CONHECIMENTOS ESPECÍFICOS

QUESTÃO 31

Em relação aos tipos de *software* e suas utilidades, assinale a opção correta.

- A O interpretador é um programa de nível 1 (L1) que substitui cada instrução de nível 2 (L2) por um conjunto equivalente de L1, gerando código objeto.
- B Um depurador não permite acompanhar a execução de um programa instrução por instrução. Essa tarefa é executada pelo interpretador.
- C Linguagem de máquina é um conjunto limitado de instruções que um circuito de computador reconhece e executa diretamente, independentemente do fabricante.
- D O *loader* é um utilitário que traduz um programa fonte em linguagem de montagem em um programa objeto não executável e carrega o resultado para a memória.
- E As funções básicas de um *linker* incluem resolver todas as referências simbólicas existentes entre os módulos e reservar memória para a execução do programa.

QUESTÃO 32

Assinale a opção que apresenta os comandos utilizados no console de Linux respectivamente para: comparar conteúdo de dois arquivos ASCII, procurar por trecho de texto dentro de arquivos e mudar as proteções de um arquivo.

- A `pine / ls / mv`
- B `cf / find / rmdir`
- C `diff / grep / umask`
- D `comp / find / tail`
- E `file / cp / chgrp`

QUESTÃO 33

O recurso do Windows 8 denominado *BitLocker*

- A é um dispositivo de segurança do sistema de arquivos do Windows que serve para bloquear arquivos danificados.
- B corresponde a um antivírus que localiza e bloqueia vírus.
- C bloqueia e compacta arquivos nas unidades do computador, cujo acesso é liberado apenas por meio de senha do dono do arquivo.
- D criptografa as unidades de disco no computador, fornecendo proteção contra roubo ou exposição de dados nos computadores e nas unidades removíveis perdidas ou roubadas.
- E não pode ser utilizado em arquivos armazenados em unidades de dados removíveis, como discos rígidos externos ou unidades *flash* USB.

QUESTÃO 34

Assinale a opção que apresenta corretamente, de acordo com o COBIT 5, o domínio do processo responsável pelo gerenciamento de programas e de projetos.

- A alinhar, planejar e organizar
- B monitorar, avaliar e medir
- C entregar, reparar e suportar
- D construir, adquirir e implementar
- E avaliar, dirigir e monitorar

QUESTÃO 35

De acordo com o PMBOK 5, concluído todo o trabalho técnico do projeto, a atividade que ainda deve ser realizada é

- A planejar a resposta aos riscos.
- B criar um plano de gerenciamento de pessoal.
- C criar um plano de encerramento do projeto.
- D validar o escopo.
- E terminar o registro das lições aprendidas.

QUESTÃO 36

De acordo com o ITIL v3, a função relacionada a grupos, áreas ou equipes que possuem experiência e conhecimento técnico especializado para suportar a operação denomina-se

- A gerenciamento de operações.
- B gerenciamento de transições.
- C central de serviços (*service desk*).
- D gerenciamento técnico.
- E gerenciamento de aplicações.

QUESTÃO 37

De acordo com o CBOK 3, o gerenciamento de processos de negócio

- A trata o que, onde, quando, por que, como e por quem o trabalho é realizado.
- B trata parte do trabalho com as respectivas correlações das atividades ao longo das funções de negócio.
- C dispensa investimentos nas capacidades de negócio.
- D é uma prescrição de estrutura de trabalho, de metodologia ou de um conjunto de ferramentas.
- E dispensa a implementação de novos papéis e responsabilidades.

QUESTÃO 38

Com base no CBOK 3, assinale a opção correta acerca das características de um gerenciamento eficaz quando se utilizam indicadores de desempenho de processos.

- A Os indicadores de desempenho de processos não fornecem padrões e(ou) tendências para a medição de processos.
- B Um indicador de desempenho de processo não tem, necessariamente, um dono de processo ou um gerente de processo responsável pela definição, monitoramento e controle.
- C O impacto dos indicadores de desempenho de processos pode ser aumentado quando se fixam compensações ou incentivos.
- D Os indicadores de desempenho de processos não devem mudar a forma como a organização se avalia.
- E Deve-se estimular o surgimento de muitos indicadores de desempenho de processos, variáveis e informações, de forma a abranger todo ou parte do processo medido.

QUESTÃO 39

Considere que, de acordo com a análise de pontos de função (APF), ALI = arquivo lógico interno, EE = entrada externa, AIE = arquivos de interface externa, SE = saída externa e que baixa, média e alta se referem à complexidade de cada um desses conceitos. Nesse contexto, é correto afirmar que a quantidade de pontos de função brutos em um *software* novo, com 01 ALI baixa, 01 AIE alta, 01 EE média e 01 SE baixa, é

A 28.
B 27.
C 23.
D 25.
E 30.

QUESTÃO 40

De acordo com a NBR ISO/IEC 9126, as qualidades externas e internas podem ser categorizadas por meio de características e subcaracterísticas. As subcaracterísticas adequação, acurácia e interoperabilidade referem-se à característica

A portabilidade.
B funcionalidade.
C usabilidade.
D manutenibilidade.
E confiabilidade.

QUESTÃO 41

Assinale a opção que apresenta definição correta para um serviço agnóstico, na SOA (*service-oriented architecture*).

A É um serviço centralizado no negócio que fundamenta o contexto e o limite funcional em uma entidade de negócio.
B É um serviço presente em uma camada distinta de serviços orientada pela tecnologia.
C Consiste em unidades lógicas que encapsulam funcionalidades não específicas a nenhum aplicativo ou processo de negócio.
D Consiste de serviços pertencentes à camada de execução, modelada pela aplicação orientada às operações CRUD (em português: criar, ler, atualizar e excluir).
E É um serviço de negócio com limite funcional, diretamente associado a tarefa ou processo específico.

QUESTÃO 42

No que se refere a *design patterns*, o padrão que objetiva separar a construção de um objeto complexo da sua representação, de modo que o mesmo processo de construção possa criar diferentes representações, é o

A Prototype.
B Mediator.
C Builder.
D Abstract Factory.
E Bridge.

QUESTÃO 43

Acerca de REST (*representational state transfer*), assinale a opção correta.

A Na implementação do REST, todos os recursos devem responder a todos os métodos.
B O método GET permite obter e alterar o estado atual de um recurso.
C O método EXPUNGE permite excluir um recurso.
D A arquitetura de comunicação entre aplicações baseia-se em um modelo rígido de recursos e localizações.
E O método MODIFY permite alterar um recurso.

QUESTÃO 44

O TDD (*test driven development*)

A apresenta como vantagem a leitura das regras de negócio a partir dos testes, e, como desvantagem, a necessidade de mais linhas de códigos que a abordagem tradicional, o que gera um código adicional.
B impede que seja aplicada a prática de programação em pares, que é substituída pela interação entre analista de teste, testador e programador.
C é um conjunto de técnicas associadas ao *eXtremme Programing* e a métodos ágeis, sendo, contudo, incompatível com o *Refactoring*, haja vista o teste ser escrito antes da codificação.
D refere-se a uma técnica de programação cujo principal objetivo é escrever um código funcional limpo, a partir de um teste que tenha falhado.
E refere-se a uma metodologia de testes em que se devem testar condições, *loops* e operações; no entanto, por questão de simplicidade, não devem ser testados polimorfismos.

QUESTÃO 45

Acerca do *Clean Code*, assinale a opção correta.

A A segurança do código é vital, por isso os programadores devem deixar o código o mais obscuro possível.
B Se um valor deve ser utilizado em múltiplos locais do código, é imperativo atribuir esse valor a uma variável ou a uma constante com nome amigável.
C As classes devem possuir nome amigável oriundo de verbos, escolhidos no infinitivo, e não no gerúndio.
D Para customizar o código, deve-se utilizar o mesmo termo para duas diferentes ideias.
E Os nomes das variáveis devem ser simplificados, de forma a não criar códigos gordos (*fat codes)* — por exemplo, o uso de `x` para o nome de uma variável é mais apropriado que `MediadosAlunosAprovados`.

QUESTÃO 46

Com relação à plataforma Android, assinale a opção correta.

A *Webkit* é uma biblioteca redenrizadora de páginas para navegadores com suporte a DOOM e AJAX.
B Dalvik é um gerenciador de banco de dados para o armazenamento de dados estruturados.
C A camada *RunTime*, na arquitetura Android, fica acima de todas as outras camadas e é nela que as aplicações Java são executadas.
D Na arquitetura Android, a *Activity Manager*, presente na camada *Libraries*, gerencia a execução de uma *activity*, incluindo sua iniciação e seu término.
E A *Content Providers*, na arquitetura Android, gerencia as apresentações de janelas e os tratamentos gráficos das aplicações.

QUESTÃO 47

Considerando que a evolução dos sistemas de cabeamento das redes de computadores está intrinsecamente ligada ao aumento das taxas de transmissão, assinale a opção correta.

- A Os cabos de fibra óptica para uso interno, assim como os cabos metálicos CAT5/6, podem ser lançados nos mesmos dutos que a rede elétrica.
- B Os cabos de fibra óptica monomodo operam em um único comprimento de onda, por isso possuem menor alcance que os cabos de fibra multimodo, que operam em diversos comprimentos de onda.
- C Os cabos metálicos CAT5 ou CAT6, destinados a redes de computadores, não podem ser usados em sistemas de transmissão de voz ou em sistemas de PABX/PBX, dadas as limitações relacionadas à banda passante.
- D Cabos de fibra óptica que apresentam gel em sua estrutura ou em sua composição física não devem ser usados na estrutura interna de edifícios, devido a sua natureza inflamável.
- E O fenômeno físico da paradiafonia, ou *next*, é detectável por equipamentos que medem o espectro da luz ou ODTRs.

QUESTÃO 48

Com relação às técnicas de comutação de circuitos, pacotes e células, assinale a opção correta.

- A Em uma rede de pacotes, é obrigatório que cada pacote siga o mesmo caminho.
- B Em uma rede comutada por células do tipo ATM, o sincronismo é dispensável, pois o seu modo de transferência é assíncrono.
- C Em uma rede comutada por pacotes, o tamanho dos pacotes em baites deve ser o mesmo.
- D Na sinalização canal comum, cada canal tem o seu próprio subcanal de sinalização privado.
- E O congestionamento em uma rede de comutação de circuitos é detectado no momento do estabelecimento da conexão.

QUESTÃO 49

Com relação às redes locais, metropolitanas e de longa distância, assinale a opção correta.

- A O Ethernet utiliza um método de alocação de canal centralizado.
- B O protocolo Ethernet pode ser usado somente em redes locais ou em redes metropolitanas, pois é um protocolo de redes de curta distância.
- C Em um mesmo comutador, a técnica de separação de redes Ethernet em VLANs em nível 2 resolve o problema de colisão, mas não resolve o problema de *broadcast*.
- D Para um mesmo número de nós, a topologia de rede em estrela necessita de mais enlaces que a topologia *full-meshed*.
- E O tempo de propagação total de uma rede LAN, MAN ou WAN está diretamente relacionado à velocidade de transmissão do enlace medido.

QUESTÃO 50

Considerando que os modelos OSI e TCP/IP são utilizados como referência para o entendimento de sistemas de comunicação, assinale a opção correta.

- A A camada de transporte, obrigatória no modelo OSI e no modelo TCP/IP, admite apenas protocolos orientados à conexão.
- B A camada de enlace de dados, também conhecida como camada 2 do modelo OSI, é responsável pelo controle de fluxo e os endereços nela utilizados têm significado global.
- C A padronização das camadas é empregada para que, na comunicação, um nó possa ter acesso a qualquer camada do nó adjacente.
- D O TCP é um protocolo que atua na camada de transporte do modelo OSI e na camada de rede do modelo TCP/IP.
- E A camada 2 do modelo TCP/IP corresponde à camada 3 do modelo OSI, na qual o protocolo IP está descrito.

QUESTÃO 51

Com relação à família de protocolos TCP/IP, assinale a opção correta.

- A O protocolo RIPv2 trabalha com IPv4 e(ou) IPv6.
- B O uso do protocolo BGP é restrito à comunicação entre sistemas autônomos distintos.
- C O IPv6 e o IPv4 são compatíveis entre si, sendo o primeiro resultante de uma evolução do segundo, em função da escassez de endereços relativos à versão 4.
- D No protocolo OSPF, a comunicação relativa à troca de informação de roteamento entre nós de duas áreas ocorre por meio da área zero ou *backbone*.
- E O protocolo RIPv1 trabalha com IPv4 e sub-redes endereçadas com máscara de comprimento variável ou *classless*.

QUESTÃO 52

Com relação à arquitetura cliente/servidor, correio eletrônico e tecnologias associadas, assinale a opção correta.

- A Um usuário interessado em transferir para um *smartphone* o conteúdo de suas mensagens do servidor, a fim de as ler posteriormente, deverá utilizar o IMAP4, pois o POP3 não permite essa funcionalidade.
- B A primeira mensagem a ser recebida por um servidor SMTP por meio da porta 25 do protocolo UDP será HELO.
- C Em ambientes cliente/servidor, a RFC 822 é usada para a padronização de formato, sendo incompatível com o padrão X.400, que deixou de ser utilizado devido a sua forma complexa de implementação.
- D Considerando-se que o emprego do padrão ASCII é obrigatório em sistemas de comunicação, com o uso dos protocolos STMP, POP3 ou IMAP4, é correto afirmar que o campo *Sender*: (Transmissor:) é responsável por transportar a informação do DNS do primeiro destinatário.
- E O padrão MIME, desenvolvido a partir da necessidade de padronização na comunicação por *email*, é caracterizado pela codificação de qualquer símbolo por ASCII, excetuando-se os tratamentos específicos de diferenciação de línguas.

QUESTÃO 53

Considerando que os servidores de aplicação e *proxy* podem ser usados de diversas formas em um ambiente de redes, assinale a opção correta.

- **A** As redes DMZ ou zonas desmilitarizadas, por estarem ligadas diretamente à Internet, não devem conter servidores de aplicação de nenhum tipo.
- **B** O servidor *proxy* é um tipo de *gateway*, também usado em substituição a um *firewall*, pois se comunica com o navegador usando HTTP e, com os servidores, usando qualquer outro protocolo definido, incluindo-se o próprio HTTP.
- **C** Os *applets* são aplicações usadas para promover a interação dos clientes com os servidores de aplicação onde as mesmas aplicações executam suas funções.
- **D** A linguagem JAVA, empregada nos servidores de aplicação atuais, é orientada a objeto e pode usar todas as classes disponíveis na linguagem C, incluindo-se as primitivas de E/S ou I/O, presentes na JAVA e na C.
- **E** Um servidor de arquivos que utiliza a arquitetura .NET deve possuir uma única pilha para tratar, simultaneamente, o IPv4 e o IPv6, quando relacionados à comunicação com a camada de rede.

QUESTÃO 54

Considerando que os serviços de Voz sobre IP são importantes para a disseminação da Internet como meio de conexão multimídia, assinale a opção correta.

- **A** O H.248 e o MEGACO padronizam o MGC (*media gateway control*) e o MG (*media gateway*) em uma única camada.
- **B** No caso do H.323, a resposta a um INVITE será um OK.
- **C** O RTCP (*real time control protocol*) tem como função monitorar uma conexão fim-a-fim (*media stream*). Isso é também necessário devido ao fato do UDP não ser orientado a conexão.
- **D** A SS7 é um tipo de sinalização específica encontrada apenas no SIP; o H.323 usa o MEGACO para a mesma função.
- **E** Em uma rede que use o SIP como protocolo de estabelecimento de sessão, o *gatekeeper* tem a função de negociar as permissões de usuários.

QUESTÃO 55

A respeito dos diferentes modelos de banco de dados — relacional, rede, hierárquico, distribuído e orientado a objetos —, assinale a opção correta.

- **A** Em bancos de dados orientados a objetos, busca-se agrupar os dados e os códigos que manipulam esses dados em vários elementos formando um grafo, e podendo, como uma extensão do modelo hierárquico, cada segmento pai ter mais de um segmento filho, e cada segmento filho ter mais de um segmento pai.
- **B** No modelo em rede, representam-se os dados em um conjunto de árvores normalizadas, sendo possível modificar sua estrutura com facilidade, uma vez que não é preciso reconstruir o banco de dados.
- **C** Nos bancos de dados relacionais, representam-se os dados em um conjunto de tabelas inter-relacionadas, o que torna o banco de dados mais flexível no que concerne à tarefa de modificação da estrutura de uma tabela dentro desse banco de dados, porque não há necessidade de reconstruí-lo.
- **D** Segundo o padrão SQL ANSI, para a definição de um esquema de um banco de dados relacional, deve-se adotar uma linguagem de definição de dados usando hierarquias de classes baseadas em linguagens orientadas a objetos.
- **E** O modelo hierárquico se assemelha a um organograma com um segmento raiz e um número qualquer de segmentos subordinados, podendo cada segmento filho ter mais de um segmento pai.

QUESTÃO 56

Acerca da aplicação dos princípios de normalização (Formas Normais), assinale a opção correta.

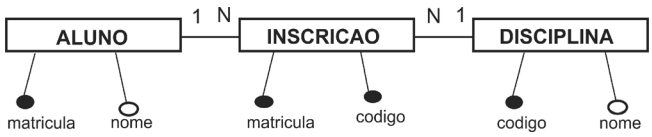
- **A** A aplicação da 1FN se dá se e somente se, para todo modelo, for aplicada a Forma Normal de Boyce-Codd (ou BCNF).
- **B** A 2FN é baseada no conceito de dependência funcional total, isto é, todo atributo não primário de uma entidade tem dependência funcional total da chave primária.
- **C** A Terceira Forma Normal (3FN) requer que não haja dependências intransitivas de atributos que não sejam com toda chave candidata.
- **D** A aplicação da Primeira Forma Normal (1FN) requer que, ao fim da sua aplicação, todos os atributos de uma relação sejam multivalorados ou estejam em tabelas aninhadas, o que garante grupos repetidos de dados, reduzindo o tamanho físico do banco de dados.
- **E** A Segunda Forma Normal (2FN) requer que, ao fim da sua aplicação, não haja dependências transitivas de atributos que não sejam com toda chave candidata.

QUESTÃO 57

Considere que existe uma entidade PESSOA com um relacionamento denominado CASAMENTO que pode associar diversas ocorrências na mesma entidade PESSOA. De acordo com as propriedades do diagrama entidade-relacionamento, o conceito desse relacionamento (CASAMENTO) pode ser definido como

- **A** generalização.
- **B** relacionamento binário.
- **C** autorrelacionamento.
- **D** entidade associativa.
- **E** especialização.

QUESTÃO 58



O modelo lógico apresentado dá origem às tabelas ALUNO, INSCRICAO e DISCIPLINA. Considerando esse modelo e sabendo que não há nenhum procedimento armazenado no banco de dados, assinale a opção que apresenta código em SQL ANSI que resultará corretamente na listagem de matricula e nome dos alunos que estão inscritos (INSCRICAO) em mais de duas disciplinas.

A
```
SELECT aluno.matricula, aluno.nome
FROM inscricao, aluno, disciplina
WHERE inscricao.matricula=aluno.matricula
AND inscricao.codigo=disciplina.codigo
GROUP BY aluno.matricula, aluno.nome
HAVING COUNT(*) > 2
```

B
```
SELECT aluno.matricula, aluno.nome
FROM inscricao, aluno, disciplina
WHERE inscricao.matricula=aluno.matricula
AND inscricao.codigo=disciplina.codigo
AND COUNT(*) > 2
```

C
```
SELECT aluno.matricula, aluno.nome
GROUP BY aluno.matricula, aluno.nome
FROM inscricao, aluno, disciplina
WHERE inscricao.matricula=aluno.matricula
AND inscricao.Codigo=diciplina. Codigo AND
COUNT
```

D
```
SELECT aluno.matricula, aluno.nome
FROM inscricao, aluno, disciplina
WHERE inscricao.matricula=aluno.matricula
AND quantidade > 2
GROUP BY inscricao, aluno, disciplina
```

E
```
SELECT aluno.matricula, aluno.nome, SUM() > 2
FROM inscricao, aluno, disciplina
WHERE inscricao.matricula=aluno.matricula
AND inscricao.codigo=disciplina.codigo
GROUP BY aluno.matricula, aluno.nome
```

QUESTÃO 59

Considerando um SGBD que respeite os padrões SQL ANSI-99, assinale a opção que apresenta corretamente um comando SQL para apagar determinados registros de uma tabela pessoa (cpf, nome, sexo) que contém registros cujo campo sexo apresenta valores iguais a 'M' e 'F'.

A `DROP pessoa WHERE sexo='M'`

B `UPDATE pessoa SET sexo=NULL WHERE sexo='M'`

C `FROM pessoa WHERE sexo='M' DELETE sexo`

D `DELETE sexo FROM pessoa WHERE sexo='M'`

E `DELETE FROM pessoa WHERE sexo='M'`

QUESTÃO 60

A respeito das características de um SGBD e das atividades de administração de banco de dados, assinale a opção correta.

A Para fins práticos, é necessário distinguir diferentes cardinalidades máximas, que podem ser maiores ou iguais a zero.

B A característica autodescritiva de um banco de dados define que o banco de dados contém o próprio dado assim como uma descrição desses dados e suas restrições. Essas descrições e restrições estão armazenadas no catálogo (dicionário) do SGBD.

C A independência física de dados consiste na habilidade de modificar o esquema conceitual sem a necessidade de reescrever os programas aplicativos. As modificações no nível conceitual são necessárias quando a estrutura lógica do banco de dados é alterada.

D Na linguagem SQL, os comandos DDL GRANT e ROLLBACK permitem a implementação de um controle de acesso discricionário, criando e retirando permissões no banco de dados.

E A coleção das informações armazenadas em um banco de dados, em determinado momento, corresponde ao esquema do banco de dados.

QUESTÃO 61

Existem dois esquemas lógicos para a implementação de um modelo de BI que envolve tabelas de fato e tabelas de dimensões: o esquema estrela (*star schema*) e o floco-de-neve (*snow-flake schema*). Acerca do esquema estrela, assinale a opção correta.

A No esquema estrela, diversas tabelas de dimensão se relacionam tanto com diversas tabelas fato como com outras tabelas de dimensão, apresentando chaves ligando todas essas tabelas.

B No esquema estrela, as tabelas de dimensão são organizadas em uma hierarquia por meio da sua normalização, com vistas a diminuir o espaço ocupado, eliminando-se, assim, quaisquer redundâncias.

C O esquema estrela exige o uso de tabelas normalizadas.

D No esquema estrela, cada tabela de dimensão está relacionada a várias tabelas de fato, formando uma estrutura na qual a tabela de dimensão se relaciona com várias tabelas de fato obrigatoriamente.

E O esquema estrela consiste em uma tabela de fato com várias tabelas para cada dimensão e propõe uma visão cuja principal característica é a presença de dados redundantes nas tabelas de dimensão.

QUESTÃO 62

Considerando um SGBD Oracle, MySQL ou PostgreSqQL que contém uma tabela pessoa com mais de 3 registros, assinale a opção que apresenta a declaração de um comando SQL (que está entre aspas duplas) que permite selecionar o campo nome dos três primeiros registros dessa tabela segundo a ordem ascendente do campo idade.

- **A** O comando "`SELECT nome FROM pessoa ORDER BY idade LIMIT 3`" será executado corretamente no SGBD PostgreSQL.
- **B** O comando "`SELECT nome FROM pessoa WHERE ROWNUM<3`" será executado corretamente no SGBD MySQL.
- **C** O comando "`SELECT nome FROM pessoa WHERE ROWNUM<3`" será executado corretamente no SGBD PostgreSQL.
- **D** O comando "`SELECT TOP 3 nome FROM pessoa ORDER BY idade`" será executado corretamente no SGBD PostgreSQL.
- **E** O comando "`SELECT TOP 3 nome FROM pessoa ORDER BY idade`" será executado corretamente no SGBD MySQL.

QUESTÃO 63

Considere que a equipe composta por quatro analistas de sistemas de um órgão do judiciário federal brasileiro deva desenvolver um plano de implantação da gerência de riscos de segurança da informação nesse órgão. Acerca das atividades que podem ser realizadas pela equipe, e considerando os conceitos de gerência de riscos, de classificação e controle dos ativos de informação, e a norma ISO/IEC 27005, é correto afirmar que essa equipe

- **A** deve produzir ou obter a lista de processos de negócios aos quais estarão vinculados os demais ativos de informação a serem identificados na atividade de identificação de riscos.
- **B** deve particionar entre os quatro membros a responsabilidade pelo desempenho dos seguintes papéis, entre outros: identificação e análise das partes interessadas, estabelecimento de ligações com as funções de gerência de riscos de alto nível, especificação dos critérios para a avaliação dos riscos, estimativa de impactos e aceitação do risco para a organização.
- **C** deve aplicar uma metodologia de análise quantitativa de riscos, excluindo a aplicação de uma metodologia qualitativa.
- **D** deve implantar o sistema de gestão de segurança da informação, antes de desenvolver o plano de gestão de riscos.
- **E** deve particionar entre seus quatro membros a responsabilidade da execução simultânea das seguintes atividades: definição do escopo, identificação dos riscos, tratamento dos riscos e comunicação do risco.

QUESTÃO 64

A equipe de analistas de segurança da informação de um órgão do judiciário federal participou de uma atividade de capacitação conduzida por uma empresa de consultoria em controle de acessos, tendo sido submetida a uma avaliação preliminar de seus conhecimentos sobre esse tema. A avaliação baseou-se em debate mediado pelos membros da consultoria, durante o qual os membros da equipe de segurança discutiram com os usuários de TI um conjunto de afirmações acerca da melhor forma de aprimorar o controle de acessos no órgão. Várias ponderações conduzidas pelos consultores eram deliberadamente errôneas, e algumas, verdadeiras. A equipe de analistas de segurança e os usuários de TI deveriam identificar as ponderações erradas e as verdadeiras.

Considerando que as opções a seguir apresentam ponderações dos consultores, assinale a opção que apresenta ponderação correta, com base nos conceitos do controle de acessos e nas normas da ISO/IEC 27001, 27002 e 27005.

- **A** A segregação de regras de controle de acessos no órgão é fundamentada na ideia de que o atendimento a pedidos de acesso, a autorização dos acessos propriamente ditos e a administração dos acessos são realizados por uma mesma pessoa no órgão.
- **B** A abordagem e o desenho dos controles de acesso físico e lógico no órgão deve ser feita de forma independente.
- **C** A autenticação baseada em três fatores é válida unicamente para sistemas de controle de acesso lógico, e não para sistemas de controle de acesso físico.
- **D** Em aderência aos controles previstos pela norma ISO/IEC 27001, faz-se necessário utilizar a autenticação baseada em dois fatores, tanto no acesso de origem externa à rede quanto no acesso de qualquer usuário ao sistema operacional, desde que esses ativos estejam incluídos em um escopo de implantação de um sistema de gestão da segurança da informação.
- **E** Para que os controles de acessos físico e lógico sejam implementados de forma consistente em diferentes sistemas e redes do órgão, é recomendada a prévia classificação, quanto à segurança necessária, dos ativos de informação a eles relacionados.

QUESTÃO 65

Um inquérito administrativo foi aberto para a apuração de responsabilidades pelos impactos da paralisação das atividades de determinado órgão do Judiciário brasileiro, em decorrência de um desastre ocorrido na área de TI. Uma equipe, composta por pessoal interno ao órgão e por investigadores independentes, contratados para assessorar as investigações, inquiriu a equipe que atua na área de segurança da informação, entre outras pessoas, tendo realizado entrevistas, coletado evidências e apresentado pareceres sobre a fragilidade dos planos de continuidade de negócios do órgão, bem como sobre os controles de becape, tratamento de incidentes e problemas. Foram evidenciadas algumas falhas conceituais, tanto operacionais quanto estratégicas, entre várias outras evidências de comportamento consistente.

Considerando essa situação e os conceitos de planos de continuidade de negócio, becape, recuperação de dados e tratamento de incidentes e problemas, assinale a opção que apresenta evidência de comportamento consistente.

A Suponha que o órgão tenha adotado uma política de continuidade que não estava baseada na análise de seus riscos próprios, mas sim baseada na cópia do documento de política obtido de outro órgão do Judiciário. Nessa situação, a política adotada está coerente com a estratégia de simplificação, uniformização e redução de custos no levantamento de requisitos de segurança para o negócio, prescrito na norma ISO/IEC 27002.

B Considerando-se que, após o desastre, uma greve e a consequente falta de funcionários na área de TI tenha implicado uma demora excessiva para recuperação de dados e operações essenciais do órgão, é correto afirmar que não havia erro no plano de recuperação, pois não existe prescrição para a observância do elemento pessoas na implementação da continuidade de negócios na norma ISO/IEC 27001.

C Considere que não havia contratação de seguro contra a perda de dados no órgão. Nesse caso, a ausência do seguro não seria evidência de que havia problemas com o plano de continuidade.

D Considere que não existiam no órgão pessoas de nível hierárquico elevado com responsabilidade pela coordenação do processo de gestão de continuidade de negócios. Nesse caso, não há indicação de que existiam problemas com o plano de continuidade de negócios.

E Considerando que o órgão não mantinha uma cópia de segurança das chaves criptográficas usadas no resguardo do sigilo de algumas informações armazenadas nos seus computadores, o que permitiu a recuperação apenas parcial de dados do becape, é correto afirmar que ocorreu um incidente, mas não um problema, com o sistema de becape.

QUESTÃO 66

Considerando que um conjunto de *malwares* de computador tenha sido detectado no ambiente computacional de um órgão público do Judiciário brasileiro, assinale a opção correta.

A Se um *adware* é detectado em ampla circulação na rede, no parque das máquinas de usuário final, então isso indica a existência de vulnerabilidades nos sistemas de gerenciamento de bancos de dados do órgão.

B Se um *worm* (verme) é detectado em ampla circulação na rede, no parque de máquinas de usuário final, isso indica que é necessário tornar as regras de *firewalls* internos à rede menos restritivas.

C Se um vírus é detectado em circulação na rede do órgão, então é altamente provável que ele tenha sido injetado na rede por meio de outro *malware* do tipo *keylogger*.

D Se um *keylogger* é detectado em ampla circulação na rede do órgão, então, de forma proporcional ao índice de infestação, os dados pessoais dos usuários da rede correm o risco de serem indevidamente copiados.

E Se um *ransomware* é detectado em circulação na rede, no parque das máquinas de usuário final, então isso indica iminente risco de consumo indevido de banda passante na rede de computadores do órgão.

QUESTÃO 67

Considerando os conceitos de segurança de redes, ataques, *malwares* e monitoramento de tráfego, assinale a opção correta.

A Um ataque de engenharia social bem-sucedido constrói situações fictícias que manipulam psicologicamente uma pessoa, conduzindo-a a realizar ações indevidas.

B Um *rootkit* é um tipo de *malware* facilmente detectável pelos administradores de uma rede.

C Os ataques de *spamming* em geral são precedidos por ataques de *phishing*.

D *Screenloggers* são programas de computador que geram incidentes ou problemas de segurança na rede por meio da geração de alto consumo da sua banda.

E O *payload* de um *malware* é um programa de computador que captura indevidamente o tráfego de pacotes TCP/IP que circulam na rede.

QUESTÃO 68

Considerando que, a fim de monitorar o tráfego na rede de computadores de determinado órgão, tenha-se empregado um *sniffer* de rede, entre outras ferramentas, assinale a opção correta com base nos conceitos de monitoramento de tráfego, *sniffer* de rede e interpretação de pacotes.

A O *payload* de um datagrama de consulta ao DNS possui tamanho fixo de 32 baites, sendo os dois primeiros baites indicadores do *transaction id* da consulta.

B Para a captura e análise de tráfego de um computador individual na rede, com vistas ao diagnóstico de problemas de desempenho nesse computador, é suficiente posicionar outro computador com *sniffer* de rede junto a qualquer porta do *switch* ao qual o primeiro se conecta por meio cabeado.

C Na inspeção de um *frame* Ethernet II capturado por um *sniffer* de rede, tal com o Wireshark, é possível identificar os seis primeiros baites do *frame*, que representam o endereço IP do *host* destino, bem como os seis baites seguintes, que representam o endereço IP do *host* origem.

D O *payload* de um *frame* Ethernet II que transporta um pacote IPv4 se inicia com o valor 0×4.

E O *payload* de um *frame* Ethernet II que transporta um pedido ARP (*request*) em uma rede IPv4 possui o tamanho de 28 baites, sendo os 20 últimos baites relativos a endereçamentos MAC e(ou) IP, dos *hosts* origem e destino de comunicações posteriores.

QUESTÃO 69

Acerca de detecção e prevenção de ataques com uso de IDS e IPS, arquiteturas de *firewalls* e ataques e ameaças da Internet e de redes sem fio, assinale a opção correta.

A A detecção de intrusão possível com o uso de IDS do tipo *host-based* em uma rede com centenas de máquinas de usuário apresenta maior facilidade de gerenciamento e instalação, quando comparada ao uso de IDS do tipo *network-based*.

B O uso de *firewalls stateless* relaciona-se a uma melhor chance de identificação de vírus, *spams* e intrusões em circulação na rede, quando comparado ao uso de um *firewall* que analisa o tráfego de uma rede com base em inspeção profunda de pacotes (*deep packet inspection*).

C Tanto o *firewall* do tipo dual *homed* quanto o do tipo *stateless* previnem a ocorrência de ataques do tipo SYN *flood*.

D O emprego de assinaturas atômicas em um sistema de prevenção de intrusão permite a construção de sistemas mais simples, quando comparado com os que empregam assinaturas *stateful*.

E O uso de IPS do tipo *network-based*, quando comparado ao uso de IPS *host-based*, possibilita a coleção de dados mais detalhados acerca de chamadas de funções e acessos a arquivos.

QUESTÃO 70

No que se refere à criptografia, seus conceitos básicos, sistemas simétricos e assimétricos, certificação e assinatura digital, e protocolos criptográficos, assinale a opção correta.

A O único sistema criptográfico matematicamente inviolável é conhecido pelo nome de One Time Pad, e o comprometimento de seu uso ocorre na eventualidade de falhas na geração de chaves aleatórias, na reutilização dessas chaves ou na sua guarda.

B No que se refere ao uso de cifradores simétricos, uma cifra de fluxo é mais adequada quando se executa a cifração de arquivos com tamanho limitado, enquanto cifras de bloco são mais adequadas para arquivos de tamanho ilimitado.

C O uso de funções *oneway*, ou de *hash* criptográfico, é opcional para a construção de assinaturas digitais convencionais.

D O protocolo de troca de chaves conhecido como Diffie-Hellman viabiliza a geração de chaves criptográficas assimétricas.

E São exemplos de primitivas criptográficas utilizadas na construção de sistemas criptográficos: Standard TLS, IPSec, Kerberos e X.509.

Espaço livre