seguintes afirmações sobre sistemas de tolerância a falhas está correta?

- A. Os sistemas de tolerância a falhas são projetados para evitar completamente todas as falhas em um sistema.
-  B. A redundância é um componente-chave dos sistemas de tolerância a falhas, permitindo a continuidade das operações mesmo após uma falha.
- C. Os sistemas de tolerância a falhas não são relevantes em ambientes de missão crítica.
- D. Apenas os componentes de hardware são importantes na implementação de sistemas de tolerância a falhas.
- E. Os sistemas de tolerância a falhas não têm impacto na disponibilidade do sistema.

- 9. Qual das seguintes afirmações sobre SLA (Service Level Agreement) está correta?**
- A. SLA é um software usado para monitorar o desempenho dos servidores em uma rede.
 - B. SLA é um padrão de segurança utilizado em criptografia de dados.
 -  C. SLA é um acordo formal que define os níveis de serviço esperados e as responsabilidades entre um provedor de serviço e um cliente.
 - D. SLA é um protocolo de comunicação utilizado para controlar o acesso à internet.
 - E. SLA é uma técnica de recuperação de desastres usada para recuperar dados perdidos em caso de falhas no sistema.

10. Conforme as diretrizes para a implementação do Perímetro de Segurança Física e do Ambiente, é apropriado que:

- I - os perímetros de segurança sejam claramente definidos.
- II - sejam construídas barreiras físicas, onde aplicável, para impedir o acesso físico não autorizado e a contaminação do ambiente.
- III - as instalações de processamento da informação gerenciadas pela organização fiquem fisicamente juntas daquelas que são gerenciadas por terceiros.

▫ Quais estão corretas?

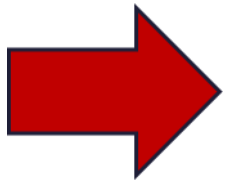
A. Apenas I.

B. Apenas II.


C. Apenas III.

D. Apenas I e II

E. Apenas II e III.



Exercícios de Fixação – Segurança Lógica e Biometria

1. Quais são os componentes básicos envolvidos quando se deseja fazer a verificação do usuário por meio de biometria?
- A. A característica biométrica do usuário e o sensor biométrico
 - B. A característica biométrica do usuário, um computador qualquer e o software que analisa a característica biométrica
 - C. Apenas a impressão digital do usuário
 -  D. Sensor biométrico, dispositivo para ler e armazenar a característica biométrica e o software que analisa a característica biométrica
 - E. NDA - nenhuma das alternativas.

2. Qual dos seguintes itens não é um componente típico de medidas de segurança lógica no âmbito de segurança da informação?

A. Antivírus e antimalware.

B. Firewall.

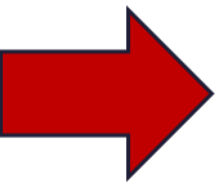
 C. Vigilância por vídeo.

D. Autenticação de dois fatores.

E. Criptografia de dados.

3. Considere os seguintes controles da política de segurança estabelecida em uma empresa:

- I. Controlar o acesso de pessoas às áreas em que se encontram os servidores computacionais da empresa.
 - II. Bloquear acesso dos funcionários para sites inseguros da internet.
 - III. Instalar Firewall para controlar os acessos externos para a rede local da empresa.
- ▣ Os controles mencionados são, respectivamente, tipificados como de Segurança:



- A. Física, Lógica e Lógica.
- B. Lógica, Lógica e Lógica.
- C. Física, Lógica e Física.
- D. Lógica, Lógica e Física.
- E. Física, Física e Lógica.

4. Quais são os passos da segurança lógica (itens que ajudarão a fechar esse processo)?

A. Identificação biométrica e liberação de acesso

 B. Identificação, autenticação, autorização e auditoria

C. Biometria por impressão digital, biometria por voz e biometria dos olhos

D. Uso de senhas fortes e com vários caracteres

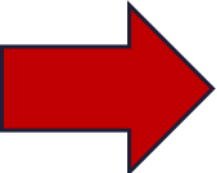
E. NDA – nenhuma das alternativas

5. Quando pensamos em senhas fortes, qual das alternativas abaixo está correta?

A. User: johndoe senha: love1234

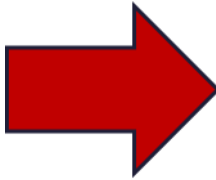
B. User: johndoe senha: asdfg

C. User: johndoe senha: johndoe

 D. User: johndoe senha: O98w&%Lock68

E. User: johndoe senha: 123456789

6. Uma empresa resolveu limitar o acesso às suas dependências por meio de portas com dispositivos biométricos. Havia quatro tipos de equipamentos com tecnologias de biometria no mercado, a saber: retina, impressão digital, assinatura e íris. A primeira providência do gerente foi ordenar os tipos por seus potenciais de precisão, do mais preciso para o menos preciso. Considerando-se a precisão de cada tipo de tecnologia, como essas quatro tecnologias seriam ordenadas, da mais precisa para a menos precisa?

- A. Retina, impressão digital, assinatura e íris
-  B. Retina, íris, impressão digital e assinatura
- C. Íris, retina, impressão digital e assinatura
- D. Assinatura, retina, impressão digital e íris
- E. Impressão digital, íris, retina e assinatura

7. Os dispositivos e sistemas de reconhecimento de impressão digital capturam o padrão único de linhas de dedos. Existem diversas características pessoais encontradas na impressão digital, EXCETO:

A. Bifurcações.

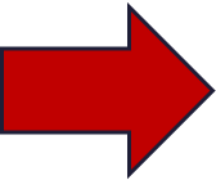
B. Centro.

 C. Curvatura.

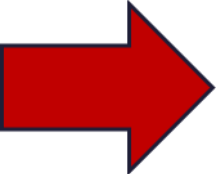
D. Poro.

E. Delta

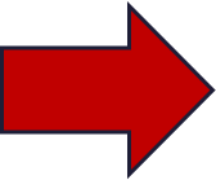
8. A autenticação de usuários para acesso restrito aos sistemas de informações pode ser feita pelo uso de senhas, tokens e sistemas biométricos. Os tokens são:

- 
- A.** Objetos que o usuário possui, que o diferencia das demais pessoas e o habilita a um determinado acesso.
 - B.** Sistemas automáticos de verificação de identidade baseados em características físicas do usuário.
 - C.** Senhas fortes bem definidas e cartões inteligentes com microprocessadores como os bancários, telefônicos e de crédito.
 - D.** Sistemas mais seguros do que os biométricos, que suprem as deficiências de segurança dos dados biométricos.
 - E.** Dispositivos usados para armazenar informações pessoais que auxiliam no processo de autenticação do usuário.

9. Qual dos seguintes fatores é mais importante para aumentar a entropia de uma senha, tornando-a mais segura?

- A. Usar uma senha curta para facilitar a memorização.
- B. Utilizar palavras do dicionário como parte da senha.
-  C. Incluir números, letras maiúsculas e caracteres especiais na senha.
- D. Manter a mesma senha por um longo período de tempo.
- E. Compartilhar a senha com colegas de trabalho para facilitar o acesso a sistemas compartilhados.

10. Qual dos seguintes princípios é fundamental para o controle de acesso lógico em sistemas de TI?

- A. O compartilhamento irrestrito de senhas entre colegas de trabalho.
- B. A concessão de permissões máximas a todos os usuários para facilitar a colaboração.
-  C. O controle de acesso baseado na função do usuário.
- D. A não auditoria das atividades de acesso.
- E. A ausência de autenticação de usuários.

Exercícios de Fixação – Segurança de Redes

1. Qual dos seguintes tipos de malware se espalha automaticamente pela rede, explorando vulnerabilidades em sistemas?

A. Vírus

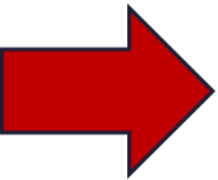
 B. Worms

C. Trojans

D. Programas legítimos

E. Arquivos maliciosos

2. Qual dos seguintes cenários de infecção por malware descreve com precisão um Trojan?

- A. Um arquivo malicioso que se espalha automaticamente pela rede e infecta sistemas explorando vulnerabilidades.
- B. Um programa malicioso que se anexa a arquivos legítimos e se propaga quando esses arquivos são abertos.
-  C. Um malware que se disfarça como um programa legítimo e realiza ações maliciosas quando executado.
- D. Um vírus que se replica rapidamente, causando danos aos dados do sistema.
- E. Um programa legítimo que bloqueia o acesso à internet em um sistema por engano.

3. Qual dos seguintes tipos de ataque envolve a sobrecarga de um sistema alvo com tráfego de rede malicioso, tornando-o inacessível a usuários legítimos?

A. Ataques de Força Bruta

B. Injeção de SQL

C. Exploração de Vulnerabilidades

D. Ransomware

 E. Ataques de Negação de Serviço (DDoS)

4. Qual dos seguintes ataques envolve a interceptação de comunicações entre duas partes, muitas vezes para espionagem ou manipulação de dados?

A. Ataques de Força Bruta

B. Ransomware

C. Ataques de Negação de Serviço (DDoS)

 D. Ataques de Man-in-the-Middle (MitM)

E. Exploração de Vulnerabilidades

5. Qual tipo de ataque envolve tentativas repetidas e automatizadas de adivinhar senhas ou chaves de criptografia até que a combinação correta seja encontrada?

A. Ataques de Negação de Serviço (DDoS)

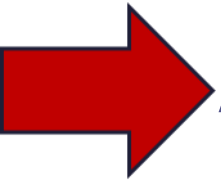
B. Injeção de SQL

 C. Ataques de Força Bruta

D. Ransomware

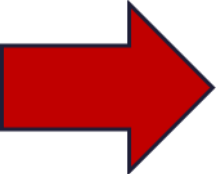
E. Ataques de Man-in-the-Middle (MitM)

6. Qual técnica de ataque envolve a falsificação de endereços IP ou outros identificadores para mascarar a origem de um ataque?



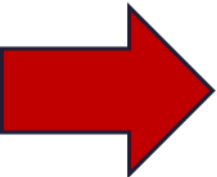
- A. Ataques de Spoofing
- B. Botnets
- C. Ataques de Zero-Day
- D. Ataques a Redes sem Fio (Wi-Fi)
- E. Ataques de Injeção de Código

7. Qual tipo de ataque envolve a inserção de código malicioso em aplicativos ou sites para executar ações não autorizadas?

- A. Ataques a Dispositivos IoT (Internet das Coisas)
- B. Ataques de Engenharia Reversa
-  C. Ataques de Injeção de Código
- D. Ataques a Redes sem Fio (Wi-Fi)
- E. Botnets

8. Qual termo descreve a exploração de vulnerabilidades de software antes que os desenvolvedores tenham a chance de lançar correções?


A. Ataques de Spoofing

 B. Ataques de Zero-Day

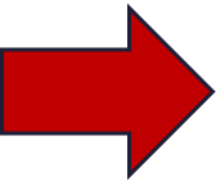
C. Ataques a Dispositivos IoT (Internet das Coisas)

D. Ataques de Engenharia Reversa

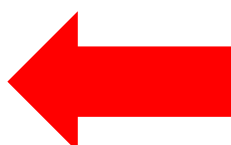
E. Ataques a Redes sem Fio (Wi-Fi)

- 9. Qual é a abordagem recomendada para proteger eficazmente as redes de computadores contra ameaças cibernéticas?**
- A. Implementar apenas firewalls e antivírus para proteger a rede.
 - B. Realizar atualizações regulares de software e não se preocupar com outras medidas de segurança.
 -  C. Adotar uma abordagem em camadas que inclua firewalls, antivírus, atualizações regulares de software, monitoramento de tráfego de rede e treinamento de conscientização para os usuários.
 - D. Depender exclusivamente de treinamento de conscientização para os usuários sem implementar outras medidas de segurança.
 - E. Ignorar a segurança cibernética e confiar na sorte para evitar ameaças.

10. Qual é a definição dos "Ataques de Engenharia Social"?

- A. Ataques que visam redes de computadores por meio de exploração de vulnerabilidades de software.
- B. Ataques que sobrecarregam um sistema alvo com tráfego de rede malicioso.
- C. Ataques que envolvem a falsificação de endereços IP ou outros identificadores.
-  D. Manipulação psicológica de pessoas para obter informações confidenciais ou acesso a sistemas.
- E. Ataques que exploram vulnerabilidades em dispositivos IoT mal protegidos.

Exercícios de Fixação VPN/Seg. Redes Sem Fio

1. Sobre VPN's analise a afirmações a seguir:
 - I - VPNs criptografam todos os dados que você envia pela internet.
 - II - VPN também protege sua privacidade.
 - III - VPNs bloqueiam sites maliciosos, anúncios e trackers.
 - Estão corretas as afirmações:
 - A. I e II, apenas.
 - B. II e III, apenas.
 - C. I e III, apenas.
 - D. I, II e III.
 - E. II, apenas.
- 

2. As VPNs permitem que empresas utilizem redes de comunicação públicas e não confiáveis para trafegar informações de forma segura. O conjunto de protocolos utilizado para configurar conexões VPN e que opera na camada de rede do modelo OSI e provê autenticação em nível da rede, verificação da integridade de dados e transmissão com criptografia é:

A. ATM.

B. PPP.


C. NETBIOS.


D. IPSEC.

E. TLS.



3. A rede de comunicação que é sobreposta às redes públicas, mas apresenta a maioria das propriedades das redes privadas é conhecida pela sigla:

- A. VPN. 
- B. DNS.
- C. DHCP.
- D. FTP.
- E. NNTP.

4. A VPN (Virtual Private Network) é uma rede de comunicação privada que utiliza meios públicos. Com relação à segurança dos dados que trafegam por meio da VPN, afirma-se que:
- A. Muitos dados se perdem pela baixa qualidade dos meios públicos de comunicação, não sendo uma rede adequada para tráfego de aplicações críticas.
 - B. Os dados podem ser acessados por pessoas não autorizadas no caso de serem encapsulados sem criptografia. 
 - C. É uma rede segura de transmissão de dados onde, mesmo utilizando canais públicos de comunicação, usa-se o protocolo padrão da Internet.
 - D. A segurança padrão oferecida pelos gestores da Internet torna viável o tráfego de dados críticos a baixos custos.
 - E. A utilização de soluções de VPN comerciais garante a confidencialidade dos dados e a estabilidade das redes privadas.

5. Sobre os fundamentos de VPN, verifique as assertivas e assinale a correta.

- I. VPN significa Virtual Private Network.
- II. Trata-se de uma conexão de rede protegida, criada para o uso privado em empresas, estabelecida sobre uma infraestrutura de rede pública e compartilhada.
- III. Uma VPN utiliza protocolos de segurança e autenticação para garantir características de uma rede privada e dedicada à corporações que utilizam uma infraestrutura não confiável, como a Internet, para interligação de suas redes ou de usuários remotos a estas.
- IV. Corporações interessadas no uso de VPN devem estar preocupadas com vários aspectos de segurança envolvidos na interligação de suas redes através de uma infraestrutura não confiável.

- A. As assertivas I, II, III e IV são corretas.
- B. Apenas as assertivas I e III são corretas.
- C. Apenas as assertivas III e IV são corretas.
- D. Apenas as assertivas I e II são corretas.
- E. NDA - Nenhuma das alternativas.



6. Você foi designado como responsável por um projeto de uma rede sem fio para visitantes. Um dos pré-requisitos é que essa rede não tenha acesso à rede corporativa. Um outro pré-requisito é referente ao algoritmo de criptografia que deve ser utilizado: o AES. Quais das tecnologias de segurança a seguir atendem aos pré-requisitos?

- WEP e WPA.
- WPA e WPA2.
- WPA2 e WPA3.
- Apenas WPA2.
- Apenas WPA3.



7. Este protocolo de segurança criptografado, cuja tecnologia ficou mais robusta que seu antecessor, protege o tráfego da internet em rede sem fio. Além disso, usa a criptografia AES, que é muito mais forte e resistente a ataques de criptoanálise. Essa descrição refere-se

- WPA.
- WPA2.
- WPA3.
- WEP.
- WEP2.



8. Qual das seguintes afirmações é verdadeira sobre métodos de autenticação em redes Wi-Fi?
- A. PSK é geralmente usado em ambientes empresariais para autenticação de dispositivos usando certificados digitais.
 - B. EAP envolve a configuração de uma senha compartilhada entre dispositivos e o ponto de acesso.
 - C. PSK e EAP são duas siglas diferentes para o mesmo método de autenticação em redes Wi-Fi.
 - D. PSK é mais seguro do que EAP devido ao uso de servidor de autenticação.
 - E. EAP é geralmente usado em ambientes empresariais para autenticação de dispositivos usando certificados digitais.




9. Um recurso disponível em muitos pontos de acesso e que é importante para aumentar a segurança de redes sem fio é a Filtragem de endereços MAC. Com relação a esse recurso são apresentadas as seguintes proposições:

- I. Permite definir quais são os endereços MAC das máquinas autorizadas a se conectar a rede. Desta forma somente os computadores que possuem o endereço MAC da sua placa de rede cadastrado no roteador podem ter acesso à rede sem fio.
- II. A ativação dos recursos de Filtragem por endereço MAC evita a técnica de ataque conhecida como Spoofing.
- III. Para aumentar a segurança da rede sem fio, deve-se combinar a ativação da Filtragem de endereços MAC com a utilização da WEP, para que os endereços MAC dos equipamentos conectados à rede sejam transmitidos criptografados.


• É correto apenas o que se afirma em:

- A. I.
- B. II.
- C. III.
- D. I e II.
- E. I e III.




10. Em um cenário recente, uma grande instituição financeira relatou uma série de incidentes de segurança envolvendo um ataque de Smishing direcionado aos seus clientes. Qual das seguintes afirmações sobre Smishing é verdadeira?
- A. Smishing é uma técnica de ataque que geralmente ocorre apenas por meio de e-mails falsos e não envolve mensagens de texto.
 - B. Smishing é uma técnica de ataque que se concentra apenas em enganar as pessoas por meio de chamadas telefônicas fraudulentas.
 - C. Smishing é uma técnica de ataque que visa principalmente redes sociais e mídias sociais para disseminar informações falsas.
 - D. Smishing é uma técnica de ataque que utiliza mensagens de texto ou SMS para enganar as vítimas e obter informações confidenciais. 
 - E. Smishing refere-se a vírus especificamente projetados para infectar smartphones com sistema operacional Android ou iOS e, com isso, roubar informações do usuário.

Exercícios de Fixação - Sistemas de Proteção em Redes de Computadores

1. “Os dispositivos com reconhecimento de estado não apenas examinam cada pacote, mas também controlam se o pacote faz parte de uma conexão estabelecida ou de outra sessão de rede. Isso oferece mais segurança do que a filtragem de pacotes ou o monitoramento de circuito sozinho, mas tem um impacto maior no desempenho da rede.” A qual tipo de firewall a descrição acima está se referindo?
 - A. Firewall de inspeção estado (Stateful Packet Filter).
 - B. Firewall de última geração (Next-generation firewall).
 - C. Gateway de nível de aplicativo.
 - D. Gateway de nível de circuito (Circuit-level gateway).
 - E. Firewall de filtragem de pacotes (Packet filtering firewall).
- 

2. A empresa XPTO foi contratada para implementar um controle de tráfego dentro na rede interna de uma empresa. Esse processo consiste na instalação de uma solução que possua capacidade de examinar dentro dos pacotes trafegados, além do cabeçalho TCP, de forma a identificar o que a aplicação está executando. A solução permite distinguir entre o tráfego HTTP, usado na navegação Web, e o tráfego HTTP usado para compartilhamento de arquivos P2P (torrent). A solução implementada pela XPTO é:
- A. Firewall filtro de pacotes;
 - B. Proxy implementado como Application Level Gateway;
 - C. Firewall em estado de conexão;
 - D. Zona desmilitarizada (DMZ);
 - E. Virtual Private Network.





3. Uma empresa utiliza a técnica de defesa em profundidade e tem um perímetro de segurança composto por elementos independentes que visam a proteger a rede interna. Diante de um ataque provocado por um verme (worm) que produz uma inundação (*um grande número de dispositivos ou computadores são inundados com tráfego de rede não solicitado e prejudicial*), o componente do perímetro capaz de alertar os administradores da rede sobre esse ataque é a(o):
- A. DMZ
 - B. IDS 
 - C. Firewall Proxy
 - D. Firewall com estado
 - E. Firewall sem estado


4. O firewall do tipo UTM (Unified Threat Manager) permite aumentar a segurança na rede corporativa devido a vários recursos existentes no UTM tais como:

- (1) Prevenção de intrusões (IPS).
- (2) Filtro de conteúdo (Proxy).
- (3) Rede privada virtual (VPN).


▫ Da relação apresentada:


- A. Existem somente o 1 e 2
- B. Existem somente o 1 e 3
- C. Existem somente o 2 e 3
- D. Existem todos 
- E. Não existe nenhum


5. Sobre IDS (Intrusion Detection System ou Sistema de Detecção de Intrusão) e IPS (Intrusion Prevention System ou Sistema de Prevenção de Intrusão), é correto afirmar que:
- A. O IPS é uma solução passiva de segurança.
 - B. O IDS é uma solução ativa de segurança.
 - C. O NIDS (Network IDS ou IDS de Rede) monitora o tráfego da rede, a fim de identificar possíveis atividades maliciosas. 
 - D. O IPS exige que um ser humano, ou outro sistema, analise os resultados e determine quais ações tomar em seguida.
 - E. O UTM (Unified Threat Management ou Gerenciamento Unificado de Ameaças) é uma solução inovadora que não é baseada em IDS e IPS.


6. No contexto de rotinas de proteção e segurança de redes de computadores, HoneyPot é um(a)
- A. Antivírus especializado na detecção e remoção de cavalos de Troia.
 - B. Dispositivo que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.
 - C. Programa que recolhe informações sobre um usuário e as transmite pela Internet, sem o conhecimento e o consentimento desse usuário.
 - D. Mecanismo para proteção de informações sigilosas que usa técnicas de criptografia.
 - E. Ferramenta que simula falhas de segurança em um sistema e colhe informações sobre eventuais invasores.
- 

7. Os mecanismos de segurança da informação proporcionam a implantação de diferentes tipos de controle. Honeypot é exemplo de um recurso que pode implantar segurança por meio de controle:

- A. Interno
- B. Lógico 
- C. Restrito
- D. Biométrico
- E. De assinatura digital


8. Qual das seguintes afirmações sobre VLANs (Redes Locais Virtuais) e segurança de rede é verdadeira?
- A. VLANs não têm impacto na segurança da rede, pois são apenas uma técnica de gerenciamento de tráfego.
 - B. VLANs ajudam a melhorar a segurança da rede, pois segmentam o tráfego em diferentes grupos lógicos, limitando o acesso não autorizado. 
 - C. VLANs são vulneráveis a ataques cibernéticos e, portanto, não devem ser usadas em ambientes de rede seguros.
 - D. VLANs são usadas exclusivamente para criar redes isoladas fisicamente, o que não afeta a segurança da rede.
 - E. VLANs não têm relação com a segurança da rede; essa é uma função exclusiva dos firewalls e antivírus.

9. O que representa uma Zona Desmilitarizada (DMZ) em relação à segurança de rede?
- A. A DMZ é uma área onde os dados confidenciais da rede são armazenados com segurança, protegidos contra acesso não autorizado.
 - B. A DMZ é uma técnica que isola completamente a rede interna de qualquer tráfego externo, tornando-a altamente segura.
 - C. A DMZ é uma parte da rede que atua como uma camada intermediária entre a rede interna e a Internet pública, onde os servidores públicos são colocados, expondo-os a ameaças externas. 
 - D. A DMZ é uma abordagem que exclui completamente a necessidade de firewalls e outras medidas de segurança, tornando a rede mais eficiente.
 - E. A DMZ é uma configuração que não afeta a segurança da rede de forma alguma, mas apenas aumenta a velocidade da conexão com a Internet.


10. Qual dos seguintes princípios é um elemento fundamental para garantir a segurança eficaz de uma rede de computadores?
- A. Ignorar atualizações de software para evitar possíveis interrupções na rede.
 - B. Compartilhar senhas de administrador com frequência para facilitar o acesso aos recursos da rede.
 - C. Permitir o tráfego de entrada indiscriminadamente, sem filtros ou firewalls.
 - D. Implementar políticas de acesso e autenticação rigorosas para controlar quem pode acessar recursos da rede. 
 - E. Deixar todos os dispositivos de rede com configurações padrão de fábrica para simplificar a manutenção.

Exercícios de Fixação - Criptografia

1. Sobre a criptografia simétrica, podemos afirmar que:

- A. O emissor usa uma chave e o receptor outra
- B. É altamente seguro
- C. Não precisa de um algoritmo criptográfico
-  D. O emissor e o receptor da mensagem usam a mesma chave
- E. NDA – nenhuma das alternativas

2. Como podemos definir os ataques por força bruta?

- 
- A. Uma pessoa mal intencionada tenta todas as chaves possíveis, até encontrar a chave que decodifica a mensagem
 - B. Uma pessoa mal intencionada procura vulnerabilidades no algoritmo de criptografia
 - C. Uma pessoa mal intencionada decodifica o algoritmo de criptografia manualmente
 - D. Uma pessoa mal intencionada abre a mensagem codificada e vai tentando trocar os caracteres
 - E. NDA – nenhuma das alternativas

3. Qual componente da criptografia simétrica é a saída do processamento do texto legível pelo algoritmo criptográfico?

A. Texto legível

B. Chave secreta

 C. Texto cifrado

D. Algoritmo de criptografia

E. Algoritmo de decifração

4. Qual algoritmo de criptografia simétrica é usado nos padrões SSL (Protocolo de Camada de Sockets Segura - tem a responsabilidade de gerenciar um canal de comunicação seguro entre o cliente e o servidor)?

- AES
- DES
- 3DES
- RC4
- Lucifer




5. Qual conceito é usado na criptografia assimétrica?




- A. Aritmética modular
- B. Chaves públicas
- C. Cifra de Cesar
- D. Chave com poucos bits
- E. Números pares

6. Quando comparamos a criptografia simétrica com a assimétrica, qual das opções abaixo é FALSA?

- A. A criptografia assimétrica é mais segura
-  B. A criptografia simétrica é mais lenta
- C. A criptografia simétrica usa apenas uma chave pública
- D. Na criptografia assimétrica, apenas uma pessoa deve saber a chave privada
- E. NDA – nenhuma das alternativas

7. Qual algoritmo de criptografia assimétrica é baseado na multiplicação de números primos e em aritmética modular?

- 
- RSA
 - Cifra de Cesar
 - Cifra de Vigenère
 - Diffie Hellman
 - NDA – nenhuma das alternativas

8. Podemos definir uma função hash como uma função que provê integridade de uma mensagem gerando um código verificador que mostra se a mensagem foi (ou não) alterada. Essa afirmação está:

- Incorreta

 • Correta

9. Qual função hash produz resultados de 160 bits?

A. SHA-160


B. SHA-320

 C. SHA-1

D. SHA-16

E. NDA – nenhuma das alternativas

10. Esteganografia é um termo pouco utilizado no âmbito da segurança da informação, mas que exige cuidados especiais de quem se preocupa com o tema. Assinale a alternativa que apresenta a definição de esteganografia.

- 
- A.** Técnica de esconder informações dentro de arquivos como imagens, sons, vídeos ou textos.
 - B.** Sinônimo de criptografia, é técnica de codificar a informação para que não seja entendida por terceiros.
 - C.** Algoritmo matemático que converte um texto claro em uma mensagem cifrada, e vice-versa.
 - D.** Estudo de técnicas de quebra de sigilo de mensagens eletrônicas criptografadas.
 - E.** Método para codificação de arquivos binários, transformando-os em texto ASCII.

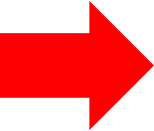
Exercícios de Fixação – Assinatura e Certificação Digital

1. A criptografia nos oferece algumas vantagens, dentre elas a irretratabilidade. O que vem a ser irretratabilidade?


- Impossibilidade de uma mensagem ser alterada
- Impossibilidade de uma pessoa não autorizada ler uma determinada mensagem
- Uso de autenticação para quem ai acessar a mensagem
- Impossibilidade de se negar a autoria de uma mensagem
- NDA – nenhuma das alternativas




2. Em assinatura digital, a função hashing:

- A. utiliza o algoritmo DSA, cuja função é produzir um valor hash de 64 bits para uma mensagem de tamanho arbitrário.
- B. é utilizada para gerar um valor de chave privada, a partir da criptografia simétrica.
-  C. funciona como uma impressão digital de uma mensagem, gerando, a partir de um valor de tamanho fixo, uma chave de tamanho variável.
- D. é utilizada para gerar um valor pequeno, de tamanho fixo, derivado da mensagem que se pretende assinar.
- E. utiliza o algoritmo DES, cuja função de espalhamento unidirecional gera um valor hash de 160 bits.


3. Certificados Digitais podem ser utilizados em um processo de comunicação segura. Esses certificados são expedidos e assinados por um terceiro confiável, denominado Autoridade Certificadora (CA – Certification Authority), o qual confirma a identidade do usuário ou host. O esquema de Certificados Digitais:

- 
- A.** Fornece um conjunto de dados confiável que atesta a associação de uma chave pública a um usuário final.
 - B.** Dispensa o conhecimento do certificado da CA que expediu o certificado do usuário ou host.
 - C.** Dispensa formatos padronizados para os certificados.
 - D.** Impede a revogação de Certificados Digitais anteriormente emitidos.
 - E.** Substitui a criptografia dos dados.

4. A Infraestrutura de Chaves Públicas Brasileira regula a validação de uma assinatura digital ICP-Brasil, realizada sobre um documento eletrônico, com o estabelecimento de alguns critérios. Um desses critérios utiliza resultados hash do documento, que têm como uma de suas finalidades:


- A. Facilitar a criptografia do documento original.
-  B. Assegurar a integridade do conteúdo digital, mostrando que não houve alteração desse conteúdo desde a criação da assinatura digital pelo signatário.
- C. Assegurar a autoria, decifrando a assinatura digital com a chave criptográfica secreta, contida no certificado digital do signatário.
- D. Proporcionar a recuperação do documento original com a aplicação da chave secreta do destinatário sobre o hash.
- E. Proporcionar a recuperação do documento original com a aplicação da chave pública do remetente sobre o hash.

5. Com relação à Infraestrutura de Chaves Públicas brasileira, é correto afirmar que:

- A. A utilização da assinatura digital em um documento tem a vantagem adicional de tornar o seu próprio conteúdo, também ele, sigiloso.
- B. Os certificados utilizam criptografia simétrica.
-  C. Os documentos eletrônicos assinados digitalmente com o uso de certificados emitidos no âmbito da ICP-Brasil têm a mesma validade jurídica que os documentos em papel com assinaturas manuscritas.
- D. A interoperabilidade dentro da ICP-Brasil está concebida de tal forma que o correto funcionamento de um sistema com um certificado da ICP-Brasil pode depender da autoridade certificadora que o tenha emitido.
- E. O certificado digital não possui um prazo de validade, sendo válido até sua revogação por parte do usuário ou da autoridade certificadora.

6. As extensões do certificado digital X.509 podem ser consideradas críticas ou não críticas. Sobre as extensões críticas, qual a alternativa correta?

A. Devem estar criptografadas

 B. Devem ser sempre reconhecidas pelo software de certificação digital

C. Devem ser implementadas com Cifra de Vigenére

D. Não precisam de nenhum reconhecimento desde que estejam no certificado

E. NDA – nenhuma das alternativas

7. Qual extensão do certificado X.509 indica qual é o diretório de consulta com as políticas de certificação associadas ao certificado digital e que foram definidas pela autoridade certificadora?




- A. Certificate policies
- B. Authority key user
- C. Policy mapping
- D. Issuer alternative name
- E. NDA – nenhuma das alternativas

8. Analise as afirmações a seguir:

- I. No cerne da certificação digital está o certificado digital, um documento eletrônico que contém informações que mostram quem somos para as pessoas e para os sistemas de informação.
- II. Depois de emitido, um certificado digital não pode ser revogado, mesmo que a chave privada tenha sido comprometida.
- III. Um exemplo comum do uso de certificados digitais é o serviço bancário provido via Internet.
- IV. A AC (Autoridade Certificadora) é o principal componente de uma infraestrutura de chaves públicas e é responsável pela emissão dos certificados digitais.


• São corretas as afirmações:

- A. I e III, somente;
- B. I e IV, somente;
- C. I, II e III, somente;
-  D. I, III e IV, somente;
- E. I, II, III e IV.


9. Identifique as afirmativas corretas a respeito da Certificação digital.

1. A operação de emissão do certificado envolve duas entidades: Autoridade responsável (AR) e Autoridade correspondente (AC).
2. É um documento eletrônico, assinado digitalmente por uma terceira parte confiável, que associa uma pessoa ou entidade a uma chave pública.
3. Um certificado digital normalmente apresenta as seguintes informações de seu titular: nome da pessoa ou entidade a ser associada à chave pública, período de validade do certificado, chave pública, nome e assinatura da entidade que assinou o certificado e número de série.

- **Assinale a alternativa que indica todas as alternativas corretas.**

- A. É correta apenas a afirmativa 1.
- B. É correta apenas a afirmativa 2.
- C. São corretas apenas as afirmativas 1 e 2.
-  D. São corretas apenas as afirmativas 2 e 3.
- E. São corretas as afirmativas 1, 2 e 3.

10. Que informação, entre outras, é fornecida por um certificado digital?

- A. Assinatura digital do proprietário do certificado.
- B. Assinatura digital da autoridade de registro responsável pela emissão do certificado digital.
-  C. Chave pública do proprietário do certificado.
- D. Chave privada do proprietário do certificado.
- E. Chave de sessão a ser empregada em conexões seguras, como HTTPS.