

CONCURSO PÚBLICO

**COMPANHIA DE PROCESSAMENTO DE DADOS
DO MUNICÍPIO DE PORTO ALEGRE - PROCEMPA**

ANALISTA EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

**Analista de Programação e Suporte de Sistemas Informatizados
e Georreferenciados, Infraestruturas e Redes Computacionais:
Segurança de Dados**

- Confira devidamente o material (CARTÃO DE RESPOSTAS e CADERNO DE QUESTÕES); se houver falha, solicite a substituição ao fiscal.
- Este caderno de questões está assim constituído: **10 questões de Língua Portuguesa e 40 questões de Conhecimentos Específicos.**
- Após conferir seus dados no cartão de respostas (NOME, Nº da INSCRIÇÃO e CARGO), assine no local indicado.

• O CARTÃO DE RESPOSTAS é o único documento de correção, devendo ser preenchido com bastante atenção, à caneta esferográfica, azul ou preta, ponta grossa, marcando uma única alternativa em cada questão. Verifique no cartão de respostas as instruções para preenchimento. Não rasure, não amasse nem dobre o CARTÃO DE RESPOSTAS. É vedada a substituição do CARTÃO DE RESPOSTAS decorrente de erro cometido por candidato.

• ATENÇÃO, MUITO IMPORTANTE! No campo indicado no seu cartão de respostas, FAÇA A MARCAÇÃO DO NÚMERO CORRESPONDENTE AO SEU TIPO DE CADERNO DE PROVA, CONFORME CONSTA NO CANTO SUPERIOR DIREITO DESTA CAPA.

- Durante a realização da prova, não é permitida a comunicação entre candidatos nem a utilização de máquina calculadora e/ou similares, livros, anotações, réguas de cálculo, impressos ou qualquer outro material de consulta.
- O tempo de duração da prova objetiva será de **até 4 horas**, incluído o tempo para preenchimento do Cartão de Respostas. O candidato somente poderá levar consigo seu caderno de provas **após 1 hora** contada do efetivo início das provas. Ao candidato que sair antes de uma hora contada do efetivo início das provas, será permitido copiar seu cartão de respostas, para conferência com o gabarito oficial.
- Em todas as questões de legislação desta prova (se houver), serão consideradas as emendas e/ou alterações da legislação com entrada em vigor até a data do início das inscrições. Na prova de Português será exigida a norma ortográfica atualmente em vigor. Para responder às questões de Informática (se houver), a menos que seja informado o contrário, considerar que os programas mencionados se encontram na versão Português-BR e em sua configuração padrão de instalação, possuem licença de uso, o mouse está configurado para destros, um clique ou duplo clique correspondem ao botão esquerdo do mouse, e teclar corresponde à operação de pressionar uma tecla e, rapidamente, liberá-la, acionando-a apenas uma vez.
- Ao final dos trabalhos, **DEVOLVA** ao Fiscal da sala o CARTÃO DE RESPOSTAS devidamente preenchido e assinado.
- Ao final da prova objetiva, os três últimos candidatos de cada sala de prova deverão permanecer no recinto, a fim de acompanhar os fiscais até a coordenação para o lacre dos envelopes, quando, então, poderão retirar-se do local, simultaneamente, após concluído.

Direitos autorais reservados à Objetiva Concursos Ltda. Proibida a reprodução, ainda que parcial, sem autorização prévia.

Boa Prova!

Seriedade e ética: nós acreditamos nesses valores.

Nome do(a) Candidato(a)

Nº de inscrição

✂ Esta parte destacável serve para copiar as suas respostas, somente poderá ser destacada no ato da entrega do material na mesa do fiscal.

CADERNO DE PROVA TIPO 01

01	☐	02	☐	03	☐	04	☐	05	☐	06	☐	07	☐	08	☐	09	☐	10	☐
11	☐	12	☐	13	☐	14	☐	15	☐	16	☐	17	☐	18	☐	19	☐	20	☐
21	☐	22	☐	23	☐	24	☐	25	☐	26	☐	27	☐	28	☐	29	☐	30	☐
31	☐	32	☐	33	☐	34	☐	35	☐	36	☐	37	☐	38	☐	39	☐	40	☐
41	☐	42	☐	43	☐	44	☐	45	☐	46	☐	47	☐	48	☐	49	☐	50	☐

LÍNGUA PORTUGUESA

Autorretrato inédito de Van Gogh é descoberto atrás de outra pintura do artista

Um autorretrato escondido de Vincent Van Gogh foi descoberto atrás de uma de suas pinturas, coberto por camadas de cola e papelão por mais de um século.

A imagem foi encontrada quando conservadores de arte tiraram um raio-X da pintura “Retrato de Mulher (Cabeça de Camponesa)” de Van Gogh, de 1885, antes de uma exposição futura.

Eles descobriram a imagem escondida na parte de trás de sua tela coberta por uma folha de papelão, de acordo com um comunicado de imprensa das Galerias Nacionais da Escócia (NGS, na sigla em inglês).

Especialistas dizem que a obra de arte revelada era desconhecida até agora. “Momentos como esse são incrivelmente raros”, disse Frances Fowle, curadora sênior de arte francesa do NGS, no comunicado à imprensa. “Descobrimos uma obra desconhecida de Vincent Van Gogh, um dos artistas mais importantes e populares do mundo.”

O mestre holandês costumava reutilizar telas para economizar dinheiro, transformando-as para trabalhar no verso, disse o NGS.

Acredita-se que o autorretrato subjacente tenha sido feito durante um momento chave na carreira de Van Gogh, quando ele foi exposto ao trabalho dos impressionistas franceses depois de se mudar para Paris.

A imagem de raio-X “totalmente convincente” mostra “um assistente barbudo com um chapéu de abas com um lenço frouxamente amarrado na garganta. Ele fixa o espectador com um olhar intenso, o lado direito do rosto na sombra e a orelha esquerda claramente visível”, de acordo com o comunicado.

Embora a condição do autorretrato real seja desconhecida, se puder ser descoberta, espera-se que ajude a lançar uma nova luz sobre o renomado artista.

O processo de remoção da cola e do papelão exigirá um delicado trabalho de conservação. A pesquisa está em andamento sobre como isso pode ser feito sem prejudicar a tela “Retrato de Mulher (Cabeça de Camponesa)”.

A pintura, que mostra uma mulher local da cidade de Nuenen, no sul da Holanda, onde o artista viveu de dezembro de 1883 a novembro de 1885, chegou ao NGS em 1960 como presente de um advogado de Edimburgo.

Foi provavelmente por volta de 1905, quando a tela foi emprestada para uma exposição no Museu Stedelijk, em Amsterdã, que foi tomada a decisão de colar a tela em papelão antes de emoldurar, segundo o comunicado de imprensa.

O NGS acrescentou que, na época, “Retrato de Mulher (Cabeça de Camponesa)” provavelmente era um quadro considerado mais “acabado” do que o autorretrato de Van Gogh.

A pintura mudou de mãos várias vezes até ir para a Escócia em 1951.

A imagem de raio-X pode ser vista publicamente pela primeira vez através de uma caixa de luz especialmente criada quando ocupa o centro do palco na exposição “A Taste for Impressionism” entre 30 de julho e 13 de novembro na *Royal Scottish Academy*, em Edimburgo.

(Fonte: CNN Brasil - adaptado.)

1) Em conformidade com o texto, marcar C para as sentenças Certas, E para as Erradas e, após, assinalar a alternativa que apresenta a sequência CORRETA:

- () A tela foi emprestada para uma exposição no Museu Stedelijk, em Amsterdã, em 1885. Na ocasião, foi tomada a decisão de colar a tela em papelão antes de emoldurar, conforme o comunicado de imprensa.
- () Segundo o comunicado, a imagem de raio-X “totalmente convincente” mostra “um assistente barbudo com um chapéu de abas com um lenço frouxamente amarrado na garganta. Ele fixa o espectador com um olhar intenso, o lado direito do rosto na sombra e a orelha esquerda claramente visível”.
- () De acordo com um comunicado de imprensa das Galerias Nacionais da Escócia, conservadores de arte descobriram a imagem evidente na parte de trás da tela coberta por uma folha de papelão.

- a) C - C - C.
- b) E - C - E.
- c) C - E - E.
- d) E - E - C.
- e) E - C - C.

2) No trecho “Descobrimos uma obra desconhecida de Vincent Van Gogh, um dos artistas mais importantes e populares do mundo.” o verbo destacado é classificado, quanto à transitividade, como:

- a) Bitransitivo.
- b) Transitivo de ligação.
- c) Transitivo nominal.
- d) Transitivo direto.
- e) Transitivo indireto.

3) Em relação aos tempos e modos verbais, analisar os itens abaixo:

- I. No trecho “O processo de remoção da cola e do papelão exigirá um delicado trabalho de conservação.”, o verbo sublinhado está no futuro do presente do modo indicativo.
- II. Em “A pintura mudou de mãos várias vezes até ir para a Escócia em 1951.”, o verbo sublinhado está no pretérito imperfeito do modo indicativo.
- III. No trecho “Especialistas dizem que a obra de arte revelada era desconhecida até agora.”, o verbo sublinhado está no pretérito perfeito do subjuntivo.

Está(ão) CORRETO(S):

- a) Somente o item I.
- b) Somente o item II.
- c) Somente o item III.
- d) Somente os itens I e II.
- e) Todos os itens.

4) No trecho “Autorretrato inédito de Van Gogh é descoberto atrás de outra pintura do artista.”, temos:

- a) Um período misto.
- b) Um período composto.
- c) Uma oração.
- d) Duas orações.
- e) Três orações.

5) O trecho “A pintura, que mostra uma mulher local da cidade de Nuenen, no sul da Holanda, onde o artista viveu de dezembro de 1883 a novembro de 1885, chegou ao NGS em 1960 como presente de um advogado de Edimburgo.” é reescrito, mantendo o sentido original, em:

- a) Chegou ao NGS, de dezembro de 1883 a novembro de 1885, a pintura, que mostra uma mulher local da cidade de Nuenen, no sul da Holanda, onde o artista viveu em 1960 como presente de um advogado de Edimburgo.
- b) Como presente de um advogado de Edimburgo, o artista viveu a pintura, que chegou ao NGS, em 1960. De dezembro de 1883 a novembro de 1885, a pintura mostra uma mulher local da cidade de Nuenen, no sul da Holanda.
- c) Uma mulher local da cidade de Nuenen, no sul da Holanda, onde o artista viveu de dezembro de 1883 a novembro de 1885, mostrou a pintura que chegou ao NGS em 1960, como presente de um advogado de Edimburgo.
- d) Chegou ao NGS, em 1960, como presente de um advogado de Edimburgo, a pintura, que mostra uma mulher local da cidade de Nuenen, no sul da Holanda, onde o artista viveu de dezembro de 1883 a novembro de 1885.
- e) Em 1960, no sul da Holanda, onde o artista viveu de dezembro de 1883 a novembro de 1885, uma mulher local da cidade de Nuenen chegou ao NGS mostrando a pintura, como presente de um advogado de Edimburgo.

6) Em relação à regência verbal, analisar os itens abaixo:

- I. A primavera enfolhou no pessegueiro.
- II. A brisa ondeia com as velas.
- III. Eles colimavam objetivos nobres.

Está(ão) CORRETO(S):

- a) Somente o item I.
- b) Somente o item II.
- c) Somente o item III.
- d) Somente os itens II e III.
- e) Todos os itens.

7) Em relação ao que completa corretamente a frase “Já _____ anos, _____ neste local casarões e praças. Hoje, só _____ prédios.”, assinalar a alternativa CORRETA:

- a) fazem | havia | existem
- b) faz | havia | existem
- c) fazem | havia | existe
- d) faz | havia | existe
- e) fazem | haviam | existe

8) No trecho “Eles descobriram que o crânio pertencia a um indivíduo do sexo feminino, [...]”, a palavra sublinhada é classificada, gramaticalmente, como:

- a) Advérbio.
- b) Adjetivo.
- c) Pronome.
- d) Substantivo.
- e) Preposição.

9) Assinalar a alternativa que apresenta a figura de linguagem chamada pleonasmo:

- a) Não se ouviu mais o tic-tac do relógio.
- b) Aqueles jardins tinham vida e morte.
- c) Não o vejo há séculos.
- d) Anote meu celular.
- e) O país desejava ter um monopólio exclusivo.

10) Em relação ao uso de G ou J, assinalar a alternativa CORRETA:

- a) Majestade | jenipapo | gengiva.
- b) Magestade | herege | fingir.
- c) Genjiva | hereje | longe.
- d) Trage | longe | gengiva.
- e) Tragetória | trage | herege.

CONHECIMENTOS ESPECÍFICOS

11) A Norma ISO 27001 tem como princípio geral a adoção, pela organização, de um conjunto de requisitos, processos e controles, com o objetivo de mitigar e gerir adequadamente o risco da organização. O principal modelo aplicado nos processos do Sistema de Gestão de Segurança da Informação é o:

- a) Plan-Do-Check-Act (PDCA).
- b) Audit-Integrity-confidentiality e privacy (AICP).
- c) Do-Plan-Avaliable-Risc (DPAR).
- d) Risc-PLAN-Available-Check (RPAC).
- e) Management-Do-Check-Audit (MDCA).

12) Um usuário enviou um e-mail com dados bancários para uma pessoa realizar um depósito. Durante a transferência da mensagem, ela foi interceptada e alterada indevidamente, fazendo com que o depósito fosse enviado para outra conta bancária desconhecida. Considerando-se os princípios da segurança da informação, a alteração da informação relatada representa violação do princípio da:

- a) Irretratabilidade.
- b) Autenticidade.
- c) Integridade.
- d) Complexidade.
- e) Confidencialidade.

13) Uma das principais estratégias para assegurar a confidencialidade da informação é realizar um controle de acesso rigoroso. Sendo assim, constitui-se como medida que vai ao encontro dessa estratégia:

- I. Dispensar o uso de algoritmos em função de *hashing*.
- II. Implementar sistemas de verificação biométrica e criptografia.
- III. Proteger o conteúdo com autenticação por senha.

Está(ão) CORRETO(S):

- a) Somente o item I.
- b) Somente o item II.
- c) Somente os itens I e II.
- d) Somente os itens II e III.
- e) Todos os itens.

14) *Malware* é um termo amplo, usado para classificar todo tipo de *software* malicioso cujo objetivo é causar danos ou qualquer tipo de prejuízo ao usuário. Sobre esse tema, marcar C para as afirmativas Certas, E para as Erradas e, após, assinalar a alternativa que apresenta a sequência CORRETA:

- () *Spywares* são usados para roubo de dados, interceptação de informações, sequestro de dados para resgate, bombardeio de anúncios, danos físicos ao sistema, corrupção de dados ou simplesmente irritação.
- () *Ransomwares* capturam o sistema, criptografam seus arquivos e exigem resgate para que se recupere o acesso aos dados.
- () *Malwares* são usados apenas para monitorar comportamento e roubar dados do usuário.

- a) C - C - E.
- b) E - E - C.
- c) E - C - E.
- d) C - E - C.
- e) C - C - C.

15) Considerando-se as características comuns a todas as implementações, em conformidade com o ECMA Script, numerar a 2ª coluna de acordo com a 1ª e, após, assinalar a alternativa que apresenta a sequência CORRETA:

- (1) Suporte universal.
- (2) Imperativa e estruturada.
- (3) Tipagem dinâmica.
- (4) Funções de primeira classe.

- () Todos os navegadores da Web modernos e populares suportam JavaScript com interpretadores integrados.
- () JavaScript suporta os elementos de sintaxe de programação estruturada da linguagem C como, por exemplo, *if*, *while*, *switch*.
- () Como na maioria das linguagens de *script*, tipos são associados com valores, não com variáveis.
- () São objetos que possuem propriedades e métodos, e que podem ser passados como argumentos, atribuídos a variáveis ou retornados, como qualquer outro objeto.

- a) 2 - 3 - 1 - 4.
- b) 1 - 2 - 3 - 4.
- c) 2 - 3 - 4 - 1.
- d) 1 - 3 - 2 - 4.
- e) 4 - 2 - 3 - 1.

16) A Programação Orientada a Objetos (POO) diz respeito a um padrão de desenvolvimento que é seguido por muitas linguagens. Considerando-se que a programação orientada a objetos possui quatro pilares, numerar a 2ª coluna de acordo com a 1ª e, após, assinalar a alternativa que apresenta a sequência CORRETA:

- (1) Abstração.
- (2) Encapsulamento.
- (3) Herança.
- (4) Polimorfismo.

- () Consiste na alteração do funcionamento interno de um método herdado de um objeto pai.
- () É uma das principais técnicas que define a programação orientada a objetos. Trata-se de um dos elementos que adicionam segurança à aplicação em uma POO pelo fato de esconder as propriedades, criando uma espécie de caixa preta.
- () O reuso de código é uma das grandes vantagens da programação orientada a objetos.
- () É a propriedade em virtude da qual apenas os detalhes essenciais são exibidos ao usuário.

- a) 2 - 3 - 1 - 4.
- b) 1 - 2 - 3 - 4.
- c) 2 - 3 - 4 - 1.
- d) 1 - 3 - 2 - 4.
- e) 4 - 2 - 3 - 1.

17) Entre as várias metodologias de auditoria de sistemas (técnicas), assinalar a alternativa que se refere à caracterizada abaixo:

Os dados no processamento de transações reais são confrontados com os dados fictícios e os resultados, comparados com os predeterminados.

- a) Simulação paralela.
- b) Lógica de auditoria embutida nos sistemas.
- c) Rastreamento e mapeamento (*accountability*).
- d) Análise da lógica de programação.
- e) Facilidade de teste integrado (*Integrated Test Facility – ITF*).

18) IPSec é um conjunto de padrões e protocolos para segurança relacionada a uma rede VPN criada sobre uma rede IP, e foi definido pelo grupo de trabalho denominado IP Security do IETF. A respeito do IPSec, é CORRETO afirmar que:

- a) O protocolo ESP (*Encapsulating Security Payload*) negocia parâmetros de conexão, incluindo chaves, para os outros dois protocolos.
- b) Não garante segurança das máquinas que estão na rede; a única coisa que faz é criptografar e garantir a segurança das informações (pacotes encapsulados) que estão passando pelo túnel.
- c) O IPSec especifica os cabeçalhos AH e ESP, que devem ser usados de forma independente, de maneira que um pacote IPSec poderá apresentar somente um dos cabeçalhos (AH ou ESP).
- d) Se em uma extremidade da rede estiver o Linux rodando IPSec, e na outra estiver rodando também o IPSec, o *FreeSwan* não se conectará.
- e) O protocolo IKE (*Internet Key Ex*) oferece serviço de autenticação para o pacote.

19) Tentativas de quebrar a segurança de algoritmos criptográficos irão sempre existir; e, assim como a criação destes algoritmos necessitaram de estudos, os ataques também necessitarão ser planejados. Assinalar a alternativa que apresenta a característica do tipo de ataque *Known-plaintext attack* [Ataque de purotexto-conhecido]:

- a) Nele o adversário aprende um ou mais pares de purotexto/cifrotexto encriptados sob a mesma chave. O objetivo do adversário é determinar o purotexto que foi encriptado para dar algum outro cifrotexto (para o qual ele não sabe o purotexto correspondente).
- b) Refere-se ao cenário em que o adversário apenas observa um cifrotexto e tenta determinar o purotexto que foi encriptado.
- c) Neste ataque, o adversário tem a capacidade de obter o cifrotexto de qualquer purotexto a sua escolha. Em seguida, ele tenta determinar o purotexto que foi encriptado para dar algum outro cifrotexto.
- d) É o tipo de ataque que o adversário, além de ser capaz de obter deciptação de qualquer cifrotexto à sua escolha, consegue outras informações sobre tal deciptação, por exemplo, se a deciptografia de algum cifrotexto gera uma mensagem em um idioma conhecido.
- e) É um tipo de ataque ativo, já que o adversário pode adaptavelmente pedir encriptação e/ou deciptação da sua escolha.

20) O Python sob a ótica da segurança da informação, mais especificamente do Pentest, pode seguir o escopo das etapas descritas: Reconhecimento, Engenharia Social, *Scanning*, Exploração e Pós-exploração. Para trabalhar com *sockets* e conexões em alto nível, na etapa de *Scanning*, é necessária a importação da biblioteca:

- a) *whois*.
- b) *argparse*.
- c) *scapy*.
- d) *threading*.
- e) *subprocess*.

21) O particionamento de discos é um ponto que deve ser levado em consideração na instalação de um sistema Linux, pois além de organizar as informações, pode adicionar mais segurança ao sistema. O comando *mount* é o responsável por permitir utilizar algumas opções para aumentar a segurança das partições. Assinalar a alternativa que se refere ao parâmetro usado para inibir que binários com direito especial de *suidbit* sejam executados em uma partição:

- a) *noatime*.
- b) *noexec*.
- c) *nodev*.
- d) *nosuid*.
- e) *nobin*.

22) Para funcionar de forma correta e eficiente, um hipervisor deve atender a alguns requisitos básicos: ele deve prover um ambiente de execução aos programas essencialmente idêntico ao da máquina real, do ponto de vista lógico. Para que seja caracterizada com um hipervisor ideal, certas propriedades devem ser satisfeitas, das quais uma está descrita abaixo. Assinalar a alternativa que se refere a esta propriedade:

Grande parte das instruções do processador virtual (o processador provido pelo hipervisor) deve ser executada diretamente pelo processador da máquina real, sem intervenção do hipervisor. As instruções da máquina virtual que não puderem ser executadas pelo processador real devem ser interpretadas pelo hipervisor e traduzidas em ações equivalentes no processador real. Instruções simples, que não afetem outras máquinas virtuais ou aplicações, podem ser executadas diretamente no hardware.

- a) Eficiência.
- b) Controle de Recursos.
- c) Gerenciabilidade.
- d) Encapsulamento.
- e) Recursividade.

23) Todo sistema de computadores interligados em rede ou conectados à internet é passível de sofrer com problemas de segurança e ficar vulnerável a ataques cibernéticos. No entanto, existem soluções capazes de identificar diferentes tipos de ameaças e ajudar nos *reports* de riscos, uma delas é o *scanner* de vulnerabilidades. Em qual das ferramentas para verificação de vulnerabilidades listadas abaixo, as identificações das ameaças são colocadas em modo *offline*, para avaliação e correção?

- a) *Aircrack-ng*.
- b) *Nikto*.
- c) *Retina network security*.
- d) *Comodo HackerProof*.
- e) *Wireshark*.

24) Os *Playbooks* do Ansible são um conjunto de instruções que especificam como um determinado sistema deve ser configurado ou gerenciado. Das diretrizes descritas abaixo para escrever *playbooks*, assinalar a alternativa INCORRETA:

- a) Ao realizar testes, use um pequeno subconjunto de servidores para que suas *plays* executem mais rapidamente.
- b) Como é possível combinar tarefas para diferentes distribuições Linux em um *playbook*, não é recomendável escrever um *playbook* separado para cada distribuição.
- c) Sempre faça um *dry run* para garantir que todos os comandos estejam funcionando (execute com *-check-mode flag*).
- d) Certifique-se de que todos os nomes de *host* definidos em */etc/ansible/hosts* sejam "resolvíveis".
- e) Como a comunicação com *hosts* remotos é feita usando SSH, as chaves devem ser aceitas pela máquina de controle, então, troque as chaves com *hosts* remotos antes do início ou esteja pronto para digitar "Sim" para aceitar solicitações de troca de chaves SSH para cada *host* remoto que você deseja gerenciar.

25) Protocolos de segurança foram desenvolvidos, com o objetivo de manter a rede sem fio mais segura. Para se atingir uma melhor configuração para rede, atingindo maiores distâncias e maiores velocidades também, deve-se utilizar a seguinte combinação protocolo/criptografia:

- a) WPA2-PSK (TKIP).
- b) WPE-TKP (EAP).
- c) WPA2-PSK (AES).
- d) WPE--TKP (AES).
- e) WPA2-PSK (EAP).

26) Kerberos é um protocolo de segurança de rede de computador que autentica solicitações de serviço entre dois ou mais *hosts* confiáveis em uma rede não confiável, como a Internet. Dentro do fluxo do protocolo, na etapa inicial, o usuário solicita:

- a) Uma chave de sessão criptografada (SK1) do servidor de autenticação (AS).
- b) Um *Ticket Granting Ticket* (TGT) do servidor de concessão de tíquetes (TGS).
- c) Uma chave de sessão de serviço (SK2) do servidor de concessão de tíquetes (TGS).
- d) Um *Ticket Granting Ticket* (TGT) do servidor de autenticação (AS).
- e) Uma chave de sessão criptografada (SK1) do servidor de concessão de tíquetes (TGS).

27) Assinalar a alternativa que preenche as lacunas abaixo CORRETAMENTE:

O DNSSec é um protocolo que se baseia na criptografia de chave _____. Todas as informações enviadas por um servidor DNS são assinadas com a chave _____ da zona de origem, de forma que o receptor possa verificar sua autenticidade.

- a) privada | pública
- b) simétrica X.25 | assimétrica
- c) pública | privada
- d) privada | simétrica
- e) pública e privada | privada

28) As páginas *web* e as mensagens de *e-mail* podem conter vários vírus capazes de trazer prejuízos a um computador. Um dos mecanismos que finge estar sendo originado e é capaz de coletar informações confidenciais de uma pessoa e ao qual esse mecanismo forjador deu a origem do desenvolvimento dos recursos de CAPTCHA. O trecho refere-se ao tipo de ataque de:

- a) *Botnet*.
- b) *Adware*.
- c) *Malware*.
- d) *Phishing*.
- e) *Scanning*.

29) Ao executar o código Python abaixo, foi identificado um erro. Este erro trata-se de um problema de:

```
1 def spam():
2     shows = 12
3     return shows
4
5     print(spam())
```

- a) Concatenação.
- b) Indentação.
- c) Repetição.
- d) Índice.
- e) *F string*.

30) A comunidade OWASP (*Open Web Application Security Project*) destacou, em seu documento OWASP top 10, as consequências dos problemas de segurança mais comuns e importantes no contexto de aplicação WEB. Dentre eles está o *Cross-Site Scripting* (XSS), que se baseia em:

- a) Manipulação de metadados, e.g. repetição ou adulteração do JSON Web Token (JWT) de controle de acesso, *cookie* ou campo escondido para elevação de privilégio.
- b) Roubar o uso da sessão do utilizador, contornar autenticação multifator, podendo direcionar usuários para páginas maliciosas.
- c) Usar força bruta para obter código e adulterar informações de páginas.
- d) Execução de injeção de códigos no navegador através da cópia oculta de informações.
- e) Execução remota de código relacionado com uma vulnerabilidade Struts 2.

31) O DoS (*Denial of Service*) é uma técnica em que um atacante utiliza um equipamento conectado à rede de computadores para tirar a operação de um serviço, um *host* conectado à internet. Quando usado de forma distribuída, temos o DDoS (*Distributed Denial of Service*). Dentre os tipos de ataques de DDoS que visam usar a exploração do consumo do uso de *hardware* até exaurir os recursos estão:

- a) HTTP Get e HTTP Post.
- b) VoIP (SIP INVITE Flood) e Slow Read DDoS.
- c) Ethernet flood e Syn Frame Realy.
- d) ICMP Distributed e Ping of Death.
- e) Fragmentação e TCP Syn Flood.

32) Dentre os protocolos de roteamento dinâmico está um que possui funcionamento transformando o conjunto de redes, roteadores e linhas reais em um grafo orientado, ao qual se atribui um custo (distância, retardo etc.) a cada arco, sendo compatível com três tipos de conexões de redes: *links* ponto a ponto, redes de multiacesso com e sem difusão. Esse protocolo é o:

- a) RIPv2
- b) OSPF
- c) MPLS
- d) EIGRP
- e) RIPv1

33) Dentre os comandos para configurar e analisar as configurações de segurança disponíveis no ambiente Microsoft Windows está um comando que permite gerir diretivas de grupo imediatamente. O comando que permite configurar as diretivas de segurança é:

- a) gpupdate /force
- b) gpedit /sec
- c) secedit /configure
- d) secedit /template
- e) sfc /scanow

34) Dentre os recursos disponíveis para Windows Server está o Failover transparente do SMB, que permite:

- a) Agregação de largura de banda e tolerância a falhas, possibilitando que o acesso aos serviços HTTP restaurem automaticamente em caso de falhas.
- b) Suporte ao uso de adaptadores de rede com capacidade RDMA, que funciona a toda velocidade com latência muito baixa.
- c) A um administrador gerenciar compartilhamentos de arquivos no servidor de arquivos, de ponta a ponta, a partir da linha de comando.
- d) Os clientes SMB se reconectar a outro nó do *cluster* de forma transparente, sem interromper os aplicativos do servidor que estão armazenando dados nesses compartilhamentos de arquivos.
- e) O impedimento de um invasor que faça o *downgrade* do dialeto negociado inicialmente e das funcionalidades entre o cliente e o servidor.

35) A modelagem de ameaças está ganhando cada vez mais notoriedade com a sofisticação dos tipos de ataques existentes. Uma premissa das ameaças é aceitar que qualquer sistema terá uma vulnerabilidade. A MITRE, assim, criou o ATT&CK, que visa mapear os fluxos de dados de acordo com suas interações e limites de confiança. Entre os mnemônicos utilizados para registros das táticas, estão:

- a) Confiabilidade, integridade, autenticidade e evasão.
- b) Acesso final, filtração, movimento vertical e defesa.
- c) Acesso central, riscos, não repúdio e privilege.
- d) Disponibilidade, privacidade, legalidade e alta disponibilidade.
- e) Acesso inicial, execução, persistência e escalação de privilégios.

36) Dentre as principais características do protocolo IPv6 está o suporte para autenticação e privacidade, que é provido por meio de:

- a) Inclusão de segurança na camada de rede através da arquitetura IPSec.
- b) Fragmentação (*Fragmentation Header*).
- c) Encriptação (Ipv6).
- d) Autoconfiguração permitindo mapear endereços e nomes.
- e) Suporte a *jumbograms*.

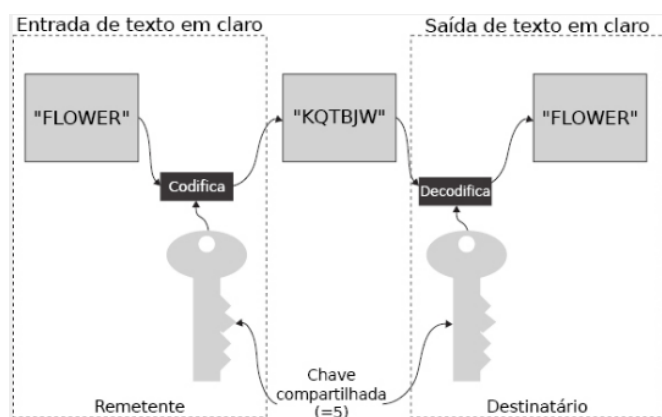
37) O gerenciamento de sessão é o procedimento de processamento seguro de muitas solicitações de um determinado usuário ou organização para um aplicativo baseado na *web*. Considerando-se as melhores práticas de programação segura, sobre o gerenciamento de sessão, analisar os itens abaixo:

- I. Disponibilizar a funcionalidade de *logout* em todas as páginas protegidas por autorização.
- II. Definir o atributo “seguro” para *cookies* transmitidos por uma conexão TLS.
- III. Utilizar o mesmo identificador de sessão em qualquer reautenticação.

Está(ão) CORRETO(S):

- a) Somente o item I.
- b) Somente o item II.
- c) Somente os itens I e II.
- d) Somente os itens II e III.
- e) Todos os itens.

38) Tendo em vista suas características, o esquema abaixo apresenta a visão esquemática de um sistema de:



- a) Criptografia assimétrica.
- b) Criptografia simétrica.
- c) Ataque cibernético.
- d) Backup.
- e) Infraestrutura de chave pública (PKI).

39) É o método mais simples de recuperação de desastres e envolve o armazenamento de dados fora do local ou em uma unidade de remoção. No entanto, tem certa limitação, pois a infraestrutura de TI em si não é submetida a esse procedimento. Assinalar a alternativa que melhor representa o método de recuperação de desastres citado:

- a) Hot site.
- b) Cold site.
- c) DRaaS.
- d) Backup.
- e) Virtualização.

40) Sobre o *firewall stateful*, marcar C para as afirmativas Certas, E para as Erradas e, após, assinalar a alternativa que apresenta a sequência CORRETA:

- () Um *firewall stateful* apenas enviará respostas de DNS se elas estiverem associadas a uma *query* interna de DNS, ou seja, ele não aceita uma resposta caso não tenha enviado uma requisição.
- () O processamento de pacotes por um filtro *stateful* envolve a verificação nas camadas de transporte e sessão, fazendo a associação da quintupla: Endereço IP Remoto + Endereço IP Local + Porta Remota + Porta Local + Protocolo de Transporte.
- () Esse *firewall* tem a habilidade de criar sessões de informação virtual para manter a inspeção sobre protocolos não orientados à conexão de pacotes que possam ter conteúdo não legal.

- a) C - C - E.
- b) E - E - C.
- c) C - E - C.
- d) E - C - E.
- e) C - C - C.

41) O programa cliente de e-mail de um funcionário da organização está enviando dezenas de mensagens para sua lista de endereços de e-mail sem que ele ou alguém tenha efetivamente enviado e escrito essas mensagens. Esse tipo de comportamento é típico de infecção por:

- a) Keyloggers.
- b) Spywares.
- c) Backdoors.
- d) Trojans.
- e) Worms.

42) Assinalar a alternativa que preenche ambas as lacunas abaixo CORRETAMENTE:

O _____ foi uma solução introduzida pela Cisco Systems que resolve a maior parte dos problemas relacionados ao esgotamento do número de endereços IP da Internet. O firewall que executa _____ realiza um mapeamento entre endereços da Internet válidos e inválidos (que são utilizados pelos computadores da rede interna), tornando-se desnecessário que cada estação possua seu próprio endereço IP válido na Internet.

- a) NAT
- b) SIEM
- c) IPS
- d) IDS
- e) WAF

43) Os serviços de prevenção de intrusão (IPS), além de alertar sobre tentativas de ataque, permitem que elas sejam bloqueadas. O IPS permite detectar os seguintes tipos de ameaças na rede:

- I. Ataques direcionados a aplicações web, como *cross site script*, *php injection* e *sql injection*.
- II. Utilização da rede por aplicações não permitidas como P2P (incluindo *Bittorrent*).
- III. Ataques direcionados a sistemas operacionais.
- IV. *Spams* e *phishing*.

Estão CORRETOS:

- a) Somente os itens I e II.
- b) Somente os itens I e III.
- c) Somente os itens I, III e IV.
- d) Somente os itens II, III e IV.
- e) Todos os itens.

44) Quanto aos algoritmos suportados pelo IPSec, marcar C para as afirmativas em que todos os algoritmos são suportados, E para as que apresentam pelo menos algum que não o é e, após, assinalar a alternativa que apresenta a sequência CORRETA:

- () Criptografia: AES, DES, 3DES, RC5, IDEA.
() Hashing: MD5, SHA-1.
() Autenticação: assinaturas digitais RSA e assinaturas digitais DSS.
- a) C - C - E.
b) C - C - C.
c) C - E - C.
d) E - C - E.
e) E - E - C.

45) São alvos colocados no sistema para chamar a atenção de atacantes e, assim, direcionar para estes pontos as forças dos atacantes. Com isso, é possível obter informações das tentativas de ataque realizadas e conseguir construir contramedidas para evitá-las. O trecho descreve o conceito de:

- a) *Bitnet*.
b) *Broadcast*.
c) Metabuscador.
d) *Honeypot*.
e) *Spoofing*.

46) Quanto à segurança cibernética, a estratégia primordial de mitigação para todos que buscam se defender de danos e impactos do *ransomware* deve ser a:

- a) Causa-raiz.
b) Exposição.
c) Recuperação.
d) Detecção.
e) Prevenção.

47) Considerando-se os métodos de *exploit* de causa-raiz de todos os *hackers* maliciosos e *malware*, atualmente, os dois métodos que se configuram como as principais causas de exploração maliciosa por *hackers* e *malware* são:

- a) Engenharia social e *software* sem *patch*.
b) Ataque remoto a servidor e furto de credencial.
c) Adivinhação de senha e RDP
d) Mídias externas e engenharia social.
e) Força bruta e *sniffing*.

48) Portas são as janelas e entradas no mundo cibernético. Para a localização de vulnerabilidades, é necessário conhecer as portas de comunicação utilizadas pelos serviços ou aplicativos, as quais poderão ser usadas pelos invasores. Nesse sentido, numerar a 2ª coluna de acordo com a 1ª e, após, assinalar a alternativa que apresenta a sequência CORRETA:

- (1) SMTP.
(2) Telnet.
(3) SSH.

- () 25/tcp.
() 23/tcp.
() 22/tcp.

- a) 1 - 2 - 3.
b) 3 - 2 - 1.
c) 2 - 3 - 1.
d) 2 - 1 - 3.
e) 1 - 3 - 2.

49) Administradores de redes podem ajudar a melhorar o cenário dos ataques DDoS implementando boas práticas que impeçam que a infraestrutura pela qual são responsáveis seja usada para gerar ataques. Entre as boas práticas, pode-se citar:

- I. Excluir os serviços desnecessários (*hardening*).
II. Monitorar os *logs*, a procura de erros e de tentativas de exploração de vulnerabilidades.
III. Verificar o tráfego de entrada na rede a procura de tentativas de acesso não autorizado.

Está(ão) CORRETO(S):

- a) Somente o item I.
b) Somente o item II.
c) Somente os itens I e II.
d) Somente os itens I e III.
e) Todos os itens.

50) As condições de uma organização mudam constantemente, assim como os riscos encontrados por ela. O foco principal de gerenciamento de riscos é antecipar-se a ameaças observadas. Uma análise de impacto de negócios (BIA - *Business Impact Analysis*) é uma análise formal das funções e atividades de uma organização, que as classifica como críticas ou não. Na BIA, o RPO - *Recovery Point Objective* expressa:

- a) O tempo máximo permitido para recuperar a função.
b) O investimento mínimo para recuperar a função.
c) A quantidade de perda de dados aceitável.
d) A probabilidade anual de uma perda.
e) A perda anual estimada devido a uma ameaça específica.