TRIBUNAL DE CONTAS DO ESTADO DE SÃO PAULO

Concurso Público

002. PROVA OBJETIVA

AGENTE DA FISCALIZAÇÃO FINANCEIRA – INFORMÁTICA
(Área de Infraestrutura de TI e Segurança da Informação)

- Você recebeu sua folha de respostas e este caderno contendo 80 questões objetivas.
- Confira seu nome e número de inscrição impressos na capa deste caderno e na folha de respostas.
- Quando for permitido abrir o caderno, verifique se está completo ou se apresenta imperfeições. Caso haja algum problema, informe ao fiscal da sala.
- Leia cuidadosamente todas as questões e escolha a resposta que você considera correta.
- Marque, na folha de respostas, com caneta de tinta azul ou preta, a letra correspondente à alternativa que você escolheu.
- A duração da prova é de 4 horas e 30 minutos, já incluído o tempo para o preenchimento da folha de respostas.
- Só será permitida a saída definitiva da sala e do prédio após transcorridos 75% do tempo de duração da prova.
- Deverão permanecer em cada uma das salas de prova os 3 últimos candidatos, até que o último deles entregue sua prova, assinando termo respectivo.
- Ao sair, você entregará ao fiscal a folha de respostas e este caderno, podendo levar apenas o rascunho de gabarito, localizado em sua carteira, para futura conferência.
- Até que você saia do prédio, todas as proibições e orientações continuam válidas.

Aguarde a ordem do fiscal para abrir este caderno de questões.

FUNDAÇÃO vunesp
08.03.2015

LÍNGUA PORTUGUESA

Leia a charge para responder às questões de números **01** e **02**.

(*Gazeta do Povo*, 22.08.2014. Adaptado)

01. De acordo com a norma-padrão da língua portuguesa, as lacunas na fala da personagem são preenchidas, respectivamente, com:

(A) querem ... mostre-lhes

(B) quer ... mostre-os

(C) querem ... os mostrem

(D) quer ... mostre a eles

(E) querem ... lhes mostre

02. Na fala da personagem, as aspas utilizadas indicam

(A) fala de outrem.

(B) sentido figurado.

(C) discurso indireto.

(D) coloquialismo.

(E) imprecisão de sentido.

Leia o texto para responder às questões de números **03** a **08**.

Em sua essência, empresas como o Google e o Facebook estão no mesmo ramo de negócio que a Agência de Segurança Nacional (NSA) do governo dos EUA. Elas coletam uma grande quantidade de informações sobre os usuários, armazenam, integram e utilizam essas informações para prever o comportamento individual e de um grupo, e depois as vendem para anunciantes e outros mais. Essa semelhança gerou parceiros naturais para a NSA, e é por isso que eles foram abordados para fazer parte do PRISM, o programa de vigilância secreta da internet. Ao contrário de agências de inteligência, que espionam linhas de telecomunicações internacionais, o complexo de vigilância comercial atrai bilhões de seres humanos com a promessa de "serviços gratuitos". Seu modelo de negócio é a destruição industrial da privacidade. E mesmo os maiores críticos da vigilância da NSA não parecem estar pedindo o fim do Google e do Facebook.

Considerando-se que, em 1945, grande parte do mundo passou a enfrentar meio século da tirania em consequência da bomba atômica, em 2015 enfrentaremos a propagação inexorável da vigilância em massa invasiva e a transferência de poder para aqueles conectados às suas superestruturas. É muito cedo para dizer se o lado "democrático" ou o lado "tirânico" da internet finalmente vencerá. Mas reconhecê-los – e percebê-los como o campo de luta – é o primeiro passo para se posicionar efetivamente junto com a grande maioria das pessoas.

A humanidade agora não pode mais rejeitar a internet, mas também não pode se render a ela. Ao contrário, temos que lutar por ela. Assim como os primórdios das armas atômicas inauguraram a Guerra Fria, a lógica da internet é a chave para entender a iminente guerra em prol do centro intelectual da nossa civilização.

(http://noticias.uol.com.br, 16.12.2014. Adaptado)

03. De acordo com o texto, empresas como o Google e o Facebook assemelham-se a agências de inteligência, porque

(A) fortalecem a segurança dos usuários, garantindo-lhes a privacidade.

(B) exploram sem limites as informações dos usuários, oferecendo-lhes segurança.

(C) rechaçam a invasão à privacidade dos usuários, lutando para garanti-la.

(D) manipulam informações dos usuários, objetivando prever comportamentos.

(E) ignoram o comportamento dos usuários, limitando a capacidade crítica desses.

04. O texto deixa claro que

(A) a humanidade tende a render-se à internet, já que é impossível pensar criticamente em relação ao tipo de poder que está se estabelecendo com esta.

(B) a relação comercial entre as grandes empresas e os seus usuários está comprometida, pois estes não acreditam mais na promessa de serviços gratuitos.

(C) a privacidade dos usuários da internet está comprometida em razão do interesse comercial subjacente às práticas das grandes empresas.

(D) a relação das agências de vigilância cada vez mais tem se distanciado do seu papel original, ou seja, a obtenção de informações secretas.

(E) a relação de poder, hoje, é mais transparente, a ponto de agências de vigilância firmarem pactos de cooperação com empresas comerciais.

05. Nas orações – ... em 2015 enfrentaremos a propagação **inexorável** da vigilância em massa invasiva... – (segundo parágrafo) e – ... para entender a **iminente** guerra em prol do centro intelectual da nossa civilização. – (terceiro parágrafo), os termos em destaque significam, respectivamente,

(A) intermitente e fácil de se evitar.

(B) implacável e prestes a acontecer.

(C) indevida e difícil de se concretizar.

(D) inestimável e vista como imprescindível.

(E) imparcial e pronta para eclodir.

06. Leia as passagens do texto:

... e é por isso que **eles** foram abordados para fazer parte do PRISM... (primeiro parágrafo)

Seu modelo de negócio é a destruição industrial da privacidade. (primeiro parágrafo)

Ao contrário, temos que lutar por **ela**. (terceiro parágrafo)

Os pronomes em destaque referem-se, respectivamente, aos termos:

(A) os usuários / o Google e o Facebook / a humanidade.

(B) o Google e o Facebook / o complexo de vigilância comercial / a internet.

(C) os anunciantes e outros mais / as agências de inteligência / a internet.

(D) o comportamento individual e o de grupo / a NSA / a civilização.

(E) os parceiros naturais da NSA / o programa de vigilância secreta / a privacidade.

07. Assinale a alternativa em que a reescrita do trecho está em conformidade com a norma-padrão da língua portuguesa e com os sentidos do texto.

(A) Elas coletam uma grande quantidade de informações sobre os usuários, armazenam, integram e utilizam essas informações... (primeiro parágrafo)
= Elas coletam uma grande quantidade de informações relativas à seus usuários, armazenam, integram e utilizam-as...

(B) E mesmo os maiores críticos da vigilância da NSA não parecem estar pedindo o fim do Google e do Facebook. (primeiro parágrafo)
= E os mesmos maiores críticos da vigilância da NSA não parecem estar pedindo o fim do Google e do Facebook.

(C) ... em 2015 enfrentaremos a propagação inexorável da vigilância em massa invasiva e a transferência de poder... (segundo parágrafo)
= ... em 2015 a propagação inexorável da vigilância em massa invasiva e a transferência de poder, será enfrentada por nós...

(D) Mas reconhecê-los – e percebê-los como o campo de luta – é o primeiro passo para se posicionar... (segundo parágrafo)
= Portanto reconhecê-los – ou perceber eles como o campo de luta – é o primeiro passo para se posicionar...

(E) A humanidade agora não pode mais rejeitar a internet, mas também não pode se render a ela. (terceiro parágrafo)
= A humanidade agora não pode mais se render à internet nem pode rejeitá-la.

08. _____ os parceiros naturais para que _____ parte do PRISM devido _____ entre eles e a NSA no que tange _____ utilização dos dados.

De acordo com a norma-padrão da língua portuguesa, as lacunas da frase são preenchidas, respectivamente, com:

(A) Abordaram-se ... fizessem ... à semelhança ... à

(B) Abordou-se ... fizessem ... a semelhança ... da

(C) Abordaram-se ... fizesse ... a semelhança ... a

(D) Abordou-se ... fizessem ... à semelhança ... a

(E) Abordaram-se ... fizesse ... semelhança ... da

LÍNGUA INGLESA

Leia o texto para responder às questões de números **09** a **12**.

E-mail Spoofing

E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source. Distributors of spam often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations. Spoofing can be used legitimately. However, spoofing anyone other than yourself is illegal in some jurisdictions.

E-mail spoofing is possible because Simple Mail Transfer Protocol (SMTP), the main protocol used in sending e-mail, does not include an authentication mechanism. Although an SMTP service extension (specified in IETF RFC 2554) allows an SMTP client to negotiate a security level with a mail server, this precaution is not often taken. If the precaution is not taken, anyone with the requisite knowledge can connect to the server and use it to send messages. To send spoofed e-mail, senders insert commands in headers that will alter message information. It is possible to send a message that appears to be from anyone, anywhere, saying whatever the sender wants it to say. Thus, someone could send spoofed e-mail that appears to be from you with a message that you didn't write.

Although most spoofed e-mail falls into the "nuisance" category and requires little action other than deletion, the more malicious varieties can cause serious problems and security risks. For example, spoofed e-mail may purport to be from someone in a position of authority, asking for sensitive data, such as passwords, credit card numbers, or other personal information – any of which can be used for a variety of criminal purposes. One type of e-mail spoofing, self-sending spam, involves messages that appear to be both to and from the recipient.

(http://searchsecurity.techtarget.com/definition/email-spoofing. Adaptado)

09. E-mail spoofing is frequently used by

(A) illegal jurisdictions.

(B) legitimate sources.

(C) the actual mail server.

(D) spam senders.

(E) distributors from your contact list.

10. According to the text, in order to avoid spoofing, one should

(A) discontinue the SMTP as the main mail protocol.

(B) be careful to include a security level with the mail server.

(C) exclude all suspect senders from your contact list.

(D) withdraw sensitive data from mails.

(E) check the authenticity of self-sending mails.

11. In the last sentence of the second paragraph – Thus, someone could send spoofed e-mail that appears to be from you with a message that you didn't write. – the word "thus" introduces a

(A) result.

(B) comparison.

(C) contrast.

(D) purpose.

(E) exception.

12. An example of sensitive data mentioned in the last paragraph is

(A) criminal purposes.

(B) self-sending spam.

(C) malicious varieties.

(D) security risks.

(E) personal information.

MATEMÁTICA E RACIOCÍNIO LÓGICO

Matemática

13. Procurando encontrar o tom exato da cor solicitada pelo cliente, um pintor preparou uma mistura de três tintas, A, B e C. Usou certa lata como medida e misturou, em um balde, $\frac{3}{5}$ de lata de tinta A, $\frac{2}{3}$ de lata de tinta B e $\frac{4}{3}$ de lata de tinta C. Da mistura preparada, reservou uma quantidade equivalente a duas latas (medida) completamente cheias e usou totalmente o restante para pintar uma área de 6,3 m², como teste. Desse modo, é correto afirmar que, aplicada de forma idêntica à aplicada na área teste, cada lata (medida) dessa mistura permite pintar uma área igual, em m², a

(A) 12,5.

(B) 11,8.

(C) 11,4.

(D) 10,8.

(E) 10,5.

R A S C U N H O

14. O responsável pela expedição constatou que o número de caixas de um lote de certo produto era 50% maior que o número máximo de caixas que poderiam ser carregadas no veículo designado para o transporte. Providenciou, então, um segundo veículo, idêntico ao primeiro, dividiu as caixas desse lote em dois grupos de igual número, sem restar nenhuma, e colocou cada grupo de caixas em um dos veículos. Se após o carregamento restou espaço para mais 12 dessas caixas em cada veículo, então é correto afirmar que o número total de caixas carregadas nos dois veículos foi igual a

(A) 96.

(B) 88.

(C) 72.

(D) 64.

(E) 60.

15. Em um terreno retangular, cuja medida do perímetro é igual a P, a razão entre as medidas de comprimento (C) e largura (L), nessa ordem, é $\frac{5}{2}$. Desse modo, é correto afirmar que

(A) P = 2 C.

(B) P = 5 L.

(C) P = 3 C.

(D) P = 7 L.

(E) P = 5 C.

16. Para certo ambulante, o lucro (L) é dado pela diferença entre o preço de venda (PV) e o preço de compra (PC) de cada produto vendido. Se o lucro obtido em certo produto é igual a 60% do seu preço de venda, então o preço de venda desse produto é igual ao seu preço de custo aumentado em

(A) 100%.

(B) 150%.

(C) 175%.

(D) 225%.

(E) 250%.

R A S C U N H O

Raciocínio Lógico

17. Uma equivalente para a afirmação “Se Carlos foi aprovado no concurso, então ele estudou” está contida na alternativa:

(A) Carlos não foi aprovado no concurso e não estudou.

(B) Se Carlos não estudou, então ele não foi aprovado no concurso.

(C) Carlos foi aprovado no concurso e não estudou.

(D) Se Carlos não foi aprovado no concurso, então ele não estudou.

(E) Carlos estudou e não foi aprovado no concurso.

18. Se Reginaldo é agente da fiscalização ou Sérgio é professor, então Márcia é psicóloga. André é administrador se, e somente se, Carmem é dentista. Constatado que Márcia não é psicóloga e André não é administrador, conclui-se corretamente que

(A) Sérgio não é professor, Carmem não é dentista e Reginaldo não é agente da fiscalização.

(B) Sérgio é professor, mas Carmem não é dentista e Reginaldo não é agente da fiscalização.

(C) Sérgio é professor, Carmem é dentista, mas Reginaldo não é agente da fiscalização.

(D) Sérgio é professor, Reginaldo é agente da fiscalização, mas Carmem não é dentista.

(E) Sérgio é professor, Carmem é dentista e Reginaldo é agente da fiscalização.

19. Sabe-se que todos os primos de Vanderlei são funcionários públicos e que todos os primos de Marcelo não são funcionários públicos. Dessa forma, deduz-se corretamente que

(A) nenhum funcionário público é primo de Vanderlei.

(B) algum primo de Vanderlei é primo de Marcelo.

(C) nenhum primo de Vanderlei é funcionário público.

(D) algum funcionário público é primo de Marcelo.

(E) nenhum primo de Marcelo é primo de Vanderlei.

20. Sabe-se que Débora é 5 centímetros mais baixa que Antonio e 4 centímetros mais alta que Mirian. Sabe-se, também, que Eduardo é 3 centímetros mais alto que Antonio e 12 centímetros mais alto que Carlos. Se for verdadeiro que Carlos é 10 centímetros mais alto que Wilson, que mede 1,65 metro, então é correto afirmar que a altura de Antonio, em metro, será

(A) 1,82.

(B) 1,83.

(C) 1,84.

(D) 1,85.

(E) 1,86.

CONHECIMENTOS ESPECÍFICOS

21. No conjunto de protocolos TCP/IP, o IP (*Internet Protocol*) é utilizado para o endereçamento dos dispositivos de rede e o roteamento das mensagens e, para facilitar o roteamento, o endereço IP é dividido em Classes. Um endereço IPv4 é identificado como de Classe B quando, no endereço IP,

(A) o primeiro *bit* à esquerda é 0.

(B) os dois primeiros *bits* à esquerda são 1 e 0.

(C) os dois primeiros *bits* à esquerda são 1 e 1.

(D) os dois primeiros *bits* à direita são 1 e 1.

(E) os três primeiros *bits* à direita são 1, 0 e 0.

22. No padrão de endereços do protocolo IPv4, alguns endereços são reservados e não podem ser atribuídos de forma particular. Por exemplo, a placa de rede principal de um computador recebe a denominação de *localhost* e o IP:

(A) 0.0.0.0.

(B) 10.0.0.0.

(C) 127.0.0.1.

(D) 192.168.0.1.

(E) 224.0.0.1.

23. O administrador de uma rede local de computadores, que utiliza os protocolos do conjunto TCP/IP, deve configurar o *Firewall* para impedir o acesso ao serviço de *e-mail* por meio do POP3, uma vez que o único protocolo disponibilizado é o IMAP. Para isso, o administrador deve bloquear, no *Firewall*, os acessos para a Porta TCP de número

(A) 25.

(B) 110.

(C) 143.

(D) 213.

(E) 443.

24. O administrador de uma rede local de computadores deve instalar um novo *Access Point*, padrão IEEE 802.11g, em um andar da empresa com 10 salas, para melhorar a qualidade do sinal de acesso. Sabendo-se que no local já existem dois *Access Points* instalados nas extremidades do conjunto de salas, um configurado para o canal 1 e outro para o canal 6, o novo *Access Point*, a ser instalado entre os dois *Access Points*, deve ser configurado para utilizar o canal

(A) 3.

(B) 5.

(C) 8.

(D) 11.

(E) 15.

25. Após a instalação do novo *Access Point*, o administrador de uma rede local de computadores foi incumbido de atualizar o esquema de segurança de todos os *Access Points* padrão IEEE 802.11g. Considerando o WPA e o WPA2, o administrador deve escolher o

(A) WPA2 devido à maior segurança oferecida pelo uso do AES.

(B) WPA2 devido ao melhor algoritmo de segurança utilizado, que é o RC4.

(C) WPA2 devido ao menor tempo de processamento requerido se comparado com o WPA.

(D) WPA devido ao maior tamanho permitido para a chave se comparado ao WPA2.

(E) WPA, pois utiliza o esquema de chaves dinâmicas enquanto o WPA2 utiliza o esquema de chaves fixas.

26. Na arquitetura do protocolo SNMP (*Simple Network Management Protocol*) para a gerência de redes de computadores, o subagente

(A) é instalado nos dispositivos monitorados e tem a função de responder às requisições do gerente.

(B) é instalado junto ao sistema gerente e tem a função de atuar em caso de falha do agente principal.

(C) é parte do agente principal e tem a função de analisar as informações da rede.

(D) é parte do agente principal e tem a função de hierarquizar as ações do gerente.

(E) trafega pela rede, ou seja, entre os roteadores, para coletar as informações de todos os dispositivos.

27. O MPLS (*Multiprotocol Label Switching*) é um protocolo eficiente para a transmissão de dados em diferentes tecnologias de rede de comunicação. Diferentemente do processo de roteamento de pacotes realizado no protocolo IP, o roteamento dos pacotes MPLS é realizado pelo(a)

(A) *Firewall*.

(B) *Gateway*.

(C) *Proxy*.

(D) *Router*.

(E) *Switch*.

28. Para melhorar a segurança de uma rede local de computadores (LAN), é possível utilizar o serviço NAT (*Network Address Translation*), que não expõe o computador da LAN para acesso externo direto. Na estrutura do NAT, o relacionamento entre o computador da LAN e a mensagem gerada por esse computador e enviada para a WAN é realizado por meio da informação inserida

(A) em um cabeçalho adicional do IPSec.

(B) no campo Porta destino do TCP.

(C) no campo Porta origem do TCP.

(D) no campo Type do *frame* Ethernet.

(E) no espaço reservado Options do IP.

29. Em uma VPN (*Virtual Private Network*) implementada por meio do IPSec,

(A) é inserido, após o cabeçalho do *frame* IP original, o campo AH para o processo de autenticação.

(B) é inserido, após o *frame* IP original, um campo de autenticação (ESP) e checagem de todo o *frame*.

(C) o *frame* IP original recebe um cabeçalho de autenticação e o novo *frame* é criptografado por completo.

(D) o *frame* IP original, que inclui o cabeçalho IP e os dados, é criptografado.

(E) os dados são criptografados, mas o cabeçalho IP original é mantido para a identificação pelos roteadores.

30. Dentre os tipos de *malwares*, o *spyware* se caracteriza por

(A) capturar as teclas digitadas no computador infectado e enviar as informações para o invasor.

(B) explorar falhas do sistema operacional para controlar o computador infectado.

(C) permitir o acesso contínuo ao computador infectado.

(D) propagar-se automaticamente pela rede enviando cópias para outros computadores.

(E) monitorar as atividades de um sistema e enviar as informações coletadas para o invasor.

31. As diferentes técnicas de criptografia são utilizadas para aumentar a segurança da troca de informações pela rede de computadores. No acesso às páginas *Web* de forma segura, utilizando o HTTPS, a criptografia utilizada para o acesso aos dados possui o esquema de chave

(A) assimétrica devido à não necessidade da troca de chave com o usuário.

(B) assimétrica devido à maior velocidade para criptografar se comparado com a simétrica.

(C) simétrica devido à maior segurança do algoritmo de criptografia se comparada com a assimétrica.

(D) simétrica, pois utiliza chave de maior tamanho, sendo assim mais seguro que a assimétrica.

(E) simétrica, pois utiliza a mesma chave para criptografar e descriptografar o dado.

32. Existem diferentes tipos de ataques de *hackers* por meio das redes de computadores. Nesse contexto, o ataque no qual vários computadores realizam requisições ou enviam pacotes mal formados para um sistema pela rede é denominado

(A) DoS.

(B) DDoS.

(C) Flooding.

(D) Phishing.

(E) Spoofing.

33. Embora um servidor DNS seja solicitado para a instalação do Active Directory, esta função

(A) apenas é necessária se o Active Directory for operar em uma floresta com mais de um controlador de domínio.

(B) deve obrigatoriamente ser oferecida por um servidor externo, que não esteja associado à rede ou ao domínio.

(C) já está inclusa no Active Directory como parte do protocolo LDAP.

(D) pode ser substituída por um servidor WINS.

(E) pode ser atribuída à mesma máquina na qual o controlador de domínio for instalado.

34. Nos sistemas operacionais Windows, um dos protocolos suportados nativamente para o compartilhamento de impressoras pela rede é o

(A) FTP.

(B) LDAP.

(C) HTTP.

(D) SMB.

(E) SSH.

35. Nos sistemas operacionais Linux, o diretório raiz do sistema é identificado pelo caractere

(A) \ (barra inclinada para a esquerda).

(B) / (barra inclinada para a direita).

(C) $ (sinal de dólar).

(D) # (cerquilha).

(E) : (dois pontos).

36. Observe as permissões de um arquivo apresentadas em um terminal Linux:

```
-r--r--rw- 1 joao admin 14 Jan 20 20:47 arq.ext
```

Se um usuário tentar alterar esse arquivo, a alteração será

(A) aceita, desde que não seja feita pelo usuário "joao" ou por algum membro do grupo "admin".

(B) aceita, pois o arquivo permite que qualquer usuário faça alterações nele, incluindo o usuário "joao" e membros do grupo "admin".

(C) negada, exceto se for feita pelo usuário "joao".

(D) negada, exceto se for feita por um membro do grupo "admin".

(E) negada, pois o arquivo não permite que qualquer usuário do sistema faça alterações nele.

37. O modelo de negócio de Computação em Nuvem em que o cliente tem acesso completo às máquinas (físicas ou virtuais) podendo, inclusive, alterar seu sistema operacional, é chamado de

(A) Disco como Serviço (DaaS).

(B) Dispositivo como Serviço (DaaS).

(C) Infraestrutura como Serviço (IaaS).

(D) Plataforma como Serviço (PaaS).

(E) Software como Serviço (SaaS).

38. O comando para alterar o diretório corrente no *prompt* de comando do Windows e no terminal do Linux é:

(A) `cd`.

(B) `ls`.

(C) `dir`.

(D) `pwd`.

(E) `md`.

39. Considere o conteúdo do arquivo texto.txt apresentado a seguir:

```
1 azeite
2 trigo
3 feijão
4 uva
```

Se o comando

```
"grep [2-4] texto.txt | grep -v uva"
```

for executado no Linux para listar o conteúdo deste arquivo, será apresentado no terminal:

(A)
```
2 trigo
```

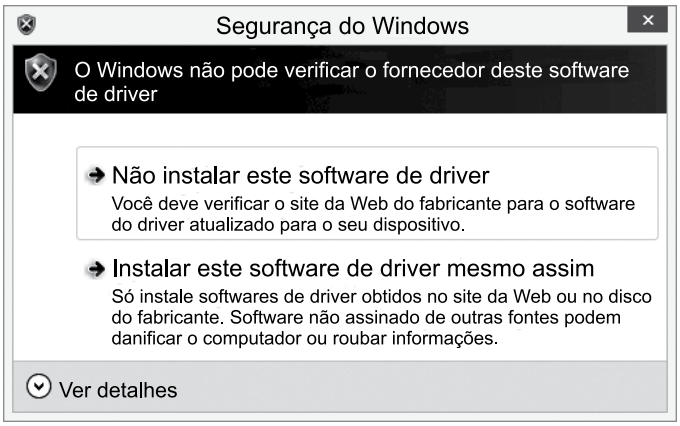
(B)
```
4 uva
```

(C)
```
2 trigo
3 feijão
```

(D)
```
1 azeite
2 trigo
3 feijão
```

(E)
```
2 trigo
3 feijão
4 uva
```

40. Durante a instalação de um *driver* em um computador executando o Windows, um administrador recebeu a seguinte mensagem:



Essa mensagem apareceu porque

(A) o computador está infectado com vírus.

(B) o dispositivo correspondente ao *driver* não está conectado no computador.

(C) o *driver* está desatualizado.

(D) o *driver* não possui uma assinatura digital válida.

(E) não é possível acessar a Internet para verificar o fornecedor do *driver*.

41. Um usuário notou que, no Windows 7, os diretórios "C:\Program Files" e "C:\Arquivos de Programas" o direcionavam para o mesmo diretório no sistema de arquivos. O recurso do sistema de arquivos NTFS que permite esse direcionamento é o(a)

(A) *Hardlink*.

(B) *Junction point*.

(C) *Registered alias*.

(D) *Soft folder*.

(E) *United data*.

42. Para alterar o nome que identifica o computador na rede, em uma estação Windows 7, deve-se acessar as configurações pelo caminho:

(A) Painel de Controle > Aparência e Personalização > Personalização > Nome do computador.

(B) Painel de Controle > Sistema e Segurança > Sistema > Configurações avançadas do sistema > Nome do computador.

(C) Painel de Controle > Sistema e Segurança > Central de Ações > Manutenção > Nome do computador.

(D) Painel de Controle > Hardware e Sons > Configurações avançadas do sistema > Nome do computador.

(E) Painel de Controle > Relógio, Idioma e Região > Região e Idioma > Configurações avançadas > Nome do computador.

43. Um dos meios de otimizar o desempenho dos sistemas *Web* é empregando mecanismos que comprimam os dados antes da transmissão. Embora eles proporcionem uma redução no tempo de transmissão, é possível afirmar que esses mecanismos também necessitam

(A) de capacidade para gerenciar um número maior de conexões, que é um efeito inerente ao processo de compressão.

(B) de um maior espaço em disco para armazenar os dados comprimidos.

(C) de uma largura de banda maior, pois as transmissões de dados comprimidos são mais custosas.

(D) de uma maior capacidade de processamento para a preparação e utilização dos dados.

(E) que a taxa de transferência dos dados seja aumentada, devido ao aumento de eficiência do servidor.

44. Algumas tecnologias *Web*, como o Java EE, são mais adequadas para realizar acesso a bases de dados do que outras tecnologias, como o JavaScript ou jQuery, por exemplo. Essa característica se dá principalmente porque o Java EE é uma tecnologia que atua do lado do

(A) cliente e, por ser uma linguagem compilada, os dados são processados com maior agilidade do que linguagens interpretadas.

(B) cliente e, por isso, garante a redução do volume de dados a serem processados no servidor ou na base de dados.

(C) servidor e, por isso, oferece a possibilidade de ocultar as informações de acesso às bases de dados do cliente.

(D) servidor e, por isso, é capaz de proporcionar maior capacidade de processamento, o que reduz a carga na base de dados.

(E) servidor, que é o único capaz de gerir otimizações no programa e diminuir o volume de dados transmitidos para a base de dados.

45. No Java EE, o ciclo de vida de um *servlet* é encerrado após a chamada do método

(A) delete.

(B) destroy.

(C) finish.

(D) service.

(E) terminate.

46. Dentre os servidores de aplicação compatíveis com o Java EE 7 disponíveis, incluem-se os seguintes:

(A) Apache, IIS e Tomcat.

(B) Django, Joomla e Drupal.

(C) GlassFish, WildFly e JEUS.

(D) Jetty, Mono e Zope.

(E) Zend, Node.js e Mongrel.

47. No Java EE, um *Servlet* é um objeto cuja função primária é

(A) armazenar informações sobre a sessão dos clientes.

(B) conectar a aplicação a uma base de dados.

(C) gerenciar a memória do servidor.

(D) oferecer persistência de dados ao servidor de aplicação.

(E) receber requisições do cliente e produzir respostas com base nelas.

48. Em um sistema gerenciador de bancos de dados, o principal objetivo de se utilizar a técnica de *fail-over* é

(A) criar um *trigger* de restauração do banco de dados a ser acionado antes da ocorrência de uma falha.

(B) duplicar a estrutura de indexação de cada tabela presente no banco de dados.

(C) excluir os registros das tabelas que possuam valores nulos.

(D) substituir o nome das tabelas presentes no banco de dados por nomes padronizados.

(E) manter o funcionamento do sistema na ocorrência de falhas no servidor originalmente designado como o servidor principal.

49. Considerando a replicação de estado em sistemas gerenciadores de bancos de dados, na replicação do tipo passiva há um gerenciador de réplica (I) que trata os pedidos de dados, comunicando-se com os demais gerenciadores (II). Os gerenciadores identificados com I e II são denominados, respectivamente,

(A) básico e complementar.

(B) inicial e final.

(C) parcial e completo.

(D) primário e *backup*.

(E) único e múltiplo.

50. Em sistemas gerenciadores de bancos de dados relacionais, uma das técnicas largamente utilizadas para a otimização de desempenho consiste no(na)

(A) limitação no número de campos de cada tabela do banco de dados.

(B) proibição da inserção de valores nulos nos registros das tabelas.

(C) uso extensivo de *triggers* ou gatilhos para a realização de procedimentos.

(D) criação de grupos de usuários, com características semelhantes, do banco de dados.

(E) criação de índices sobre alguns campos das tabelas do banco de dados.

51. Consultas SQL são submetidas a sistemas gerenciadores de bancos de dados. Nesses gerenciadores, por sua vez, as consultas são submetidas a um módulo compilador de consultas SQL. A função básica desse módulo compilador é

(A) eliminar consultas anteriores ainda armazenadas na memória do computador.

(B) gerar mensagens de uso do banco de dados ao DBA do sistema.

(C) limpar a pilha de requisições feitas pelos usuários do sistema.

(D) transformar as consultas em um formato compatível com a estrutura interna do sistema gerenciador.

(E) verificar se não há mensagens de erro geradas pelo servidor de banco de dados.

52. Considerando o uso de sistemas gerenciadores de bancos de dados, podem ser utilizadas arquiteturas paralelas, visando, por exemplo, um incremento do desempenho no uso dos bancos de dados. Um fator importante de medição de computadores utilizados em arquiteturas paralelas é o fator denominado *throughput*, que representa o

(A) número de tarefas que podem ser completadas em um determinado intervalo de tempo.

(B) número de processos possíveis de serem executados em paralelo, de forma simultânea.

(C) tamanho médio de cada banco de dados utilizado.

(D) tamanho médio de cada tabela presente no banco de dados.

(E) tempo máximo para a inserção de um registro no banco de dados.

53. O nível RAID que corresponde a uma cópia de espelho de todos os dados do disco principal em um segundo disco, sem informações de paridade, é o nível

(A) 0.

(B) 1.

(C) 3.

(D) 4.

(E) 5.

54. Embora o RAID 0 (zero) seja o nível com maior aproveitamento de espaço de armazenamento em relação a outros níveis RAID, ele

(A) exige que sejam calculadas informações de paridade para todos os dados salvos.

(B) possui baixo desempenho de leitura.

(C) possui baixo desempenho de gravação.

(D) não oferece tolerância a falhas.

(E) não pode ser associado a outros níveis RAID.

55. A topologia do *Fibre Channel* para a implantação de Redes de Área de Armazenamento (SAN), que se caracteriza por ter seus dispositivos conectados em forma de anel, é chamada de

(A) barramento.

(B) estrela.

(C) *loop* arbitrado.

(D) malha comutada.

(E) ponto a ponto.

56. Dentre as diversas tecnologias de armazenamento disponíveis, algumas oferecem acesso direto ao dispositivo de armazenamento e, portanto, requerem que o cliente estabeleça um sistema de arquivos. Dentre as tecnologias que possuem essa capacidade, estão incluídas:

(A) AFS, IDE e SCSI.

(B) FTP, IDE e SATA.

(C) FCoE, NFS e SATA.

(D) SATA, SFTP e SMB.

(E) IDE, Fibre Channel e iSCSI.

57. Na execução de um *backup* incremental, é feita uma cópia de segurança

(A) apenas dos arquivos alterados desde o último *backup*.

(B) apenas dos arquivos criados desde o último *backup*.

(C) de todos os arquivos dos discos selecionados.

(D) dos arquivos apagados desde o último *backup*.

(E) dos arquivos criados e alterados desde o último *backup*.

58. Um sistema de armazenamento diretamente conectado ao dispositivo que não possui a atuação de componentes de rede entre eles é denominado

(A) DAS.

(B) LAN.

(C) MAN.

(D) NAS.

(E) SAN.

59. Em um arranjo RAID 6 com 10 discos, pode haver falha simultânea em até

(A) 2 discos.

(B) 3 discos.

(C) 4 discos.

(D) 5 discos.

(E) 6 discos.

60. Uma empresa verificou que a norma NBR ISO/IEC 27002:2013 define como se deve proceder na questão da segurança ligada a recursos humanos. A norma estabelece, em um de seus capítulos, que os recursos humanos devem ter um acompanhamento

(A) apenas antes e após o término do vínculo contratual.

(B) apenas antes e durante o vínculo contratual.

(C) apenas durante a vigência do período contratual.

(D) apenas durante e após o término do vínculo contratual.

(E) antes, durante e após o término do vínculo contratual.

61. Na norma NBR ISO/IEC 27001:2013, no item que trata do estabelecimento de um sistema de gestão da segurança da informação (SGSI), há a indicação da necessidade da fase de identificação dos riscos. Uma das atividades contempladas nessa fase é:

(A) aplicar as ações corretivas preconizadas no plano de recuperação de desastres.

(B) determinar a aceitação ou não dos riscos pelos usuários do sistema.

(C) estimar os níveis de risco presentes.

(D) identificar os riscos e seus responsáveis.

(E) transferir os riscos identificados para outros sistemas similares.

62. A norma NBR ISO/IEC 27002:2013 recomenda que seja feita a classificação das informações, proporcionando um nível adequado de proteção. Essa recomendação faz parte da etapa ou seção de

(A) controle de acessos.

(B) gestão de ativos.

(C) gerenciamento das operações e comunicações.

(D) gestão de incidentes da segurança da informação.

(E) segurança física e do ambiente.

63. A norma NBR ISO/IEC 15999:2007 prevê um Plano de Gerenciamento de Incidentes (PGI). Esse plano está inserido no seguinte elemento do ciclo de vida da Gestão de Continuidade de Negócios:

(A) Desenvolvendo e implementando uma resposta de GCN.

(B) Determinando a estratégia de continuidade dos negócios.

(C) Entendendo a organização.

(D) Gestão de programa de GCN.

(E) Incluindo a GCN na cultura da organização.

64. O ciclo de vida da Gestão de Continuidade de Negócios (GCN) da norma NBR ISO/IEC 15999:2007, em seu elemento Gestão de Programa de GCN, inclui os seguintes 3 passos:

(A) análise de impacto no negócio, opções de estratégia e atribuição de responsabilidade.

(B) atribuição de responsabilidade, implementação da continuidade de negócio na organização e gestão contínua da continuidade de negócios.

(C) determinação de escolhas de fornecedores, análise de impacto nos negócios e determinação de requisitos de contingência.

(D) determinação de requisitos de contingência, definição de técnicas de gestão e aquisição de suprimentos.

(E) identificação de atividades críticas, seleção de pessoal e gestão contínua da continuidade de negócios.

65. A norma NBR ISO/IEC 27005:2011 estabelece a correspondência entre processos de um Sistema de Gestão de Segurança da Informação (SGSI) e processos de gestão de riscos da segurança da informação. Assinale a alternativa que contém uma correspondência correta entre os dois tipos de processos.

(A) Agir – implementação do plano de tratamento de risco.

(B) Executar – aceitação do risco.

(C) Executar – análise/avaliação de riscos.

(D) Planejar – plano de tratamento de risco.

(E) Verificar – definição do contexto.

66. Segundo a norma NBR ISO/IEC 27005:2011, considerando uma iteração completa do processo de gestão de riscos, são previstas as seguintes atividades (não necessariamente na ordem correta de execução):

I. Tratamento de riscos
II. Análise de riscos
III. Identificação de riscos
IV. Aceitação de riscos
V. Avaliação de riscos

Considerando uma sequência direta na execução dessas atividades, sem pontos de retorno intermediários, a ordem correta de execução dessas 5 atividades é:

(A) I, IV, V, III e II.

(B) II, III, IV, V e I.

(C) III, II, V, I e IV.

(D) IV, III, V, II e I.

(E) V, I, II, IV e III.

67. No PMBOK 5ª edição há um grupo de processos que visam finalizar as atividades de projetos, verificando se tais projetos foram completados em todos os grupos de processos. O grupo de processos citado inicialmente corresponde à(ao)

(A) execução.

(B) encerramento.

(C) iniciação.

(D) monitoração e controle.

(E) planejamento.

68. O PMBOK 5ª edição abrange diversos processos que são agrupados nos chamados grupos de gerenciamento de processos. Sobre esses processos e seus grupos de gerenciamento, é correto afirmar que o processo

(A) controlar a comunicação faz parte do grupo de processos de planejamento.

(B) planejar o gerenciamento dos custos faz parte do grupo de processos de iniciação.

(C) orientar e gerenciar o trabalho do projeto faz parte do grupo de processos de execução.

(D) sequenciar as atividades faz parte do grupo de processos de monitoramento e controle.

(E) validar o escopo faz parte do grupo de processos de encerramento.

69. O PMBOK 5ª edição define 3 tipos de escritórios de gerenciamento de projetos. Dentre eles há um tipo que visa assumir o controle dos projetos, realizando seu gerenciamento direto. Tal tipo de escritório recebe a denominação de

(A) diretivo.

(B) informal.

(C) parcial.

(D) provisório.

(E) suporte.

70. Assinale a alternativa que contém a afirmação correta sobre documentos de entrada e saída e seu relacionamento com as áreas de conhecimento, segundo o PMBOK 5ª edição.

(A) O documento Estimativa de Duração das Atividades é uma entrada do processo Controlar o Escopo.

(B) O documento Plano de Gerenciamento das Aquisições é uma saída do processo Conduzir as Aquisições.

(C) O documento Plano de Gerenciamento de Riscos é uma entrada do processo Planejar o Gerenciamento das Comunicações.

(D) O documento Registro das Questões é uma entrada do processo Controlar os Riscos.

(E) O documento Termo de Abertura de Projeto é uma entrada do processo Identificar as Partes Interessadas.

71. O PMBOK 5ª Edição estabelece uma classificação de recursos e pessoas participantes de projetos, baseada na estrutura organizacional desses projetos. Segundo essa classificação,

(A) a autoridade do gerente de projeto é baixa, considerando uma estrutura matricial fraca da organização.

(B) a disponibilidade de recursos é alta, considerando uma estrutura matricial fraca da organização.

(C) a disponibilidade de recursos é baixa, considerando uma estrutura projetizada da organização.

(D) o gerente de projetos é de tempo parcial, considerando uma matricial forte da organização.

(E) o gerente funcional é o responsável por gerenciar o orçamento do projeto, considerando uma estrutura projetizada da organização.

72. A publicação Estratégia de Serviços do ITIL v3 define recursos que os provedores de serviço devem possuir. Dentre tais recursos estão:

(A) Organização e Pessoas.

(B) Conhecimento e Organização.

(C) Infraestrutura e Informação.

(D) Pessoas e Gerenciamento.

(E) Processos e Aplicações.

73. A publicação Estratégia de Serviços do ITIL v3 apresenta algumas medidas relacionadas ao impacto dos negócios. As medidas que dizem respeito à confiabilidade e manutenibilidade, conforme apontadas pelo ITIL v3, são, respectivamente,

(A) CMDB (*Configuration Management DataBase*) e ITSM (*IT Service Management*).

(B) LOS (*Line of Service*) e FTA (*Fault Tree Analysis*).

(C) LOS (*Line of Service*) e RACI (*Responsible Accountable Consulted and Informed*).

(D) MTBF (*Mean Time Between Failures*) e MTRS (*Mean Time to Restore*).

(E) RACI (*Responsible Accountable Consulted and Informed*) e CMDB (*Configuration Management DataBase*).

74. A publicação Desenho de Serviços do ITIL v3 estabelece algumas opções de modelos de fornecimento de serviços (*delivery*), dentre os quais se encontram

(A) *agreement* e *multi-sourcing*.

(B) *assembly* e *co-sourcing*.

(C) *capability* e ASP (*Application Service Provider*).

(D) *control* e *no-sourcing*.

(E) *insourcing* e *outsourcing*.

75. A publicação Transição de Serviços do ITIL v3 define os chamados 7 Rs (na língua inglesa) do Gerenciamento de Mudanças. Dois desses Rs que também correspondem a Rs na língua portuguesa são:

(A) Rota e Relação.

(B) Ramificação e Riscos.

(C) Razão e Recursos.

(D) Replicação e Retorno.

(E) Resposta e Responsável.

76. Na publicação Operação de Serviços do ITIL v3, consta o Gerenciamento de Incidentes, que contempla as seguintes atividades (não necessariamente na ordem correta):

I. Escalação	V. Investigação e Diagnóstico
II. Fechamento	VI. Categorização
III. Priorização	VII. Diagnóstico Inicial
IV. Registro	VIII. Resolução e Recuperação

A ordem correta para a execução dessas atividades é:

(A) III, VII, VIII, I, VI, IV, V e II.

(B) IV, VI, III, VII, I, V, VIII e II.

(C) V, VIII, I, III, IV, VI, VII e II.

(D) VII, III, IV, VIII, I, VI, V e II.

(E) VIII, VII, V, VI, I, III, IV e II.

77. O COBIT 5 identifica, dentre as necessidades de *stakeholders* (partes interessadas), a criação de valor como objetivo de governança de TI. Dentre os objetivos identificados para essa criação de valor, o COBIT cita diretamente o(a)

(A) aumento do número de funcionários.

(B) contratação de consultoria especializada.

(C) otimização de recursos.

(D) uso de mecanismos de criptografia.

(E) uso de *software* proprietário.

78. O COBIT 5 estabelece alguns objetivos corporativos e outros objetivos de TI. Os números desses objetivos são, respectivamente,

(A) 15 e 16.

(B) 16 e 16.

(C) 16 e 17.

(D) 17 e 17.

(E) 17 e 18.

79. O processo denominado, no COBIT 5, Gerenciar a Segurança está inserido no grupo

(A) Alinhar, Planejar e Organizar.

(B) Avaliar, Dirigir e Monitorar.

(C) Construir, Adequar e Implementar.

(D) Entregar, Prestar Serviços e Fornecer Suporte.

(E) Monitorar, Avaliar e Analisar.

80. O COBIT 5 define um ciclo de vida de implementação no qual há 3 componentes:

(A) Definição de Elementos Responsáveis, Catalogação de Serviços e Análise de Qualidade.

(B) Definição de Elementos Responsáveis, Definição de Métricas e Catalogação de Serviços.

(C) Definição de Métricas, Gestão de Ciclo Econômico e Capacitação de Mudanças.

(D) Implementação de Serviços, Gestão de Ciclo Econômico e Melhoria Contínua.

(E) Melhoria Contínua, Capacitação de Mudanças e Gestão do Programa.