Pontifícia Universidade Católica do Paraná
Concurso Público da Companhia Paranaense de Energia - COPEL

COPEL

24 de Janeiro de 2010

CARGO Nº 18

ANALISTA DE SUPORTE TÉCNICO JÚNIOR

Atuação: Analista de Segurança da Informação

N.º DO CARTÃO

NOME (LETRA DE FORMA)

ASSINATURA

INFORMAÇÕES / INSTRUÇÕES:

1. Verifique se a prova está completa: questões de números 1 a 50 e 1 redação.
2. A compreensão e a interpretação das questões constituem parte integrante da prova, razão pela qual os fiscais não poderão interferir.
3. Preenchimento do **Cartão-Resposta**:
   - Preencher para cada questão apenas uma resposta
   - Preencher totalmente o espaço ▭ correspondente, conforme o modelo: ■
   - Usar caneta esferográfica, escrita normal, tinta azul ou preta
   - Para qualquer outra forma de preenchimento, a leitora anulará a questão

O CARTÃO-RESPOSTA É PERSONALIZADO.
NÃO PODE SER SUBSTITUÍDO, NEM CONTER RASURAS.

Duração total da prova: 4 horas e 30 minutos

Anote o seu gabarito.

1.	2.	3.	4.	5.	6.	7.	8.	9.	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.

CONHECIMENTOS ESPECÍFICOS E GERAIS

1. Para a operação correta de uma rede TCP/IP, é necessária a disponibilização de uma série de entidades lógicas e físicas. Dentre essas, está uma entidade que recebe o nome de *gateway* em função do seu papel desempenhado. A respeito dela, analise as afirmativas mostradas a seguir:

I. Um roteador pode ser visto como um *gateway*, pois normalmente ele é um nó da rede que tem por função interligar computadores que estão em redes distintas.
II. O uso dos *gateways* para computadores de uma rede local ligados por meio de um *switch* é indispensável para que a comunicação entre eles possa ocorrer de modo satisfatório.
III. Para que uma estação da rede possa acessar a Internet, ela precisa de um *gateway*, o qual pode ser configurado estaticamente ou dinamicamente.
IV. Para que um equipamento desempenhe o papel de *gateway,* ele precisa necessariamente de *hardware* especializado, uma vez que tal função demanda uma série de recursos, os quais estão indisponíveis em computadores convencionais.

As afirmações **VERDADEIRAS** são:

A) I, II e IV.
B) I, II e IV.
C) III e IV.
D) II e III.
E) I e III.

2. Um dos principais conceitos envolvidos na operação das redes TCP/IP é o processo de encapsulamento. A respeito desse processo, analise as afirmativas mostradas a seguir:

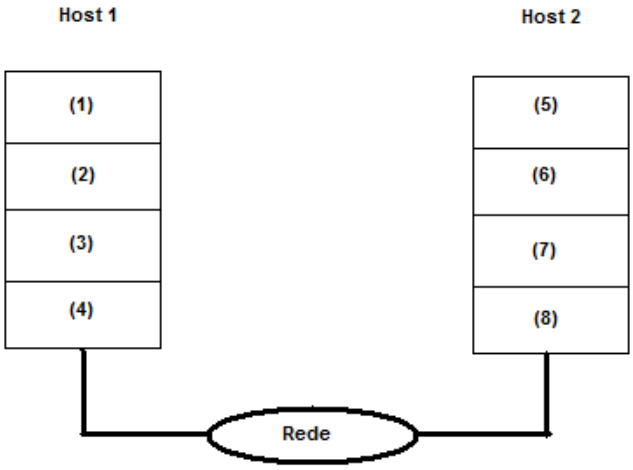
I. Permite estabelecer caminhos livres de erros ao longo dos *hosts* envolvidos na comunicação.
II. Permite a criação de *logs* do tráfego de pacotes entre os *hosts* envolvidos na comunicação.
III. Permite identificar partes distintas dos dados como sendo participantes da mesma comunicação entre *hosts*.
IV. Permite associar partes distintas dos dados para suas respectivas entidades de recebimento.

As afirmações **VERDADEIRAS** são:

A) III e IV.
B) I, II e IV.
C) II e IV.
D) II e III.
E) I e III.

3. A figura abaixo (figura A) apresenta um cenário de uma rede formada por dois *hosts* interligados por redes *Ethernet* e TCP/IP. Cada número corresponde a uma camada da arquitetura TCP/IP. Considere esta figura para responder às questões 3, 4 e 5.

Figura A



Assinale qual das alternativas abaixo apresenta uma afirmação **CORRETA** a respeito do cenário apresentado na figura em questão (figura A).

A) Um protocolo de comunicação é utilizado para comunicação entre camadas, como, por exemplo, entre (2) e (3).
B) Um protocolo de comunicação é utilizado para comunicação entre camadas, como, por exemplo, entre (2) e (6).
C) As camadas (3)/(7) e (2)/(6) indicam para este cenário, respectivamente, o *Ethernet* e o protocolo IP.
D) A rede apresentada na figura pode ser considerada genérica quanto à sua composição, podendo ser uma rede local, ponto-a-ponto ou uma rede de longa distância.
E) A sequência transmitida na rede, após o encapsulamento, será (3)(2)(1); nela dizemos que a camada mais à esquerda encapsulou aquela citada à sua direita.

4. Suponha que no *Host* 2 da figura A (contido na questão anterior, questão 3) fosse instalado um servidor WEB (isto é, um serviço baseado no protocolo Http) com LINUX. Também, suponha que no *Host* 1 tenha sido instalado o sistema operacional *Windows* e um *browser* qualquer. A sequência que representa **CORRETAMENTE** os protocolos e camadas de um acesso do *browser* a uma página mantida no servidor WEB nas interfaces de redes correspondentes é:

A) (1)-ETHERNET,(2)-ICMP,(3)-IP,(4)-HTTP,(5)-ETHERNET,(6)-ICMP,(7)-IP,(8)-HTTP
B) (1)-ETHERNET,(2)-IP,(3)-TCP,(4)-HTTP,(5)-ETHERNET,(6)-IP,(7)-TCP,(8)-HTTP
C) (1)-HTTP,(2)-TCP,(3)-IP,(4)-ETHERNET,(5)-HTTP,(6)-TCP,(7)-IP,(8)- ETHERNET
D) (1)-HTTP,(2)-IP,(3)-TCP,(4)-ADSL,(5)-HTTP,(6)-IP,(7)-TCP,(8)-ADSL
E) (1)-HTTP,(2)-TCP,(3)-ICMP,(4)-ETHERNET,(5)-HTTP,(6)-TCP,(7)-ICMP,(8)- ETHERNET

5. Suponha que a Rede indicada na figura A (contida na questão 3) tenha sido implementada apenas utilizando um HUB *ethernet*. Assinale a alternativa abaixo que apresenta uma afirmação **VERDADEIRA** acerca desse cenário.

A) A comunicação no cenário indicado não possui controle de recebimento de dados no nível das camadas (4) e (8), uma vez que o meio é considerado confiável, com baixos níveis de perdas de quadros.
B) O cenário indicado está incorreto, pois o protocolo *Ethernet,* no contexto apresentado, dependeria das funcionalidades de um *switch* para sua correta operação.
C) A entidade de interconexão das máquinas utiliza endereços físicos, também conhecidos como endereços *MAC*, para promover a segmentação da rede envolvendo as duas máquinas.
D) Considerando que a rede tenha apenas os hosts 1 e 2 conectados, podemos assumir que ela apresenta dois domínios de colisão, um para cada porta do *HUB*.
E) Considerando que a rede tenha apenas os *hosts* 1 e 2 conectados, ela pode operar nos modos *half duplex* ou *full duplex*, dependendo de como o dispositivo de interconexão foi configurado.

6. Nas arquiteturas dos sistemas computacionais, podemos encontrar uma grande diversidade de dispositivos periféricos. Para implementar o acesso a esses dispositivos, os sistemas operacionais usam uma série de interfaces, as quais variam em termos de desempenho e custo. A respeito dessas interfaces, assinale abaixo a alternativa que apresenta uma afirmação **CORRETA**.

A) A interface *FibreChannel* tem se apresentado como importante interface para interconexão entre equipamentos em ambientes sem fio.
B) A interface ATA permite maiores taxas de transferência quando comparada com a interface IDE; no entanto, possui menores taxas quando comparadas com a interface serial ATA.
C) Interfaces utilizadas em dispositivos orientados a caráter se baseiam na transferência de dados em blocos.
D) A interface *DMA* permite o *upload* e o *download* de configurações diretamente à memória de configuração de um dispositivo periférico, facilitando enormemente o processo de manutenção e operação dos mesmos.
E) Recentemente, a arquitetura de barramento EISA tem merecido mais destaque no projeto de placas de sistemas computacionais pela sua capacidade de facilitar a padronização de interfaces entre arquiteturas heterogêneas.

7. Nas arquiteturas de sistemas computacionais, é típico o uso de mecanismos que visam dar maior proteção aos dados quando ocorrem falhas de *hardware*. Neste contexto, os sistemas RAID se apresentam como uma estratégia comumente empregada. A respeito das possibilidades de configuração do RAID, assinale a alternativa que apresenta uma afirmação **CORRETA**.

A) A configuração RAID 2 é o nome dado ao que se conhece como espelhamento de disco através do qual há uma duplicação total dos dados e, portanto, alto consumo de recursos de armazenamento.
B) A configuração RAID 0, apesar de ser a mais cara, é aquela que fornece maior nível de redundância dos dados e, portanto, é considerada a mais segura.
C) A configuração RAID 1 combina vários discos de forma a proteger os dados contra as falhas de qualquer um deles. A tolerância a faltas é alcançada por meio do armazenamento de informações de paridade em um disco extra.
D) A configuração RAID 3 combina vários discos de forma a proteger os dados contra as falhas de qualquer um deles. A tolerância a faltas é alcançada por meio do armazenamento de informações de paridade ao longo dos próprios discos que compõem o sistema RAID.
E) É possível combinar alguns sistemas RAID básicos para criar RAID híbridos utilizando características dos sistemas que foram combinados.

8. As chamadas de sistema (*system calls*) desempenham um papel importante no contexto da operação dos sistemas operacionais. A respeito delas, é **CORRETO** afirmar:

A) São usadas para permitir o acesso a serviços oferecidos pelo sistema operacional, os quais, tipicamente, requerem acesso privilegiado, não sendo permitido o acesso direto sem a intermediação do sistema operacional.
B) São usadas por um dispositivo periférico para notificar um evento ocorrido no sistema. Por exemplo, quando chega um pacote de rede, a interface de rede emite uma chamada do sistema para avisar o sistema operacional que isto aconteceu.
C) São usadas pela CPU para notificar que um evento de exceção ocorreu. Por exemplo, quando ocorre uma divisão por zero, a primeira coisa que CPU faz é notificar o SO por meio de uma chamada de sistema específica.
D) São chamadas internas do próprio sistema operacional que permitem aos módulos do núcleo do sistema trocar mensagens entre si.
E) Mensagens específicas são emitidas por uma aplicação para avisar ao sistema operacional que ela está parada devido ao bloqueio ocorrido pela falta de acesso a um recurso compartilhado.

9. Nos servidores LINUX, tipicamente, é habilitado um conjunto de serviços para suprir as necessidades dos usuários. Como exemplo, podemos citar os serviços de transferência de arquivos, acesso remoto seguro, entre outros. A respeito deles, é **CORRETO** afirmar:

A) O serviço DNS fornece o suporte à configuração de máquinas, o qual permite a alocação de endereços IP, *gateway* padrão, entre outras informações.
B) O serviço TELNET utiliza o protocolo TCP para prover o acesso remoto através de uma sessão segura criptografada.
C) A transferência de arquivos de configuração para dispositivos de redes se dá comumente pelo protocolo FTP, o qual é baseado no protocolo de transporte UDP.
D) O serviço CIFS é usualmente utilizado para prover interoperabilidade entre ambientes distintos, como Windows e Linux.
E) O servidor WEB pode ser visto como um repositório de páginas e arquivos cujo acesso é baseado no protocolo de aplicação HTML.

10. Em um dado *host* da rede, com sistema operacional LINUX, foi observado o conteúdo parcial do arquivo de configuração */etc/fstab* mostrado na figura abaixo:

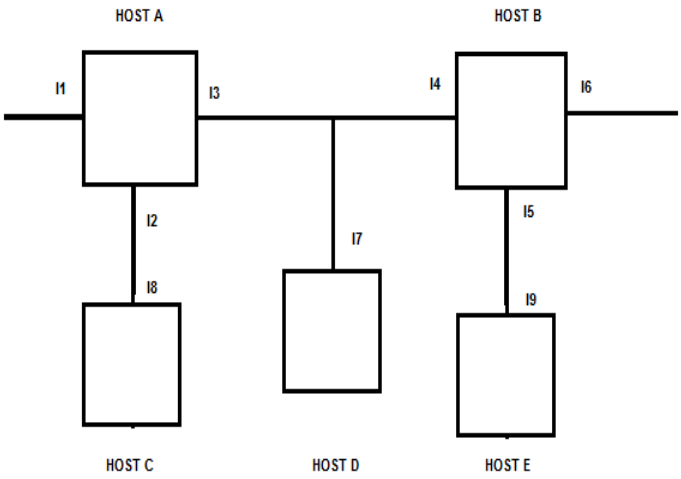
```
/dev/hda2          /              ext3
/dev/hda6          swap           swap
/dev/cdrom         /mount/cdrom   udf
/dev/fd0           /mount/floppy  auto
/dev/hda1          /mnt/WinXP     ntfs
/dev/hda7          /mnt/shared    vfat
tmpfs              /mnt/tmpfschk  tmpfs
master:/store      /store         nfs
```

De acordo com essa listagem, é **CORRETO** afirmar:

A) Deve haver um servidor na rede acessível pelo diretório */store*
B) Os dispositivos *cdrom* e *fd0* não apresentam sistemas de arquivos configurados corretamente.
C) O diretório raiz do sistema de arquivos da máquina foi montado em uma partição errada, pois ele deveria estar em alguma partição primária, como /dev/hda0
D) Deve haver um servidor na rede acessível pelo diretório /mnt/WinXP
E) A participação configurada para *swap* permite uma extensão do sistema de arquivos de local.

11. A figura a seguir (figura B) apresenta um cenário de uma rede formada pelos hosts A, B, C, D e E. Todos eles estão interligados por redes *Ethernet* e TCP/IP. Também, considere que exista um equipamento que permite a interconexão dos hosts A, D e B. Considere esta figura para responder às questões de 11 a 14.

Figura B



Suponha que foi adquirido, junto ao órgão gestor da Internet, um único endereço base 209.134.199.0/24 para atribuir endereços IPs para todas as interfaces dos cinco *hosts*. Assinale qual alternativa abaixo atende de forma **CORRETA** a esse requisito. Note que abaixo estão apresentados os endereços IP das redes às quais as interfaces estão conectadas.

A) REDE I1: 209.134.199.0/27; REDE I2,I8: 209.134.199.32/27; REDE I3,I4,I7: 209.134.199.48/27; REDE I5,I9: 209.134.199.64/27; REDE I6: 209.134.199.96/27.
B) REDE I1: 209.134.199.10/28; REDE I2,I8: 209.134.199.20/28; REDE I3,I4,I7: 209.134.199.30/28; REDE I5,I9: 209.134.199.40/28; REDE I6: 209.134.199.50/28.
C) REDE I1: 209.134.199.0/28; REDE I2,I8: 209.134.199.32/28; REDE I3,I4,I7: 209.134.199.48/28; REDE I5,I9: 209.134.199.64/28; REDE I6: 209.134.199.96/28.
D) REDE I1: 209.134.199.10/24; REDE I2,I8: 209.134.199.20/24; REDE I3,I4,I7: 209.134.199.30/24; REDE I5,I9: 209.134.199.40/24; REDE I6: 209.134.199.50/24.
E) REDE I1: 209.134.199.0/24; REDE I2,I8: 209.134.200.0/24; REDE I3,I4,I7: 209.134.201.0/24; REDE I5,I9: 209.134.202.0/24; REDE I6: 209.134.203.0/24.

12. Na figura B (da questão anterior) suponha que esteja sendo planejada a instalação de um serviço para realizar o *caching* de páginas dos acessos http dos *hosts* C, D e E. Também, a instalação de um servidor http que deve servir tanto aos *hosts* externos provenientes da Internet quanto aos *hosts* C, D e E. Supondo que a saída para *Internet* esteja acessível via interface I6, assinale qual das proposições abaixo apresenta procedimentos parciais alinhados com uma possível implementação desse cenário.

A) Na verdade, o cenário proposto não representa uma implementação possível, pois não foram previstos roteadores IP para interconexão das redes.
B) Deve ser feita a instalação do servidor http no HOST D; enquanto deve ser feita a do serviço PROXY nos HOSTS A e B.
C) Deve ser feita a instalação do servidor http no HOST D; enquanto deve ser feita a dos serviços NAT/NAPT nos HOSTS A e B.
D) Deve ser feita a instalação do servidor http no HOST B; enquanto deve ser feita a dos serviços NAT/NAPT nos HOSTS A e B.
E) Deve ser feita a instalação do servidor http no HOST D; enquanto deve ser feita a do serviço PROXY no HOST B.

13. Na figura B (da questão 11), suponha que o administrador de segurança da rede esteja implantando uma arquitetura de firewall para proteger todos os *hosts* mostrados. Neste caso, ele selecionou um sistema de *firewall* sem estados. Considerando que estejam instalados os seguintes serviços nos *hosts* da rede e que os mesmos usem seus protocolos de transportes e portas *default*: HOSTS C e E: serviço http; HOST D: serviço DNS; e HOSTS A e B: serviço SSH. Além disso, todos os *hosts* possuem seus sistemas operacionais e *browsers* instalados e configurados. A saída para a Internet está acessível pela interface I6. Assinale a alternativa que apresenta regras (parciais) de filtragem alinhadas com a autorização do acesso interno/externo apenas aos serviços citados a serem aplicadas nos *hosts* das interfaces correspondentes.

A) Autorizar tráfego TCP na porta destino 22 entrando na interface I2; autorizar tráfego UDP na porta destino 53 entrando na interface I6; autorizar tráfego TCP na porta origem 22 saindo da interface I6; autorizar tráfego TCP na porta origem 80 saindo na interface I3.
B) Autorizar tráfego TCP na porta destino 22 entrando na interface I2; autorizar tráfego UDP na porta destino 53 entrando na interface I3; autorizar tráfego TCP na porta destino 22 saindo da interface I6; autorizar tráfego TCP na porta origem 80 saindo na interface I3.
C) Autorizar tráfego TCP na porta destino 22 entrando na interface I2; autorizar tráfego UDP na porta origem 53 saindo na interface I3; autorizar tráfego TCP na porta origem 22 saindo da interface I6; autorizar tráfego TCP na porta 80 origem saindo na interface I3.
D) autorizar tráfego TCP na porta origem 22 entrando na interface I5; autorizar tráfego UDP na porta origem 53 entrando na interface I2; autorizar tráfego TCP na porta origem 22 saindo da interface I6; autorizar tráfego TCP na porta 80 origem saindo na interface I3.
E) autorizar tráfego TCP na porta destino 22 entrando na interface I2; autorizar tráfego UDP na porta destino 53 entrando na interface I6; autorizar tráfego TCP na porta destino 22 saindo da interface I6; autorizar tráfego TCP na porta origem 443 saindo na interface I3.

14. Na Figura B (questão 11), suponha que o administrador de segurança da rede esteja implantando uma solução de *firewall* que deve seguir a arquitetura DMZ. De acordo com a abordagem proposta por esta arquitetura, assinale qual alternativa fornece uma solução adequada a ela considerando que a saída para a Internet está acessível pela interface I6.

A) Os *Hosts* D e E seriam os *hosts* das redes interna; o *Host* A seria o firewall interno; o *Host* B seria o *firewall* externo; o *host* C seria o *bastion host*; a rede formada pelas interfaces I3, I7 e I4 representaria a rede de perímetro; não haveria duplicação de algumas regras nos dois firewalls.
B) Os *Hosts* D e E seriam os *hosts* das redes interna; o *Host* A seria o *firewall* interno; o *Host* B seria o *firewall* externo; o host C seria o bastion host; a rede formada pelas interfaces I5 e I9 representaria a rede de perímetro; haveria duplicação de algumas regras nos dois *firewalls*.
C) Os *Hosts* C e D seriam os hosts das redes interna; o *Host* A seria o *firewall* interno; o *Host* B seria o *firewall* externo; o *host* E seria o *bastion host*; a rede formada pelas interfaces I5 e I9 representaria a rede de perímetro; não haveria duplicação de algumas regras nos dois *firewalls*.
D) Os Hosts C e E seriam os hosts das redes interna; o *Host* A seria o *firewall* interno; o Host B seria o *firewall* externo; o *host* D seria o *bastion host*; a rede formada pelas interfaces I2 e I8 representaria a rede de perímetro; haveria duplicação de algumas regras nos dois firewalls.
E) Os *Hosts* C e E seriam os *hosts* das redes interna; o Host A seria o *firewall* interno; o *Host* B seria o *firewall* externo; o *host* D seria o *bastion host*; a rede formada pelas interfaces I3, I7 e I4 representaria a rede de perímetro; haveria duplicação de algumas regras nos dois *firewalls*.

15. As soluções de segurança em redes corporativas não se resumem a apenas uma técnica de proteção; muito pelo contrário, várias técnicas são combinadas visando aumentar a capacidade de combater os ataques aos quais as redes estão sujeitas. Duas tecnologias bastante utilizadas são os sistemas de IDS e IPS. A respeito desses sistemas, assinale a alternativa abaixo que apresenta uma afirmação **VERDADEIRA**:

A) Normalmente, um sistema IDS segue duas estratégias para implementação. Na primeira, se está interessado em monitorar o tráfego em um segmento de rede; enquanto na segunda, o objetivo é monitorar o tráfego em um *host* específico.
B) Ambas as soluções fazem o monitoramento da rede, analisando os pacotes que chegam e os comparam com determinadas regras, disparando alarmes quando necessário. Contudo, o IDS leva vantagem no quesito pró-atividade, podendo parar o tráfego malicioso quando necessário.
C) Tanto o IPS quanto o IDS podem ser substituídos por filtros de pacotes sem estado, sem qualquer prejuízo à política de segurança implementada.
D) O tunelamento implementado por essas tecnologias se apresenta como principal recurso para prover a segurança necessária.
E) O mascaramento da identidade implementado por essas tecnologias se apresenta como principal recurso para prover a segurança necessária.

16. Com relação ao objetivo da norma ABNT NBR ISO/IEC 27002:2005, da Associação Brasileira de Normas Técnicas, podemos afirmar:

I. Esta Norma estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização.
II. Os objetivos definidos nesta Norma proveem diretrizes gerais sobre as metas geralmente aceitas para a gestão de segurança da informação.
III. É uma versão antiga (não mais vigente) da norma ABNT NBR ISO/IEC 27005:2008.

A) Apenas as assertivas I e III estão corretas.
B) Apenas a assertiva I está correta.
C) Todas as assertivas estão corretas.
D) Apenas as assertivas I e II estão corretas.
E) Apenas a assertiva II está correta.

17. O processo de gestão de riscos é um conjunto de atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos. Faz(em) parte desse processo:

I. Análise/Avaliação de riscos - processo completo de análise e avaliação de riscos.
II. Tratamento do risco - risco remanescente após o tratamento do risco.
III. Aceitação do risco - decisão de aceitar um risco.
IV. Avaliação de riscos - processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.

A) Apenas as assertivas I e II estão corretas.
B) Apenas as assertivas I, III e IV estão corretas.
C) Apenas as assertivas I, II e III estão corretas.
D) Todas as assertivas estão corretas.
E) Apenas a assertiva II está correta.

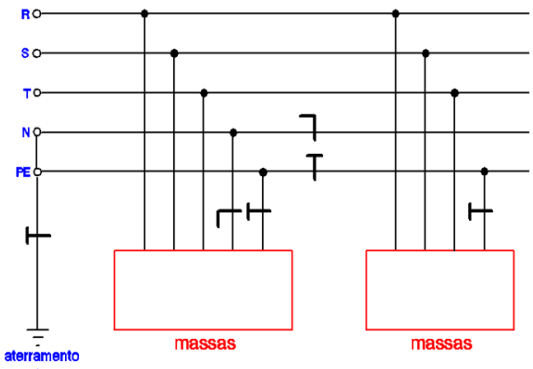
18. Conforme a NBR-5410/2004 os esquemas de aterramento TN / TT / IT, temos:

[TN] - T = Ponto diretamente aterrado. N = Massas ligadas ao ponto da alimentação aterrado (em corrente alternada, o ponto aterrado é normalmente o ponto neutro).
[TT] - T = Ponto diretamente aterrado. T = Massas diretamente aterradas, independentemente do aterramento eventual de um ponto da alimentação.
[IT] - I = Isolação de todas as partes vivas em relação a terra ou aterramento de um ponto através de impedância. T = Massas diretamente aterradas, independentemente do aterramento eventual de um ponto da alimentação.

Assim como tem-se à disposição do condutor neutro e do condutor de proteção:

[S] - Funções de neutro e de proteção asseguradas por condutores distintos.
[C] - Funções de neutro e de proteção combinadas em um único condutor (condutor PEN).

Identificar, no circuito abaixo, o tipo de aterramento



A) Circuito IT
B) Circuito TN-C-S
C) Circuito TN-C
D) Circuito TT
E) Circuito TN-S

19. Conforme a NBR-5410/2004 para os esquemas de aterramento TN / TT / IT, podemos afirmar:

I. O esquema **TN–C** é o mais econômico porque são utilizados 4 condutores no sistema trifásico e 2 no sistema monofásico
II. No esquema de aterramento **IT** não deve haver desligamento da fonte quando ocorrer a primeira falta a terra. No esquema IT todas as partes vivas são isoladas do terra e/ou um ponto da alimentação é aterrado através de impedância (neutro). As massas da instalação são aterradas.
III. No esquema TT os pontos de terra e neutro são conectados em um ponto comum, tornando-o mais econômico.

A) As alternativas I, II e III estão corretas.
B) As alternativas I e II estão corretas.
C) As alternativas II e III estão corretas.
D) As alternativas I e III estão corretas.
E) A alternativa II está correta.

20. O que é **CORRETO** afirmar sobre a segurança da informação?

I. É a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio maximizando o retorno sobre o investimento e as oportunidades de negócio.
II. Seus requisitos são identificados por meio de análise/avaliação sistemática dos riscos à segurança. Então, os resultados da análise/avaliação ajudarão a direcionar e a determinar as ações gerenciais apropriadas e as prioridades para o gerenciamento dos riscos.
III. É obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *softwarte e hardware*.
IV. A segurança da informação é importante para os negócios, tanto do setor público como do setor privado, e para proteger as infraestruturas críticas. Em ambos os setores, a função da segurança da informação é viabilizar os negócios como governo eletrônico (*e-gov*) ou comércio eletrônico (*e-business*), e evitar ou reduzir os riscos relevantes.

A) Todas as assertivas estão corretas.
B) Apenas as assertivas I e II estão corretas.
C) Apenas a assertiva I está correta.
D) Apenas as assertivas I, II e III estão corretas.
E) Apenas as assertivas II e III estão corretas.

21. É essencial que uma organização identifique os seus requisitos de segurança da informação. É **CORRETO** afirmar que as principais fontes de requisitos de segurança da informação são:

I. A análise/avaliação de riscos para a organização, levando-se em conta os objetivos e as estratégias globais de negócio da organização.
II. A legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais,

contratados e provedores de serviços têm que atender, além do seu ambiente sociocultural.
III. Um conjunto particular de princípios, objetivos e os requisitos do negócio para o processamento da informação que a organização precisa desenvolver para apoiar suas operações.
IV. A norma ABNT NBR ISO/IEC 7799:2005.

A) Apenas as assertivas I e II estão corretas.
B) Apenas as assertivas II e III estão corretas.
C) Todas as assertivas estão corretas.
D) Apenas as assertivas I, II e III estão corretas.
E) Apenas as assertivas III e IV estão corretas.

22. A experiência tem mostrado que alguns dos seguintes fatores são críticos para o sucesso da implementação da segurança da informação dentro de uma organização. Quais são estes fatores?

I. Adoção de política de segurança da informação, bem como de objetivos e atividades que reflitam os objetivos do negócio, aliados a um bom entendimento dos requisitos de segurança da informação, da análise/avaliação de riscos e da gestão de risco.
II. Adoção de uma abordagem e de uma estrutura para a implementação, manutenção, monitoramento e melhoria da segurança da informação que seja consistente com a cultura organizacional, além de provisão de conscientização, treinamento e educação adequados.
III. Provisão de recursos financeiros para as atividades da gestão de segurança da informação.
IV. Estabelecimento de um processo eficiente de gestão de incidentes de segurança da informação.

A) Apenas as assertivas I, II e III estão corretas.
B) Todas as assertivas estão corretas.
C) Apenas as assertivas I e II estão corretas.
D) Apenas as assertivas II e III estão corretas.
E) Apenas as assertivas III e IV estão corretas.

23. Podemos afirmar sobre política de segurança da informação:

I. O seu objetivo é prover orientação e apoio da direção de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes.
II. Convém que seja analisada criticamente em intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua continua pertinência, adequação e eficácia.
III. É um conjunto de regras conhecidas e definidas no nível gerencial da organização para evitar a revelação de informações sensíveis aos funcionários da empresa.

A) Apenas as assertivas I e III estão corretas.
B) Apenas a assertiva I está correta.
C) Apenas as assertivas I e II estão corretas.
D) Todas as assertivas estão corretas.
E) Apenas a assertiva II está correta.

24. As responsabilidades pela proteção de cada ativo e pelo cumprimento de processos de segurança da informação específicos devem ser definidas na atribuição das responsabilidades pela segurança da informação. Isso significa que:

I. Os ativos e os processos de segurança da informação associados com cada sistema sejam identificados e claramente definidos.
II. O gestor responsável por cada ativo ou processo de segurança da informação deve ter atribuições documentadas e os detalhes dessa responsabilidade devem estar claramente definidos.
III. Os níveis de autorização devem ser claramente definidos e documentados.
IV. Pessoas com responsabilidades definidas pela segurança da informação podem delegar tarefas de sua responsabilidade para outros, mas continuam responsáveis pela correta execução das mesmas.

A) Todas as assertivas estão corretas.
B) Apenas as assertivas I, II e III estão corretas.
C) Apenas as assertivas I e II estão corretas.
D) Apenas as assertivas II e III estão corretas.
E) Apenas as assertivas III e IV estão corretas.

25. A coordenação da segurança da informação deve envolver a cooperação de gerentes, usuários, administradores, desenvolvedores, auditores, pessoal de segurança e especialistas com habilidades nas áreas de seguro, questões legais, recursos humanos, TI e gestão de riscos. O que se pode afirmar com relação a atividade de coordenação?

I. Visa aprovar as metodologias e processos para a segurança da informação, tais como análise/avaliação de riscos e classificação da informação.
II. Deve promover, de forma eficaz, a educação, o treinamento, e a conscientização sobre a segurança da informação por toda a organização.
III. Deve avaliar as informações recebidas do monitoramento e da análise crítica dos incidentes de segurança da informação e recomendar ações apropriadas como resposta para tais incidentes.
IV. Se a organização não comporta a integração de representantes de diferentes áreas como mencionado no enunciado dessa questão (devido a seu tamanho, por exemplo), as atividades de

coordenação podem ser conduzidas por um único gestor.

A) Apenas as assertivas I, II e III estão corretas.
B) Apenas as assertivas I e II estão corretas.
C) Apenas as assertivas II e III estão corretas.
D) Apenas as assertivas III e IV estão corretas.
E) Todas as assertivas estão corretas.

26. A análise crítica da segurança da informação deve incluir a avaliação de oportunidades para melhoria das políticas da organização e ter um enfoque de gerência da segurança em resposta às mudanças no ambiente organizacional, às circunstâncias do negócio, às condições legais, ou ao ambiente técnico. Os resultados (saídas) da análise crítica da direção devem incluir decisões e ações relacionadas a:

I. Melhoria do enfoque da organização para gerenciar a segurança da informação e seus processos.
II. Melhoria dos controles e dos objetivos desses controles.
III. Melhoria na alocação de recursos e/ou responsabilidades.
IV. Melhoria nos resultados de análises críticas anteriores feitas pela direção.

A) Todas as assertivas estão corretas.
B) Apenas as assertivas I e II estão corretas.
C) Apenas as assertivas II e III estão corretas.
D) Apenas as assertivas I, II e III estão corretas.
E) Apenas as assertivas III e IV estão corretas.

27. O projeto, a operação, o uso e a gestão de sistemas de informação podem estar sujeitos a requisitos de segurança contratuais, regulamentares ou estatutários para evitar violações de quaisquer obrigações legais. Com relação aos requisitos legais é **CORRETO** afirmar que:

I. Procedimentos apropriados devem ser implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais no uso de materiais que podem estar protegidos por propriedade intelectual, incluindo os *softwares*.
II. Registros importantes devem ser protegidos contra perda, destruição e falsificação, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.
III. Os usuários devem ser dissuadidos de usar recursos de processamento da informação para propósitos não autorizados.
IV. Os controles de criptografia podem ser usados sem preocupação com as leis, principalmente na *internet*, pois esta é de livre acesso, de alcance global e, portanto, não está sob jurisdição de nenhum país em específico.

A) Todas as assertivas estão corretas.
B) Apenas as assertivas I e II estão corretas.
C) Apenas as assertivas I, II e III estão corretas.
D) Apenas as assertivas II e III estão corretas.
E) Apenas as assertivas III e IV estão corretas.

28. Após um incidente de segurança da informação pode ser necessário que evidências sejam coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da jurisdição pertinente. Com relação à coleta de evidências, é **CORRETO** afirmar que:

I. O perito deve se preocupar com a admissibilidade da evidência – avaliar se a evidência pode ou não ser utilizada na corte.
II. O perito deve se preocupar com a importância da evidência – avaliar a qualidade e inteireza da evidência.
III. Para obter admissibilidade da evidência, a organização deve assegurar que sistemas de informação estejam de acordo com qualquer norma ou código de prática publicado para produção de evidências admissíveis.
IV. Para manter registros fortes de evidência durante o processo de cópia de mídias eletrônicas, o registro de todas as ações tomadas deve ser guardado e o processo testemunhado.

A) Apenas as assertivas I, II e III estão corretas.
B) Todas as assertivas estão corretas.
C) Apenas as assertivas I e II estão corretas.
D) Apenas as assertivas II e III estão corretas.
E) Apenas as assertivas III e IV estão corretas.

29. A continuidade do negócio é também conhecida como contingência do negócio. Toda organização deve estar preparada para enfrentar situações de contingência e de desastre que tornem indisponíveis recursos que possibilitam seu uso. Qual o requisito para implantação de um plano de continuidade?

A) Análise e gestão de riscos.
B) Política de segurança de informação.
C) Classificação das informações em função dos riscos mercadológicos.
D) Notificação de eventos de segurança da informação.
E) Controle do processamento interno.

30. Convém que as instalações de processamento da informação críticas ou sensíveis sejam mantidas em áreas seguras, protegidas por perímetros de segurança definidos, com barreiras de segurança e

controles de acesso apropriados. Convém que a proteção oferecida seja compatível com os riscos identificados. Estas afirmações referem-se a quê?

A) À segurança física.
B) À segurança lógica.
C) À segurança motivacional.
D) À segurança operacional.
E) À segurança financeira.

31. Sobre segurança operacional (*safety)*, é **CORRETO** afirmar:

I. É uma situação na qual o risco de lesões às pessoas ou danos às propriedades é reduzido e mantido em, ou abaixo de, um nível aceitável, mediante um contínuo processo de identificação de perigos e gerenciamento de riscos.
II. É a proteção dos sistemas de informação contra acesso não autorizado.
III. É o requisito para que um sistema de informação contenha integridade, confidencialidade e privacidade das informações.
IV. É o mesmo que continuidade dos negócios.

A) Todas as assertivas estão corretas.
B) Apenas as assertivas I, II e IV estão corretas.
C) Apenas as assertivas II e III estão corretas.
D) Apenas as assertivas III e IV estão corretas.
E) Apenas a assertiva I está correta.

32. Nem toda informação é crucial ou essencial a ponto de merecer cuidados especiais. Por outro lado, determinada informação pode ser tão vital que o custo para manter a sua integridade, qualquer que seja, ainda será menor que o custo de não dispor dela adequadamente.

I. Uma forma de classificar as informações é atribuir níveis de prioridade a ela. Exemplo: Pública, Interna, Confidencial e Secreta.
II. Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização.
III. Convém que seja de responsabilidade do proprietário do ativo definir a classificação de um ativo, analisando-o criticamente a intervalos regulares, e assegurar que ele está atualizado e no nível apropriado.
IV. Em geral, a classificação dada à informação é uma maneira de determinar como essa informação vai ser tratada e protegida.

A) Todas as assertivas estão corretas.
B) Apenas a assertiva I está correta.
C) Apenas as assertivas I, II e IV estão corretas.
D) Apenas as assertivas II e III estão corretas.
E) Apenas as assertivas III e IV estão corretas.

33. Sobre segurança física, é **CORRETO** afirmar:

I. De modo geral, deve ser permitida a entrada de pessoas, portanto, objetos estranhos, à sala dos computadores.
II. Todo material que for entrar na sala de computadores deve ser controlado, autorizado e examinado previamente.
III. Toda visita deve ser monitorada e o visitante deve ser acompanhado por algum funcionário da empresa.
IV. O visitante deve portar um crachá de identificação.

A) Apenas a assertiva I está correta.
B) Apenas as assertivas II, III e IV estão corretas.
C) Apenas as assertivas I, II e IV estão corretas.
D) Apenas as assertivas III e IV estão corretas.
E) Todas as assertivas estão corretas.

34. Num mundo de negócios competitivo como o de hoje, as empresas simplesmente não podem mais ficar indisponíveis para seus clientes, mesmo que tenham problemas com seus processos de negócios, recursos e/ou dados e informações. Velocidade de processamento e de decisões, altíssima disponibilidade, flexibilidade e foco em produtos de acordo com o mercado são requisitos fundamentais para "sobrevivência e sucesso". Porém, se não houver Planejamento para Segurança e Contingência adequado, alguns ou até todos os requisitos estarão ameaçados e, consequentemente, a empresa também. Sobre um plano de continuidade, é **CORRETO** afirmar que:

I. Serve para não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, bem como assegurar a sua retomada em tempo hábil, se for o caso.
II. Serve para dar tempo hábil à empresa para que ela possa comunicar seus acionistas e órgãos reguladores sobre suas dificuldades financeiras.
III. Os planos de Contingência são desenvolvidos para cada ameaça considerada em cada um dos processos do negócio pertencentes ao escopo, definindo em detalhes os procedimentos a serem executados em estado de contingência.
IV. Serve para evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.

A) Apenas as assertivas I e III estão corretas.
B) Apenas a assertiva I está correta.
C) Apenas as assertivas I, II e IV estão corretas.
D) Apenas as assertivas III e IV estão corretas.
E) Todas as assertivas estão corretas.

35. As empresas estão procurando dar mais atenção ao ser humano, pois é ele que faz com que as engrenagens empresariais funcionem perfeita e harmonicamente, buscando um relacionamento cooperativo e satisfatório para ambas as partes, com objetivos comuns. Entre a(s) melhor(es) maneira(s) de garantir que o ser humano se comporte adequadamente com relação às suas atribuições profissionais, estão:

I. Ministrar treinamentos periódicos.
II. Ter campanhas de sensibilização.
III. Criar uma política de segurança, bem distribuída e divulgada, que contenha os direitos, deveres e penalidades.
IV. Auditar, periodicamente, as movimentações financeiras dos colaboradores a fim de identificar possíveis vazamentos de informações em troca de compensação financeira. II.

A) Apenas as assertivas I e III estão corretas.
B) Apenas a assertiva I está correta.
C) Apenas as assertivas III e IV estão corretas.
D) Todas as assertivas estão corretas.
E) Apenas as assertivas I, II e III estão corretas.

36. O risco não é um novo problema ou uma nova terminologia; os seres humanos sempre tiveram de enfrentar (ou encarar) os riscos no seu meio ambiente, embora seu significado tenha mudado, como tem mudado a sociedade e o próprio meio onde vivem. O perigo (condição, objeto ou atividade que potencialmente pode causar lesões ao pessoal, danos aos equipamentos ou estruturas, morte, ou redução da habilidade de desempenhar uma função determinada) e o risco (a possibilidade de perda ou dano, medida em termos de severidade e probabilidade; a possibilidade que algo possa ocorrer e suas conseqüências se ocorrer) estão no dia-a-dia das organizações. Sobre riscos, perigos e suas conseqüências, é **CORRETO** afirmar que:

I. A existência de um lixão próximo a um aeródromo é um perigo. A possibilidade de que uma aeronave colida com um urubu, atraído pelo lixão, durante a decolagem ou o pouso, que pode resultar em um acidente, é um risco.
II. A existência de um lixão próximo a um aeródromo é um risco. A possibilidade de que uma aeronave colida com um urubu, atraído pelo lixão, durante a decolagem ou o pouso, que pode resultar em um acidente, é um perigo.
III. O risco residual (risco remanescente após o tratamento de riscos) também deve ser contemplado na análise e gestão de riscos.
IV. O perigo tem duas importantes características: a gravidade (algumas vezes denominada de dano) e a probabilidade da ocorrência.
V. A gravidade do perigo é definida como o pior acidente possível de ocorrer, resultante do perigo causado pelo ambiente na sua condição menos favorável.

A) Apenas as assertivas I, III, IV e V estão corretas.
B) Apenas as assertivas I, II e IV estão corretas.
C) Apenas as assertivas II, IV e V estão corretas.
D) Apenas as assertivas I e III estão corretas.
E) Todas as assertivas estão corretas.

37. Os objetivos "assegurar que a informação receba um nível adequado de proteção", "alcançar e manter a proteção adequada dos ativos da organização" e "assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil" referem-se a quê?

A) À conformidade, à Gestão de Ativos e à Gestão de Incidentes de Segurança da Informação, respectivamente.
B) À Classificação da Informação, à Gestão de Ativos e à Gestão de Incidentes de segurança da informação, respectivamente.
C) Gestão de Ativos, à Classificação da Informação e à Gestão de Incidentes de Segurança da Informação, respectivamente.
D) À Gestão de Risco, à Gestão de Ativos e à Gestão de Incidentes de Segurança da Informação, respectivamente.
E) À Classificação da Informação, à Gestão de Incidentes de Segurança da Informação e à Gestão de Ativos, respectivamente.

38. Vários incidentes de segurança podem ocorrer por questões comportamentais, tais como falhas de configuração, desconhecimento ou ignorância, ou mesmo incidentes gerados propositadamente por pessoas internas à organização. Para minimizar o impacto destas ações?

I. Convém assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, de forma a reduzir o risco de roubo, fraude ou mau uso de recursos.
II. Convém que as responsabilidades pela segurança da informação sejam atribuídas antes da contratação, de forma adequada, nas descrições de cargos e nos termos e condições de contratação.
III. Convém que todos os funcionários, fornecedores e terceiros, usuários dos recursos de processamento da informação, assinem acordos sobre seus papéis e responsabilidades pela segurança da informação.
IV. Convém que todos os candidatos ao emprego, fornecedores e terceiros sejam adequadamente

analisados,especialmente em cargos com acesso a informações sensíveis.

V. Convém criar uma política de segurança, bem distribuída e divulgada, que contenha os direitos, deveres e penalidades.

A) Apenas as assertivas I , II, III e IV estão corretas.
B) Apenas a assertiva I, II, III e V estão corretas.
C) Todas as assertivas estão corretas.
D) Apenas as assertivas I, II e IV estão corretas.
E) Apenas as assertivas II, III e IV estão corretas.

39. Os ataques normalmente exploram problemas e vulnerabilidades existentes em qualquer nível organizacional. Enquanto o profissional de segurança se preocupa com todas as vulnerabilidades existentes em um sistema para que o mesmo seja menos sujeito a um ataque, o atacante está à procura de apenas uma vulnerabilidade para que consiga obter as informações. Uma forma de melhorar a segurança em tecnologia da informação é montar um Sistema de Gestão de Segurança da Informação (SGSI). Esse sistema, na prática, é a implementação de vários requisitos do planejamento em segurança da informação. Entre eles, está:

I. Plano de Continuidade de Negócios.
II. Análise e Gerência dos Riscos do Negócio.
III. Implantação de uma política de segurança.
IV. Realizar a Gestão de Ativos.
V. Realizar a classificação das informações.

A) Todas as assertivas estão corretas.
B) Apenas as assertivas I, III e V estão corretas.
C) Apenas as assertivas I, II, III e V estão correta.
D) Apenas as assertivas I, II e IV estão corretas.
E) Apenas as assertivas III e IV estão corretas.

40. A segurança operacional é um misto de segurança focada em ativos (tecnologia), processos e pessoas. Dessa forma, podemos dizer que a segurança operacional envolve:

I. Segurança Lógica das Informações.
II. Segurança Física da Infraestrutura.
III. Análise e Gerência de riscos.
IV. Planos de Continuidade.
.

A) Apenas as assertivas I, III e IV estão corretas.
B) Apenas as assertivas II, III e IV estão correta.
C) Apenas as assertivas I e II estão corretas.
D) Apenas as assertivas III e IV estão corretas.
E) Todas as assertivas estão corretas.

INGLÊS TÉCNICO

Read the text below and answer questions 41, 42 and 43.

BRACE YOURSELF FOR THE REAL-TIME WEB

London, England (CNN) -- Real-time is a top 10 Web trend for 2010, I proposed in this column last week. Now the stage is set: Google this week launched real-time search, bringing live updates from Twitter, Facebook, MySpace and more into a scrolling pane in your Google search results.

How will the real-time trend evolve in 2010? Rapidly, no doubt. Why will it sweep the Web? Because it fuels our insatiable info-addiction.

What's driving this real-time trend anyway? In large part, lowered barriers to content creation: Posting a 140-character update to Twitter is so effortless that Web users are becoming conditioned to create.

They've learned to expect a response, too: The immediate feedback provided by Facebook comments and Twitter replies is an incentive to make continued contributions.

But the real answer may be in our heads. These technologies are literally addictive, says psychologist Susan Weinschenk, fueling a "dopamine-induced loop" of seeking behavior and instantaneous reward.

A vast array of Web sites and applications will try to capitalize on the real-time Web in 2010, serving our need to be engaged in the moment. Serving, perhaps, but never quite satisfying.

"Do you ever feel like you are addicted to email or Twitter or texting," Weinschenk asks.

Of course you are. We all are ... and soon we'll be addicted to a whole lot more.

Fonte: http://www.cnn.com/2009/

41. According to the author, why will real-time web evolve in 2010?

A) Because it meets our info-addiction needs.
B) Because it brings live updates from Twitter and Facebook.
C) because people are tired of the web search tools available nowadays.
D) Because it brings live updates from My Space and more.
E) Because the author proposed it in his column last week.

42. Based on the text, what are the reasons pushing forward real-time web? Select the statements that are true.

I. Less limits to content creation.
II. The delays in feedback.
III. Technologies are addictive.
IV. People seek behavior and instantaneous rewards.

A) I and IV are true.
B) I, III and IV are true.
C) III and IV are true.
D) II and IV are true.
E) All alternatives are true.

43. Does the author think real-time web will serve people´s needs?

A) He thinks it will serve people´s needs but not quite satisfy.
B) He thinks people Will be absolutely fulfilled by real-time web.
C) He thinks people´s addictions will come to an end.
D) He thinks people´s addictions will be met and satisfied.
E) He thinks people´s heads will be turned by real-time web forever.

Read the text and answer questions 44 and 45.

RIP MICROSOFT ENCARTA

Microsoft will stop making MSN Encarta encyclopaedia websites and software after being forced out of the market by Wikipedia.
According to a message posted on the Encarta website, the sites will be discontinued on 31st October, although the Japanese version will run till the end of December. Software programmes Microsoft Student and Encarta Premium will stop production by June. Those with premium services as of 30th April will receive a refund for services paid beyond that date and will have access to premium services until October.
The posting reads: "Encarta has been a popular product around the world for many years. However, the category of traditional encyclopedia and reference material has changed. People today seek and consume information in considerably different ways than in years past."
It appears that the free online encyclopaedia has forced Encarta and just about every other online encyclopaedia off the market. According to Hitwise, an internet tracker website, Wikipedia accounts for 97% of all online encyclopaedia visits in the United States. Encarta is second, but only forms 1.27% of the market. Third is Encyclopedia.com, with 0.76%.
Although the services will be stopped, the company believes that the assets gained from Encarta may be used in developing "future technology solutions."
Other Microsoft software being stopped include OneCare, a consumer antivirus product; Equipt, a subscription security software package; and its Flight Simulator software.

Fonte: http://www.gi.com/Mar 31st, 2009.

44. Based on the message Microsoft posted on the Encarta website, why does it state it will discontinue the software?

A) Because the number of people visiting Encarta´s website is only 1.27%.
B) Because Wikipedia bought 97% of Encarta´s shares in the United States.
C) Because people´s search and consumption for information has changed and this forced the traditional encyclopedia to change as well.
D) Because Encarta will be used in the development of future technology solutions.
E) Because Microsoft will not accept being second in the ranking of the North American market.

45. According to the text which Microsoft softwares have stopped being made? Choose the best alternative.

I. OneCare and Encyclopedia.com.
II. Microsoft Student and Encarta Premium.
III. Microsoft´s Flight Simulator software.
IV. Equipt and Wikipedia.

A) I and IV.
B) I and II.
C) II and III.
D) II and IV.
E) III and IV.

COMPUTER SCIENCE

Computer science or **computing science** is the study of the theoretical foundations of information and computation, and of practical techniques for their implementation and application in computer systems. It is frequently described as the systematic study of algorithmic processes that create, describe and transform information. According to Peter J. Denning, the fundamental question underlying computer science is, "What can be (efficiently) automated?" Computer science has many sub-fields; some, such as computer graphics, emphasize the computation of specific results, while others, such as computational complexity theory, study the properties of

computational problems. Still others focus on the challenges in implementing computations. For example, programming language theory studies approaches to describing computations, while computer programming applies specific programming languages to solve specific computational problems, and human-computer interaction focuses on the challenges in making computers and computations useful, usable, and universally accessible to people.
The general public sometimes confuses computer science with vocational areas that deal with computers (such as information technology), or think that it relates to their own experience of computers, which typically involves activities such as gaming, web-browsing, and word-processing. However, the focus of computer science is more on understanding the properties of the programs used to implement software such as games and web-browsers, and using that understanding to create new programs or improve existing ones.

Fonte: http://en.wikipedia.org/wiki/Computer_science

46. Which of the following statements are true according to the text?

I. Computer Science is the same as information technology.
II. computer graphics study the properties of computational problems.
III. human-computer interaction is concerned about the challenges in making computers accessible to people.
IV. Computer science is described as the systematic study of algorithmic processes that create, describe and transform information.

A) I and III are true.
B) II and III are true.
C) II and IV are true.
D) III and IV are true.
E) I and IV are true.

47. Which of the alternatives below are the real focus of computer science? Select the correct option.

I. Being able to play games and use a word-processor
II. Understanding the properties of the programs used to implement software
III. Using Web-browsing and computer graphics.
IV. Using the comprehension of the properties of programs to create new programs or improve existing ones.

A) II and IV are correct.
B) II, III and IV are correct.
C) I, II and IV are correct.
D) Only IV is correct.
E) All of the alternatives are correct.

IS A WARRANTY ON LAPTOPS WARRANTED?

A study by SquareTrade, an online vendor of extended warranties, says 20.4 percent of laptops fail over three years. It's in the interest of SquareTrade that people know how often a laptop fails. If you think it is going to be high, you are more likely to buy a warranty.
But the statistics also provide the consumer with some basic information on how much they should pay for the warranty. Usually, the failure rate of a product is not known. Consumers tend to think the rate is higher than it is and, being risk-averse, buy the warranty.
Knowing that 20 percent of all laptops fail in three years tells you a little about how much to pay for that warranty. A warranty for a $800 laptop would be worth 20.4 percent of $800, or about $163. If indeed laptop failure rates are as high as 20 percent, that would suggest that laptop warranties aren't particularly bad deals.
SquareTrade looked at the failure rates by brand and concluded that Asus and Toshiba laptops fail about 15 percent of the time while Hewlett-Packard is at the other end of the scale with a rate of more than 25 percent. In some cases, it would appear that failure is not only an option, but the expectation.

Fonte: http://gadgetwise.blogs.nytimes.com/November 23, 2009.

48. Square Trade is a company that:

A) Sells laptops online.
B) Carries out research and studies on laptop failures.
C) Repairs laptops.
D) Represents different brands of laptop manufacturers.
E) Sells warranties online.

49. In the sentence " If you think it is going to be high, you are more likely to buy a warranty.", the pronoun "it" refers to:

A) The frequency a laptop fails.
B) The frequency people buy laptops.
C) The frequency people buy warranties.
D) The frequency people have to use their warranties.
E) The frequency the study is carried out.

50. According to the text it is correct to affirm that:

I. Because consumers do not know products' failure rate they buy warranties more easily.
II. 25 percent of all computers fail in three years.
III. Hewlett-Packard laptops fail more than 25 percent of the time.
IV. A warranty for a laptop would be worth 20.4 percent of its price.

A) Items I and IV are correct.
B) Items I, II and III are correct.
C) All the items are incorrect.
D) All items are correct.
E) Only item I is correct.

REDAÇÃO

Leia os textos a seguir:

TEXTO I

A partir da metade do século XX, ocorreu um conjunto de transformações econômicas e sociais cuja dimensão é difícil de ser mensurada: a chamada explosão da informação. Embora essa expressão tenha surgido no contexto da informação científica e tecnológica, seu significado, hoje, em um contexto mais geral, atinge proporções gigantescas.

Por estabelecerem novas formas de pensamento e mesmo de lógica, a informática e a Internet vêm gerando impactos sociais e culturais importantes. A disseminação do microcomputador e a expansão da Internet vêm acelerando o processo de globalização tanto no sentido do mercado quanto no sentido das trocas simbólicas possíveis entre sociedades e culturas diferentes, o que tem provocado e acelerado o fenômeno de hibridização amplamente caracterizado como próprio da pós-modernidade.

FERNANDES, M. F.; PARÁ, T. *A contribuição das novas tecnologias da informação na geração de conhecimento*. Disponível em: http://www.coep.ufrj.br. Acesso em: 11 ago. 2009 (adaptado). In: LINGUAGENS, CÓDIGOS E SUAS TECNOLOGIAS- *Enem* – 2009. Caderno 7, pág. 7. http://download.globo.com/vestibular/dia2_caderno7.pdf . Acesso: 06/12/2009.

TEXTO II

As tecnologias de informação e comunicação (TIC) vieram aprimorar ou substituir meios tradicionais de comunicação e armazenamento de informações, tais como o rádio e a TV analógicos, os livros, os telégrafos, o fax etc. As novas bases tecnológicas são mais poderosas e versáteis, introduziram fortemente a possibilidade de comunicação interativa e estão presentes em todos os meios produtivos da atualidade. As novas TIC vieram acompanhadas da chamada *Digital Divide*, *Digital Gap* ou *Digital Exclusion*, traduzidas para o português como ***Divisão Digital*** ou **Exclusão Digital**, sendo, às vezes, também usados os termos Brecha Digital ou Abismo Digital.

LINGUAGENS, CÓDIGOS E SUAS TECNOLOGIAS- *Enem* – 2009. Caderno 7, pág. 7. http://download.globo.com/vestibular/dia2_caderno7.pdf . Acesso: 06/12/2009. (adaptado:grifo)

PROPOSTA DE REDAÇÃO

Com base nesses dois textos, e em outras informações/argumentos que julgar pertinentes, escreva um artigo jornalístico, entre 15 e 20 linhas, a ser enviado para a seção de opinião (*Tendência e Debates*) do jornal Folha de S. Paulo, discorrendo sobre o tema: **As tecnologias de informação e comunicação: vantagens e limites.**

SOBRE A REDAÇÃO

1. Estruture o texto da sua redação com um **mínimo de 15** e um **máximo de 20 linhas**.
2. Faça o rascunho no espaço reservado.
3. Transcreva o texto do rascunho para a FOLHA DE REDAÇÃO que lhe foi entregue em separado.
4. Não há necessidade de colocar título.
5. Não coloque o seu nome, nem a sua assinatura na FOLHA DE REDAÇÃO, nem faça marcas nela. A FOLHA DE REDAÇÃO já se encontra devidamente identificada.

REDAÇÃO – Rascunho