

Concurso Público UERJ 2024 - Técnico Universitário Superior (TUS)

ANALISTA DE TECNOLOGIA DA INFORMAÇÃO - INFRAESTRUTURA (101)

PROIBIDO FOLHEAR ESTE CADERNO ANTES DA AUTORIZAÇÃO PARA O INÍCIO DA PROVA

Além deste caderno de **50** questões, você recebeu:

- um cartão-resposta personalizado com questões de múltipla escolha com quatro alternativas.

Duração máxima da prova: **4 horas e 30 minutos**

Autorização para deixar o local de prova: **após 1 hora** do início da prova

INSTRUÇÕES DA PROVA OBJETIVA

- 1) Na mesa, são permitidos apenas este caderno, o cartão-resposta e a caneta esferográfica transparente de tinta preta ou azul **SEM A TAMP A**. Demais pertences devem estar devidamente guardados embaixo da carteira.
- 2) Terminada a prova, entregue este caderno e o cartão-resposta ao fiscal de sala.
- 3) Os três últimos candidatos somente poderão deixar a sala, juntos, quando último entregar a prova. Os três deverão assinar a ata de sala, atestando a idoneidade e a regularidade da finalização da prova.

NO CARTÃO-RESPOSTA:

- 4) Confira os seus dados pessoais, número de inscrição e cargo/programa escolhido.
- 5) Assine e transcreva a frase impressa no cartão assim que o receber (cartões entregues sem a assinatura e/ou sem a transcrição da frase **NÃO** serão corrigidos).
- 6) Marque a alternativa correta de acordo com a ilustração instrutiva. A bolinha deve estar completamente preenchida, caso contrário sua resposta poderá não ser computada. Somente as respostas nele assinaladas serão objeto de correção.

Atenção: Por motivo de segurança, o candidato **NÃO** poderá anotar seu gabarito em nenhum outro local que não seja seu cartão-resposta.

NO CADERNO DE QUESTÕES:

- 7) Verifique, somente após autorização para o início da prova, a numeração das questões e das páginas (havendo irregularidade no material, comunique ao fiscal de sala).
- 8) Não arranque, destaque ou rasgue nenhuma folha ou parte dela.

Atenção: Por motivo de segurança, este caderno **NÃO** poderá ser levado pelo candidato em nenhum momento.

Todos os casos e nomes utilizados nas provas do CEPUERJ são fictícios.

ORGANIZADOR



CEPUERJ

LÍNGUA PORTUGUESA

Texto I

A revolução da IA mudará o trabalho?

1 Seja no mercado de trabalho ou nas tarefas do cotidiano, ainda não é possível mensurar os impactos a longo prazo da inteligência artificial. De qualquer forma, sua existência não pode ser ignorada: a chegada da IA foi um marco revolucionário. E, como toda nova tecnologia, pode gerar medo – mas também oportunidades.

5 Para Bill Gates, fundador da Microsoft, o desenvolvimento de ferramentas de IA, como o ChatGPT, foi uma das maiores revoluções que ele já presenciou. “Durante a minha vida, vi duas demonstrações de tecnologia que me pareceram revolucionárias”, escreveu Gates em seu blog. “A primeira vez foi em 1980, quando fui apresentado a uma interface gráfica de usuário – a precursora de todos os sistemas operacionais modernos, incluindo o Windows. A segunda veio ano passado. Tenho me reunido com a
10 equipe da OpenAI desde 2016 e fiquei impressionado com o constante progresso”.

Dados do Fundo Monetário Internacional (FMI) mostram que quase 40% dos empregos no mundo serão afetados pelo avanço da IA. No entanto, isso não significa a extinção de profissões. “À medida que o poder computacional fica mais barato, a capacidade do ChatGPT de expressar ideias será cada vez mais semelhante a ter um funcionário administrativo disponível para ajudá-lo em diversas tarefas”,
15 escreve o magnata em seu blog.

O que pode acontecer, na verdade, é a alocação da inteligência humana em atividades mais estratégicas e que demandam senso crítico e criatividade. “Seres humanos são treinados utilizando conjuntos de dados e, em breve, esses conjuntos de dados também serão utilizados para treinar as IAs, que capacitarão as pessoas a realizar seus trabalhos de forma mais eficiente.”

20 Gates descreve as capacidades do ChatGPT 4 como “dramáticas”, destacando sua habilidade avançada de leitura e escrita. Embora as habilidades da ferramenta sejam impressionantes, especialistas afirmam que a tecnologia tende a automatizar tarefas, e não profissões inteiras.

Estima-se que até 2030 os conjuntos de habilidades necessárias para nossos empregos mudarão em até 65%. Se antes as funções eram apenas definidas por títulos, agora o profissional precisa
25 desenvolver um conjunto de competências diversificadas e adaptativas para se enquadrar nesse novo modelo de trabalho.

Diante desse cenário, torna-se necessário que os profissionais saibam conviver com essa realidade e aprendam a usar a IA de forma estratégica em suas carreiras.

“Estamos apenas no início dessa transição, uma época empolgante, mas confusa”, ressalta Gates. No
30 entanto, nesta nova onda de tecnologia, a inovação torna-se uma questão de sobrevivência para as empresas.

A capacidade da IA de processar grandes volumes de dados, identificar padrões e tomar decisões inteligentes está transformando a maneira como as empresas operam e como as pessoas interagem com a tecnologia.

35 Em paralelo a essa transformação, líderes e gestores ganham um novo papel: o de agentes de mudança, a fim de conduzir o movimento de transformações resultantes da implementação da inteligência artificial nos processos do dia a dia.

Isso quer dizer que os tomadores de decisão também serão responsáveis por promover a colaboração com outros departamentos e funções para garantir a integração e o alinhamento do trabalho com a IA,
40 não apenas nas suas equipes, mas também com clientes e parceiros.

Disponível em: https://exame.com/carreira/a-revolucao-da-ia-mudara-o-trabalho-veja-o-que-bill-gates-pensa-sobre-o-assunto/?utm_source=pushnews&utm_medium=pushnotification.

Texto adaptado.

De acordo com o Texto I, responda às questões de números 1 a 9.

1) A reportagem traz como título uma pergunta sobre a Inteligência Artificial (IA). Como resposta a essa pergunta, o texto leva à conclusão de que a revolução da IA mudará o trabalho, pois:

- a) os profissionais precisarão desenvolver um conjunto diversificado de competências para se enquadrar em um novo modelo de trabalho
- b) o desenvolvimento de ferramentas de IA configura-se como a mais recente revolução tecnológica a acontecer no mundo digital
- c) a IA promove a colaboração entre departamentos e funções para garantir a integração e o alinhamento do trabalho
- d) algumas profissões desaparecerão à medida que o uso da tecnologia da IA ficar mais barato

2) De acordo com o texto, o cenário das novas tecnologias apresenta uma dualidade entre:

- a) instabilidade e constância
- b) diversidade e convergência
- c) insegurança e possibilidade
- d) individualismo e universalidade

3) Uma das ideias defendidas nesse texto é a de que a IA será uma aliada da produtividade. A fala de Gates que serve de argumento para sustentar a validade dessa ideia é:

- a) “Estamos apenas no início dessa transição, uma época empolgante, mas confusa” (l. 29)
- b) “Durante a minha vida, vi duas demonstrações de tecnologia que me pareceram revolucionárias” (l. 6 e 7)
- c) “Tenho me reunido com a equipe da OpenAI desde 2016 e fiquei impressionado com o constante progresso.” (l. 9 e 10)
- d) “esses conjuntos de dados também serão utilizados para treinar as IAs, que capacitarão as pessoas a realizar seus trabalhos de forma mais eficiente.” (l. 18 e 19)

4) Em meio a tantos avanços, Bill Gates tece algumas considerações sobre a tecnologia de IA. Considerando-se o aspecto revolucionário, Gates equipara:

- a) habilidade de liderança da IA e papel de gestores que operam no mundo do trabalho
- b) desenvolvimento do ChatGPT e tecnologia que antecedeu os atuais sistemas operacionais
- c) uso de ferramentas de IA no processamento de dados e aplicação dessas ferramentas na tomada de decisões
- d) atuação do ChatGPT em diferentes profissões e desempenho de profissionais em carreiras definidas por títulos

5) A sequenciação temática é o mecanismo que faz o texto avançar no nível da informação. O terceiro parágrafo retoma e dá continuidade à ideia presente no primeiro parágrafo de que o:

- a) advento da IA não pode ser ignorado
- b) aperfeiçoamento da IA pode gerar medo
- c) impacto da IA ainda não pode ser medido
- d) desenvolvimento da IA trará novas oportunidades

6) “De qualquer forma, sua existência não pode ser ignorada: a chegada da IA foi um marco revolucionário”. (l. 2 e 3) A relação semântica que a segunda oração estabelece com a primeira é de:

- a) explicação
- b) condição
- c) tempo
- d) modo

7) “Gates descreve as capacidades do ChatGPT 4 como ‘dramáticas’”. (l. 20) Nessa oração, a palavra “dramáticas”, empregada entre aspas, significa:

- a) teatrais
- b) patéticas
- c) comoventes
- d) surpreendentes

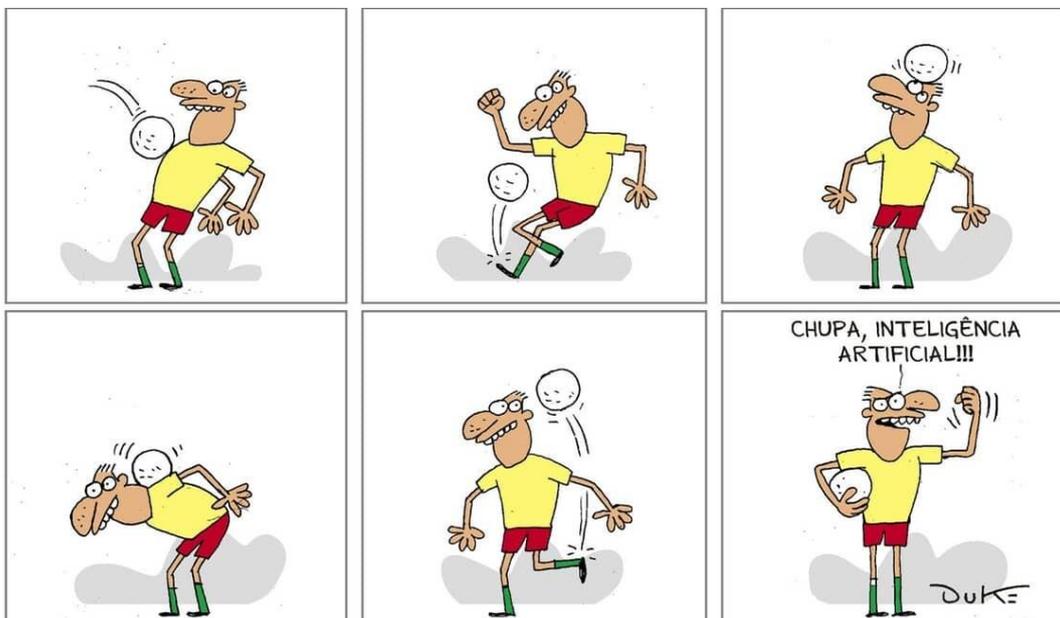
8) Os sinais de pontuação têm a importante função de colaborar para a construção da coerência dos textos. O trecho do qual a vírgula não pode ser retirada sob pena de causar, nele, alteração de sentido é:

- a) “No entanto, isso não significa a extinção de profissões.” (l. 12)
- b) “De qualquer forma, sua existência não pode ser ignorada” (l. 2)
- c) “Em paralelo a essa transformação, líderes e gestores ganham um novo papel” (l. 35)
- d) “esses conjuntos de dados também serão utilizados para treinar as IAs, que capacitarão as pessoas a realizar seus trabalhos de forma mais eficiente.” (l. 18 e 19)

9) “Dados do Fundo Monetário Internacional (FMI) mostram que quase 40% dos empregos no mundo serão afetados pelo avanço da IA. No entanto, isso não significa a extinção de profissões.” (l. 11 e 12)
A reescrita que mantém o significado básico desse trecho é:

- se dados do Fundo Monetário Internacional (FMI) mostram que quase 40% dos empregos no mundo serão afetados pelo avanço da IA, isso não significa a extinção de profissões
- como dados do Fundo Monetário Internacional (FMI) mostram que quase 40% dos empregos no mundo serão afetados pelo avanço da IA, isso não significa a extinção de profissões
- embora dados do Fundo Monetário Internacional (FMI) mostrem que quase 40% dos empregos no mundo serão afetados pelo avanço da IA, isso não significa a extinção de profissões
- quando dados do Fundo Monetário Internacional (FMI) mostram que quase 40% dos empregos no mundo serão afetados pelo avanço da IA, isso não significa a extinção de profissões

Texto II



Disponível em: <https://www.itatiaia.com.br/editorias/charges/2023/04/14/charge-do-duke-a-inteligencia-artificial-vai-substituir-humanos>.

Acesso em: 09 mar. 2024.

De acordo com o Texto II, responda à questão de número 10.

10) Essa charge de Duke constrói o humor a partir da relação IA / ser humano. A mensagem construída no Texto II, que também está presente no Texto I, é:

- os seres humanos superam a IA no âmbito da criatividade
- a IA é incompetente em questões concernentes aos esportes
- as habilidades humanas serão superadas pela IA em futuro próximo
- atividades mais complexas serão exercidas tanto por seres humanos quanto pela IA

LEGISLAÇÃO

11) A lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) – estabelece como princípio, dirigido aos agentes de tratamento, “a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão”. Essa descrição refere-se ao princípio da:

- a) qualidade
- b) segurança
- c) adequação
- d) necessidade

12) O Estatuto da Pessoa com Deficiência (lei nº 13.146/2015) estabelece uma série de direitos à pessoa com deficiência. Ao mesmo tempo, impõe deveres ao Estado no que diz respeito ao direito à educação, sendo um deles:

- a) participação dos estudantes com deficiência e de suas famílias nas diversas instâncias de atuação da comunidade escolar
- b) sistema educacional inclusivo apenas nos níveis fundamental e médio, bem como o aprendizado ao longo de toda a vida
- c) oferta de educação bilíngue, na modalidade escrita da língua portuguesa como primeira língua e em Libras como segunda língua
- d) disponibilização de professores para o atendimento especializado, dispensada a exigência de nível superior aos tradutores e intérpretes da Libras em salas de aula de cursos de graduação

13) De acordo com o plano de cargos, carreiras e remuneração do quadro de pessoal dos servidores técnico-administrativos da Universidade do Estado do Rio de Janeiro (UERJ), lei nº 6.701/2014, é direito desses servidores:

- a) acesso, mediante pagamento, aos serviços assistenciais prestados pela Universidade
- b) acesso, mediante pagamento, aos programas de capacitação prestados pela Universidade
- c) matrícula no colégio de aplicação da UERJ para seus dependentes, no limite de vagas estipuladas para essa destinação
- d) matrícula nos cursos de graduação da UERJ para seus dependentes, no limite de vagas estipuladas para essa destinação

De acordo com o Estatuto dos Funcionários Públicos Cíveis do Poder Executivo do Estado do Rio de Janeiro (decreto-lei nº 220/75), responda às questões de números **14** e **15**.

14) Considerando esse Estatuto e o Regulamento do Estatuto dos Funcionários Públicos Cíveis do Poder Executivo do Estado do Rio de Janeiro (decreto nº 2.479/79), é dever do servidor público:

- a) assiduidade
- b) assistência médica
- c) assistência judiciária
- d) representação de gabinete

15) Após o devido procedimento administrativo disciplinar, observada a ampla defesa e o contraditório, ficou constatado que um servidor concursado da UERJ, que nunca havia sofrido quaisquer sanções, por simples negligência, descumpriu deveres funcionais impostos pelo Estatuto. A sanção disciplinar cabível, nesse caso, é:

- a) demissão
- b) suspensão
- c) advertência
- d) destituição de função

De acordo com a lei nº 5.427/2009, que estabelece normas sobre atos e processos administrativos no âmbito do Estado do Rio de Janeiro, responda às questões de números **16** a **18**.

16) No curso de procedimento administrativo disciplinar, a situação que sempre atenua a penalidade é a:

- a) reincidência nas infrações
- b) reparação espontânea do dano
- c) obtenção de vantagem pecuniária
- d) ausência de comunicação do risco de danos

17) É um princípio do processo administrativo:

- a) singularidade
- b) verdade real
- c) finalidade
- d) oralidade

18) O superintendente da Superintendência de Gestão de Pessoas da UERJ (SGP) verifica que há requerimento de progressão, formulado por um servidor concursado, a ser apreciado pelo coordenador, responsável por analisar o pedido. Notando que o coordenador extrapolou consideravelmente o prazo legal de análise do expediente, o superintendente, superior hierárquico, solicita o processo e, após constatar que o servidor faz jus ao requerido, defere o pedido de licença. Nesse caso, o superintendente se valeu do seguinte instituto de direito administrativo:

- a) anulação
- b) avocação
- c) *bis in idem*
- d) recurso hierárquico

De acordo com a Constituição da República Federativa do Brasil de 1988, responda às questões de números **19** e **20**.

19) A vedação à prática do nepotismo, isto é, a proibição do favorecimento de parentes ou amigos próximos em detrimento de pessoas mais qualificadas, é um efeito do ordenamento jurídico. Tal prevenção é uma exteriorização do princípio constitucional da:

- a) eficiência
- b) publicidade
- c) razoabilidade
- d) impessoalidade

20) Os atos de improbidade administrativa são práticas contrárias ao bom funcionamento da Administração Pública. A Constituição prevê a seguinte penalidade para os casos de improbidade:

- a) proibição de frequentar determinados lugares
- b) privação de liberdade em regime fechado
- c) proibição de inscrever-se em concurso
- d) perda da função pública exercida

CONHECIMENTOS ESPECÍFICOS

21) O comando *ping* é um teste simples de conectividade. Ao perceber um problema de conectividade em um dispositivo externo, um usuário realizou os dois testes A e B, a seguir, em um intérprete de comandos.

| Teste A | Teste B |
|----------------------|---------------------|
| \$ ping 152.92.1.117 | \$ ping www.uerj.br |

Considerando os testes A e B, é correto afirmar que são:

- a) idênticos; se o teste B falhar, o teste A também falha
- b) idênticos, somente se o endereço IP de www.uerj.br for 152.92.1.117
- c) não idênticos; o teste A pode falhar, enquanto o teste B pode ter sucesso
- d) não idênticos; o teste B pode falhar, enquanto o teste A pode ter sucesso

22) Para navegar na Internet, é necessário que algumas configurações de rede sejam efetuadas. Em geral, essas configurações são realizadas a partir de informações disponibilizadas por um determinado tipo de servidor. A atribuição de endereço IP, a máscara de rede e o endereço de *gateway* são exemplos de informações de configurações disponibilizadas pelo servidor do tipo:

- a) DHCP
- b) DNS
- c) NAT
- d) Web

23) A rede de computadores pode ser considerada um sistema complexo, que possui muitos componentes, inúmeras aplicações e protocolos. Didaticamente, uma possível forma de organização é a separação em camadas, como o modelo de referência *Open Systems Interconnection* (OSI). Uma característica da camada de rede do modelo OSI é:

- a) definir técnicas dos dispositivos elétricos e ópticos do sistema
- b) fornecer aplicações de rede e de seus protocolos aos usuários
- c) prover serviço de entrega de segmentos à camada de transporte
- d) proporcionar garantia de entrega entre enlaces do transmissor ao receptor

24) A inspeção da configuração de rede de um dispositivo pode proporcionar uma noção da sua forma de funcionamento. Considere um computador conectado a uma rede IP, operando normalmente, com navegação à Internet e as seguintes configurações de rede:

| | |
|----------------|----------------------|
| Endereço IP | : 192.168.10.100 / 8 |
| DNS primário | : 192.168.10.200 |
| Gateway padrão | : 192.168.10.1 |

É correto afirmar que o acesso:

- a) à Internet dependerá, em alguma etapa, da utilização do protocolo NAT
- b) a outro endereço IP, externo a essa rede, dependerá de conexão via VPN
- c) via DNS está na mesma rede do dispositivo, o que torna a configuração inadequada
- d) ao endereço 192.200.10.101, que pertence à outra rede, deve ser realizado de maneira indireta

25) As LANs sem fio são uma das mais importantes tecnologias de rede de acesso à Internet. Embora muitas tecnologias e padrões para redes sem fio tenham sido desenvolvidos, uma classe de padrões bem popular é a IEEE 802.11, também conhecida como *Wi-Fi*. Com relação a esse padrão, é correto afirmar que:

- a) define o ponto de acesso (AP) com o qual o hospedeiro irá se associar, primariamente, através da inspeção de carga do AP
- b) apresenta elementos semelhantes, tais como as mesmas frequências e mesmos canais de todos os outros padrões existentes
- c) especifica um algoritmo para selecionar com qual, ou quais dos pontos de acesso (APs) disponíveis o dispositivo deve se associar
- d) compartilha características tais como o mesmo protocolo de acesso ao meio e a mesma estrutura de quadros da camada de enlace

26) Uma forma de indicar a quantidade de endereços IPs disponíveis vem da configuração de máscara de rede. Considerando que a Rede 1 deve conter 60 endereços IPs disponíveis e que a Rede 2 deve conter 200 endereços IPs disponíveis, a configuração das máscaras de rede que permite a quantidade necessária com o menor desperdício de endereços IPs, respectivamente, é:

- a) 255.255.255.0 / 255.255.254.0
- b) 255.255.255.192 / 255.255.255.0
- c) 255.255.255.252 / 255.255.255.0
- d) 255.255.255.254 / 255.255.254.0

27) O computador A possui a configuração de rede a seguir.

| | |
|-----------------|-----------------|
| Endereço IP | : 10.100.195.10 |
| Máscara de rede | : 255.255.192.0 |

O computador A deseja se comunicar com o computador B, que está fisicamente na mesma rede. Para que a comunicação entre ambos seja realizada de maneira direta, a configuração de endereço IP para o computador B deve ser:

- a) 10.100.59.2
- b) 10.100.112.1
- c) 10.100.129.30
- d) 10.100.193.10

28) Um aplicativo útil, do sistema operacional Linux, para análise em redes de computadores que mostra a sequência de roteadores pelos quais um pacote enviado passou é denominado:

- a) *traceroute*
- b) *tcpdump*
- c) *ethtool*
- d) *route*

29) A entidade de rede que atende requisições HTTP em nome de um servidor *web* de origem e que mantém cópias de objetos recentemente requisitados é o:

- a) *common gateway interface* - CGI
- b) servidor de aplicação
- c) *backend interface*
- d) servidor *proxy*

30) O protocolo TCP é conhecido por possuir “partida lenta”, seguido por um crescimento exponencial na quantidade de dados enviados, que termina se, necessariamente:

- a) houver mais de um evento de perda e transmissão que ocupe toda a banda disponível na interface de rede e detectar três ACKs duplicados
- b) houver um evento de perda, igualar o valor de cwnd ao valor da variável de estado ssthresh, ou detectar três ACKs duplicados
- c) houver mais de um evento de perda, ultrapassar o valor da variável de estado ssthresh, ou detectar dois ACKs duplicados
- d) houver um evento de perda, ultrapassar o valor da variável de estado ssthresh, ou detectar um ACK duplicado

31) A construção de projeto de sistemas possui uma prática complexa devido à quantidade de ações e tarefas envolvidas. Para facilitar o desenvolvimento do projeto, existem modelos de processos, como o modelo cascata. A fase do modelo cascata que define as estimativas de recursos necessários e o cronograma é:

- a) construção
- b) modelagem
- c) comunicação
- d) planejamento

32) O elemento que faz parte do processo de garantia da segurança dos sistemas de informação é:

- a) auditoria de permissões
- b) aplicação de métodos ágeis
- c) desenvolvimento de software
- d) seleção de recursos humanos

33) Em 1999, foi lançado o produto *VMWare Workstation* para *Linux*, destinado ao uso na área de virtualização. Esse produto trata-se de um hipervisor do tipo:

- a) I
- b) II
- c) III
- d) IV

34) *Amazon Elastic Cloud Computing (EC2)* é um serviço de nuvem oferecido pela Amazon que implementa um modelo de:

- a) SAAS
- b) PAAS
- c) IAAS
- d) HPC

35) Os processadores modernos da família x86 oferecem suporte à virtualização, como o Intel VT, que busca reduzir o custo computacional associado às técnicas tradicionais de virtualização. A origem desse custo advém da captura de:

- a) interrupções
- b) tempo de acesso à TLB
- c) chamadas de sistemas
- d) tempo de tradução binária

36) Em relação aos estados possíveis de um processo em um sistema operacional moderno, quando um determinado processo é interrompido por uma solicitação de disco, esse processo entrará no estado de:

- a) pronto
- b) terminado
- c) bloqueado
- d) em execução

37) Em um sistema de memória virtual, quando é necessário descartar uma página da memória, escolha aquela que não está em uso há mais tempo. Esse algoritmo é conhecido como:

- a) LRU
- b) FIFO
- c) Ótimo
- d) WSClock

38) A *Memory Management Unit* (MMU) é o componente responsável por gerenciar os acessos que a CPU envia à memória em decorrência da execução de um programa. Em relação à organização da memória física pela MMU, em um sistema com memória virtual usando paginação, a memória principal é dividida em:

- a) linhas
- b) blocos
- c) quadros
- d) segmentos

39) Em um sistema operacional multiprogramado interativo, a primeira ação que o Escalonador de Tarefas deve realizar para a correta operação do sistema computacional é:

- a) escolher o processador para o novo processo
- b) interromper o processo atual
- c) selecionar o novo processo
- d) salvar o contexto da MMU

40) Considere um sistema de armazenamento que utilize RAID 5 e possua três discos em seu grupo de proteção. Cada disco possui uma capacidade de 1TB. A quantidade total necessária de dados brutos para esse sistema de armazenamento é de:

- a) 15TB
- b) 5TB
- c) 4TB
- d) 3TB

41) Suponha a notação KB^+ e KB^- para representar as chaves pública e privada do usuário B, $KB^+(m)$ e $KB^-(m)$ para representar a mensagem m , cifrada com cada uma das duas chaves. Considere também que, em um sistema criptográfico assimétrico, a usuária A pretenda enviar uma mensagem sigilosa para B, e que KA^+ e KA^- representam as chaves pública e privada de A. A criptografia com a qual o usuário B consegue confirmar que a mensagem foi enviada pela usuária A é:

- a) $KB^+(KA^+(m))$
- b) $KB^+(KA^-(m))$
- c) $KB^-(KA^-(m))$
- d) $KB^-(KA^+(m))$

42) Considere que existe um segredo s , previamente compartilhado entre os usuários A e B, e que ambos podem apenas usar uma função de espalhamento (*Hash*) criptográfica $H(m)$. Para que a usuária A receba uma mensagem m do usuário B, garantindo que essa mensagem não foi manipulada, é necessário que B:

- a) calcule o $H(m)$; envie uma mensagem estendida $(m, H(m))$ para A, que pode calcular localmente $H(m)$ para confirmar a integridade da mensagem m
- b) calcule o $H(m)$ e $H(s)$; envie uma mensagem estendida $(m, H(m), H(s))$ para A, que pode calcular localmente $H(m)$ e $H(s)$ para confirmar a integridade da mensagem m
- c) concatene s com m para criar $m + s$; calcule o $H(m)$; envie uma mensagem estendida $(m, H(m), s)$ para A, que pode calcular localmente $H(m)$ e $H(s)$ para confirmar a integridade da mensagem m
- d) concatene s com m para criar $m + s$; calcule o $H(m+s)$; envie uma mensagem estendida $(m, H(m+s))$ para A, que pode calcular localmente $H(m+s)$ para confirmar a integridade da mensagem m

43) O ataque que **NÃO** explora o software diretamente é denominado:

- a) engenharia social
- b) ponteiros pendentes
- c) transbordamento de buffer
- d) ataque por cadeias de caracteres de formato

44) A combinação de propriedades que **NÃO** é desejável na comunicação segura é:

- a) integridade da mensagem e redundância
- b) sigilo do algoritmo criptográfico e codificação
- c) confidencialidade e integridade da mensagem
- d) autenticação das partes envolvidas e redundância

45) Com relação ao uso e funcionamento do *Secure Sockets Layer* (SSL) para proteção de conexões TCP entre um cliente e um servidor, o procedimento correto a ser realizado pelo cliente é:

- a) verificar o certificado, usar criptografia AES, cifrar o Segredo Pré-Mestre (PMS) com a chave pública do servidor e enviar o PMS ao servidor
- b) usar criptografia DES para criptografar e RSA para descriptografar a mensagem, gerando um Segredo Pré-Mestre (PMS), e enviar o PMS para o servidor
- c) usar um algoritmo específico de chave simétrica, análogo ao do servidor; gerar um Segredo Pré-Mestre (PMS) com a chave privada; e enviar o PMS cifrado para o servidor
- d) verificar o certificado, extrair a chave pública do servidor, gerar um Segredo Pré-Mestre (PMS), cifrar o PMS com a chave pública do servidor e enviar o PMS cifrado ao servidor

46) Estar conectado à Internet expõe um sistema a diversos riscos, tais como o envio de informações confidenciais a pessoas não autorizadas. Alguns mecanismos de segurança são necessários para manter ou tornar um sistema seguro, como, por exemplo, a inspeção de pacotes, que é realizada pela ferramenta:

- a) VPN
- b) IPSec
- c) *firewall*
- d) *wireshark*

47) A realização de *backups* regulares é uma das ações recomendadas para evitar a perda de dados. O *daemon* que pode executar tarefas agendadas com comandos que realizam *backups* é o:

- a) *date*
- b) *cron*
- c) *uptime*
- d) *prompt*

48) Considerando uma máquina na qual está instalado um sistema UNIX, o diretório que **NÃO** necessita de uma cópia de segurança é o:

- a) */etc*
- b) */usr*
- c) */dev*
- d) */home*

49) Ao realizar um *backup*, se o sistema copiar somente os arquivos que foram modificados a partir da última cópia de segurança realizada, a estratégia implementada, nesse caso, corresponde ao(à):

- a) *checkpoint* periódico
- b) *dumping* periódico
- c) cópia incremental
- d) cópia física

50) A norma ABNT NBR ISO/IEC 27005:2011 adota um processo genérico de gestão de riscos, composto de seis fases: definição do contexto; processo de avaliação de riscos; tratamento do risco; aceitação do risco; comunicação e consulta do risco; e monitoramento e análise crítica de riscos. Tal processo é fundamentado no ciclo PDCA. A fase do processo de gestão de riscos que tem como resultado a lista de riscos residuais é:

- a) análise crítica de riscos
- b) tratamento de riscos
- c) aceitação do risco
- d) definição de risco

**PROIBIDO DESTACAR ESTA E QUALQUER
OUTRA FOLHA DOS CADERNOS DE PROVA**

ORGANIZADOR



CEPUERJ