

**CONHECIMENTOS ESPECÍFICOS****QUESTÃO 31**

Em relação aos conceitos de orientação a objetos, assinale a opção correta.

- A A alteração no método de uma classe modifica o comportamento dos objetos das suas subclasses.
- B Com a herança múltipla, todos os métodos de cada uma das superclasses passam a compor o comportamento das subclasses.
- C Em um programa orientado a objetos, os métodos a serem efetivamente executados podem não estar determinados em tempo de compilação.
- D Todas as classes de um programa orientado a objetos implementam ou herdam métodos que deverão compor o comportamento dos seus objetos instanciados.
- E O polimorfismo permite construir uma hierarquia de classes em que todo o comportamento comum esteja concentrado na superclasse, sendo implementados na subclasse apenas métodos não definidos na superclasse.

**QUESTÃO 32**

Assinale a opção correta acerca do NET Framework.

- A O Garbage Colector atua a cada instanciação de objetos com o objetivo de liberar espaço de memória referente a objetos que não mais estejam em uso.
- B Objetos de uma classe, quando passados como parâmetros, não permitem alterações, visto que a passagem é sempre feita por valor.
- C Uma enumeração pode ser de qualquer tipo, apesar de, por definição, ter o tipo *int*.
- D A ocorrência de uma exceção é tratada por meio da instanciação da classe *Exception*, ou de uma classe derivada da classe *Exception* e da captura desse objeto.
- E A classe *BitVector32* apresenta melhor desempenho em comparação com a classe *BitArray*, embora elas tenham a mesma funcionalidade.

**QUESTÃO 33**

Com base em aplicações *web*, assinale a opção correta.

- A Para validar usuários, o Form Authentication utiliza credenciais que devem ser armazenadas no arquivo de configuração da aplicação.
- B Utilizando-se ASP, é impossível, nos casos em que o *browser* não suporta o uso de *cookies*, passar informações de uma página para outra em uma aplicação.
- C No LINQ, os métodos que implementam operadores de consulta padrão devem ser chamados com o uso da sintaxe de métodos estáticos.
- D Usando-se ADO.NET, a conexão com um *data source* fornece as informações de autenticação necessárias e deve ser feita com a utilização de um objeto *Connection*, que depende do tipo de *data source* adotado.
- E No Padrão MVC, as regras do negócio que definem a forma de acesso e modificação dos dados são geridas pelo controlador.

**QUESTÃO 34**

Assinale a opção em que é apresentada uma recomendação de acessibilidade expressa no modelo e-Mag.

- A As páginas de uma aplicação *web* devem ser criadas com atualização automática.
- B As páginas de aplicações *web* não devem estabelecer limite de tempo de execução.
- C Os *links* de uma página só podem remeter a páginas no mesmo sítio.
- D Os arquivos devem ser disponibilizados preferencialmente no formato pdf.
- E Novas janelas só devem ser abertas com permissão do usuário.

**QUESTÃO 35**

A arquitetura de interoperabilidade do governo federal, e-Ping, estabelece que

- A os sistemas do governo que forneçam serviços de governo eletrônico por meio da Internet devem, necessariamente, ser projetados para uso em navegadores.
- B os serviços de governo eletrônico que disponibilizem documentos, as informações quanto a sua versão e a data de publicação devem estar disponibilizadas no próprio documento.
- C os serviços de governo eletrônico devem ser construídos de forma que todos os sítios utilizem HTTP.
- D os sistemas de informação do governo devem prever a construção de adaptadores que permitam o acesso às informações por diversos ambientes.
- E os sistemas que forneçam serviços eletrônicos devem ser capazes de utilizar a Internet como meio de comunicação.

**QUESTÃO 36**

Com relação aos padrões XML, XSTL, UDDI, WSDL e SOAP, assinale a opção correta.

- A Um documento XML pode conter caracteres não ASCII.
- B No processo de transformação realizado pelo XSLT, os *templates* de regras devem ser construídos de forma a não existirem conflitos de regras, visto que esses conflitos não podem ser automaticamente resolvidos.
- C No UDDI, quando uma entidade é apagada, são também apagadas todas as entidades referenciadas por ela.
- D No WSDL, o elemento de definição de serviço *message* fixa o formato de acesso ao serviço.
- E Uma limitação do SOAP é a exigência do uso do HTTP como transporte.

**QUESTÃO 37**

De acordo com SOA, a perspectiva arquitetural que considera o suporte aos objetos de negócio e suas implementações denomina-se

- A arquitetura de implementação.
- B arquitetura de negócio.
- C arquitetura de aplicação.
- D arquitetura de serviço.
- E arquitetura de componente.

**QUESTÃO 38**

Quando um *portlet* é colocado em uma página de portal, os dados armazenados na *PortalSession*

- A serão passíveis de compartilhamento se não tiverem sido alterados pela *portlet*.
- B serão automaticamente compartilhados com todas as *portlets* da mesma aplicação.
- C ficarão necessariamente restritos à *portlet* à qual pertencem.
- D será possível mantê-los acessíveis a qualquer *portlet* que faça parte da mesma aplicação.
- E serão compartilhados com todas as aplicações que estejam em execução.

**QUESTÃO 39**

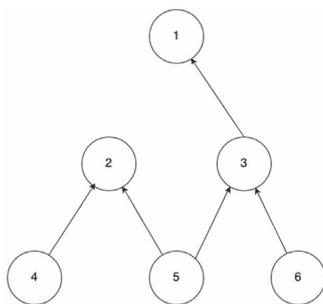
Na construção de um RSS, o elemento que determina o tempo para que o canal seja recarregado de sua fonte é

- A refreshTime.
- B skipHours.
- C nextRefresh.
- D timeToRefresh.
- E ttl.

**QUESTÃO 40**

Para vendas durante o período de natal, uma loja decidiu criar na *web* um sítio exclusivo, em que os itens vendidos podem ser pesquisados a partir da seção à qual pertencem. Nesse modo de pesquisa, a forma de estruturação da informação utilizada foi

- A a hierarquia.
- B a localização.
- C o alfabeto.
- D o tempo.
- E a categoria.

**QUESTÃO 41**

Considerando o grafo ilustrado acima, assinale a opção em que é apresentada a descrição em vértices (V) e arestas (A).

- A  $V = \{1, 2, 3, 4, 5, 6\}$   
 $A = \{(2, 4), (2, 3), (2, 5), (3, 6), (1, 5)\}$
- B  $V = \{2, 4, 1, 3, 6, 5\}$   
 $A = \{(4, 2), (1, 3), (5, 2), (6, 3), (5, 3)\}$
- C  $V = \{1, 2, 3, 4, 5, 6\}$   
 $A = \{(4, 2), (3, 4), (5, 2), (6, 3), (5, 3)\}$
- D  $V = \{1, 2, 3, 4, 5, 6\}$   
 $A = \{(4, 2), (3, 1), (5, 1), (6, 2), (5, 3)\}$
- E  $V = \{2, 4, 1, 3, 6, 5\}$   
 $A = \{(4, 2), (3, 1), (5, 2), (6, 3), (5, 3)\}$

**QUESTÃO 42**

O processo de ordenação de vetores que busca o menor elemento do vetor e o insere na primeira posição do vetor e que, posteriormente, busca o segundo menor valor do vetor e o coloca na segunda posição do vetor, e assim sucessivamente até que todo o vetor esteja ordenado, denomina-se

- A ordenação por seleção.
- B ordenação *merge sort*.
- C busca linear.
- D busca binária.
- E ordenação por inserção.

**QUESTÃO 43**

Quando executada no servidor, a aplicação, disponível para Windows e Linux, que gera documentos HTML, coleta dados de formulários, gera páginas com conteúdo dinâmico ou envia e recebe *cookies* é denominada

- A HTTP.
- B SMTP.
- C DHCP.
- D PHP.
- E FTP.

**QUESTÃO 44**

O conjunto de operações cujo resultado seja uma nova relação e que envolve seleção, projeção, união e produto cartesiano é denominado

- A mapeamento de cardinalidades.
- B álgebra relacional.
- C generalização.
- D chave primária.
- E herança.

**QUESTÃO 45**

Assinale a opção em que são apresentados tipos abstratos de dados.

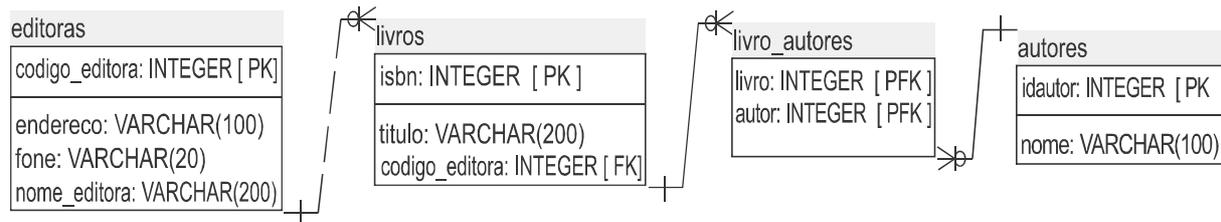
- A Float e pilha
- B Int e fila
- C fila-carro e pilha-carro
- D *byte* e *boolean*
- E Int e float

**QUESTÃO 46**

Em um sistema, podem ocorrer diversos tipos de falhas. Um tipo de falha simples de tratar é aquele que não resulta em perda de dados no sistema. Considerando essa informação, o procedimento que possibilita o armazenamento de informações acerca das transações executadas em um banco de dados denomina-se

- A *log* de chaves primárias.
- B *trigger*.
- C *backup* total.
- D *stored procedures*.
- E mapeamento de cardinalidades.

## QUESTÃO 47



Considerando o diagrama de entidade e relacionamento presente na figura acima, assinale a opção em que é apresentada a expressão DDL (*data definition language*) utilizada para criar as tabelas, as chaves e os relacionamentos descritos.

- A**
- ```

create table autores (
  idautor integer primary key,
  nome varchar(100)
);
create table editoras (
  codigo_editora integer primary key,
  endereco varchar(100),
  fone varchar(20),
  nome_editora varchar(200)
);
create table livros (
  isbn integer primary key,
  titulo varchar(200),
  codigo_editora integer,
  constraint fk_livros_editores foreign key (codigo_editora) references editoras
);
create table livro_autores (
  livro integer primary key,
  autor integer,
  constraint fk_livro_autores foreign key (livros) references livros,
  constraint fk_livro_livros foreign key (autores) references autores
);
  
```
- B**
- ```

create table autores (
  idautor integer primary key,
  nome varchar(100)
);
create table editoras (
  codigo_editora integer primary key,
  endereco varchar(100),
  fone varchar(20),
  nome_editora varchar(200)
);
create table livros (
  isbn integer primary key,
  titulo varchar(200),
  codigo_editora integer,
  constraint fk_livros_editores foreign key (codigo_editora) references editoras
);
create table livro_autores (
  livro integer,
  autor integer,
  constraint pk_livro_autores primary key (livro, autor),
  constraint fk_livro_autores foreign key (autor) references autores,
  constraint fk_livro_livros foreign key (livro) references livros
);
  
```

- C**
- ```

create table autores (
  idautor integer,
  nome varchar(100),
  constraint primary key (nome)
);
create table editoras (
  codigo_editora integer,
  endereco varchar(100),
  fone varchar(20),
  nome_editora varchar(200),
  constraint primary key (fone)
);
create table livros (
  isbn integer,
  titulo varchar(200),
  codigo_editora integer,
  constraint primary key (isbn),
  constraint fk_livros_editores foreign key (codigo_editora) references editoras
);
create table livro_autores (
  livro integer,
  autor integer,
  constraint pk_livro_autores primary key (livro, autor),
  constraint fk_livro_autores foreign key (autor) references autores,
  constraint fk_livro_livros foreign key (livro) references livros
);

```
- D**
- ```

create table autores (
  idautor integer,
  nome varchar(100)
);
create table editoras (
  codigo_editora integer,
  endereco varchar(100),
  fone varchar(20),
  nome_editora varchar(200)
);
create table livros (
  isbn integer,
  titulo varchar(200),
  codigo_editora integer
);
create table livro_autores (
  livro integer,
  autor integer
);
alter table autores add constraint primary key (nome);
alter table editoras add constraint primary key (fone);
alter table livros add constraint primary key (isbn);
alter table livros add constraint fk_livros_editores foreign key (codigo_editora) references editoras;
alter table livro_autores add constraint pk_livro_autores primary key (livro, autor),
alter table livro_autores add constraint fk_livro_autores foreign key (autor) references autores,
alter table livro_autores add constraint fk_livro_livros foreign key (livro) references livros

```
- E**
- ```

create table editoras (
  idautor integer primary key,
  nome varchar(100)
);
create table autores (
  codigo_editora integer primary key,
  endereco varchar(100),
  fone varchar(20),
  nome_editora varchar(200)
);
create table livros_autores (
  isbn integer primary key,
  titulo varchar(200),
  codigo_editora integer,
  constraint fk_livros_editores foreign key (codigo_editora) references editoras
);
create table livro (
  livro integer,
  autor integer,
  constraint pk_livro_autores primary key (livro, autor),
  constraint fk_livro_autores foreign key (autor) references autores,
  constraint fk_livro_livros foreign key (livro) references livros
);

```

**QUESTÃO 48**

A ferramenta presente no SQL Server que, após analisar uma carga de trabalho, pode recomendar a adição, remoção ou modificação de estruturas de *design* físicas em bancos de dados é denominada

- A SQL Server Studio.
- B SQL Server Admin.
- C SQL Server Configuration Manager.
- D Orientador de Otimização do Mecanismo de Banco de Dados.
- E SQL Server Profiler.

**QUESTÃO 49**

Assinale a opção em que é apresentada uma folha de estilo composta por camadas, que é utilizada para definir a apresentação em páginas da Internet que adotam linguagens de marcação, como XML, HTML e XHTML.

- A TAG
- B COOKIE
- C XML
- D CSS
- E DIV

**QUESTÃO 50**

Uma forma de observação de dados de uma ou mais entidades que compõem uma base de dados e que é considerada uma tabela virtual ou consulta armazenada denomina-se

- A esquema conceitual.
- B entidade.
- C chave primária.
- D integridade referencial.
- E *views*.

**QUESTÃO 51**

Com relação às etapas para elaboração do planejamento estratégico, assinale a opção correta.

- A Na primeira etapa do planejamento estratégico, são verificados os acertos e as falhas da implementação ou da estratégia em relação aos objetivos.
- B As etapas de um plano estratégico não possuem limite de tempo, visto que as estratégias podem ser alteradas durante a sua execução.
- C Independentemente da organização e da metodologia adotada, a sequência de etapas para elaboração de um plano estratégico é rígida e sem variações.
- D As etapas do plano estratégico devem ter início e fim, além de não serem concorrentes ou paralelas no *cômputo* total.
- E A orientação adotada por uma organização e a sua função são repensadas na etapa de avaliação da estratégia vigente.

**QUESTÃO 52**

No que se refere ao planejamento estratégico de TI e ao *balanced scorecard* (BSC), assinale a opção correta.

- A O BSC reflete o equilíbrio entre os objetivos de curto e de longo prazo, entre medidas financeiras e não financeiras, pois suas perspectivas são clientes, financeira, objetivos internos e conhecimento.
- B O BSC é um método desenvolvido especificamente para o planejamento da área de TI de uma empresa e tem implicações diretas na definição de sistemas de informação com impacto estratégico.
- C O BSC é um método utilizado para medição e gestão das ações empresariais, portanto não deve ser utilizado juntamente com o planejamento estratégico de TI.
- D O mapa estratégico de TI desenvolvido por intermédio do BSC é mais estratégico para as áreas de negócio da empresa que para o planejamento estratégico.
- E A formulação do BSC é orientada à estratégia, sendo útil para esclarecer e traduzir a visão e a estratégia, comunicar e associar objetivos e medidas, planejar, estabelecer metas e alinhar expectativas, inclusive para um plano estratégico de TI.

**QUESTÃO 53**

Considere que, em uma organização matricial fraca, o poder gerencial de dois gerentes de projeto seja limitado. Um gerente percebeu que, na verdade, é um facilitador de projetos e o outro, que atua como coordenador de projetos. Considerando essa situação hipotética, é correto afirmar que o gerente facilitador de projetos

- A está subordinado a um gerente de nível mais alto que o nível praticado por ele.
- B possui autoridade em relação a alguns assuntos.
- C é um gerente funcional típico de organizações matriciais fracas.
- D pode tomar mais decisões que o coordenador de projetos.
- E não pode tomar decisões.

**QUESTÃO 54**

Os conhecimentos contidos no PMBOK representam as boas práticas aceitas pela comunidade de gerentes de projetos. Nesse sentido, é correto afirmar que esses conhecimentos

- A devem constituir a base para o gerenciamento de projetos sem, contudo, substituir o julgamento do gerente do projeto e de sua equipe.
- B derivam de um método científico utilizado como apoio às atividades gerenciais.
- C foram criados para que as organizações filiadas e os projetos tenham sucesso garantido.
- D devem ser aplicados indiscriminadamente em todos os projetos e atividades da organização.
- E representam, para o gerente de projetos, aquilo que é necessário para a obtenção de uma certificação profissional em gerenciamento, o que garante o sucesso dos projetos em que o gerente vier a atuar.

**QUESTÃO 55**

Ao término da primeira fase de um projeto, o gerente do projeto deve, antes de ser iniciada a fase seguinte,

- A** verificar o progresso do projeto comparado à sua linha de base.
- B** redigir o relatório de desempenho para o devido acompanhamento pelo PMO (escritório de projetos) da organização.
- C** confirmar se os objetivos da primeira fase foram alcançados e obter o aceite formal das entregas.
- D** recomendar ações corretivas para alinhar os resultados do projeto às expectativas do projeto.
- E** verificar se os recursos estão disponíveis para a próxima fase.

**QUESTÃO 56**

Ao executar o processo de identificar os riscos, um gerente de projeto redigiu uma lista completa dos riscos identificados por todas as partes interessadas, utilizando-se de diversos métodos. Desse modo, ele verificou se todos os riscos haviam sido entendidos e se os gatilhos haviam sido devidamente identificados. Posteriormente, no processo de planejar as respostas aos riscos, esse gerente considerou todos os riscos identificados pelas partes interessadas e determinou formas de mitigá-los.

Com base nessa situação hipotética, assinale a opção em que é apresentado um erro cometido pelo gerente do projeto.

- A** Outras pessoas responsáveis pelas respostas a riscos deveriam estar envolvidas nesse processo de planejamento e não apenas o gerente.
- B** Os gatilhos não foram identificados anteriormente ao processo de identificar os riscos.
- C** O gerente do projeto não aguardou até o processo de realizar a análise qualitativa dos riscos para envolver as partes interessadas.
- D** A lista priorizada de riscos é uma saída do processo de planejar o gerenciamento dos riscos e não do processo de identificar os riscos.
- E** O gerente do projeto não desenvolveu soluções de contorno.

**QUESTÃO 57**

A melhor descrição de problema para o ITIL v3 é

- A** qualquer ação ou pessoa que ocasione a interrupção do serviço.
- B** um erro conhecido de um ou mais incidentes.
- C** a causa conhecida de uma interrupção.
- D** um ou mais erros conhecidos.
- E** a causa raiz de um ou mais incidentes.

**QUESTÃO 58**

O processo do ITIL v3 que utiliza o tempo médio entre falhas (TMEF) corresponde ao gerenciamento

- A** da continuidade dos serviços em TI.
- B** do nível de serviço.
- C** da segurança da informação.
- D** da disponibilidade.
- E** da capacidade.

**QUESTÃO 59**

Presente nas publicações do ITIL v3 relativas à melhoria contínua de serviço, ao desenho de serviço e à estratégia de serviço, a modelagem analítica

- A** é utilizada para avaliar e dimensionar os recursos de TI necessários ao gerenciamento da capacidade, sendo normalmente empregada no gerenciamento de disponibilidade e no gerenciamento de risco.
- B** utiliza-se de modelos matemáticos para prever o comportamento de serviços de TI, sendo empregada no gerenciamento de capacidade e no gerenciamento de disponibilidade.
- C** constitui uma técnica de projeto lógico normalmente empregada em serviços de TI relacionados a banco de dados, sendo uma técnica contrastante com a modelagem entidade-relacionamento.
- D** é utilizada para avaliar e dimensionar os itens de TI necessários à operação do serviço, sendo normalmente empregada no gerenciamento da capacidade.
- E** constitui uma técnica similar à modelagem de dados, sendo também aplicável às publicações do ITIL.

**QUESTÃO 60**

De acordo com o ITIL v3, constitui item de configuração (IC)

- A o incidente.
- B o problema.
- C a documentação.
- D o processo.
- E a chamada.

**QUESTÃO 61**

Tendo em vista que a segurança da informação tem importância estratégica, contribuindo para garantir a realização dos objetivos da organização e a continuidade dos negócios, assinale a opção correta.

- A Os principais atributos da segurança da informação são a autenticidade, a irretratabilidade e o não repúdio.
- B No contexto atual do governo e das empresas brasileiras, a segurança da informação tem sido tratada de forma eficiente, não permitindo que dados dos cidadãos ou informações estratégicas sejam vazados.
- C A privacidade constitui uma preocupação do comércio eletrônico e da sociedade da informação, não estando inserida como atributo de segurança da informação, uma vez que é prevista no Código Penal brasileiro.
- D A área de segurança da informação deve preocupar-se em proteger todos os ativos de informação de uma organização, governo, indivíduo ou empresa, empregando, em todas as situações, o mesmo nível de proteção.
- E Entre as características básicas da segurança da informação estão a confidencialidade, a disponibilidade e a integridade.

**QUESTÃO 62**

Assinale a opção correta acerca dos mecanismos de segurança disponíveis para a implementação da segurança da informação.

- A A seleção de mecanismos e controles a serem implementados para promover a segurança da informação deve seguir critérios com base na avaliação do que se deseja proteger, dos riscos associados e do nível de segurança que se pretende atingir.
- B Todos os mecanismos de segurança disponíveis devem ser utilizados, tendo em vista que a segurança da informação exige sempre o grau máximo de proteção dos ativos de informação.
- C Controles físicos, barreiras que limitem o contato ou acesso direto a informação ou à infraestrutura para garantir a existência da informação, não são geridos pela área de segurança da informação.
- D Mecanismos de cifração ou encriptação que permitem a transformação reversível da informação, de forma a torná-la ininteligível a terceiros, em geral, são suficientes para apoiar uma boa estratégia de segurança da informação.
- E Os mais importantes mecanismos de segurança da informação incluem, necessariamente, o emprego de *firewalls*, detectores de intrusões, antivírus, filtros *anti-spam* e controle de acesso.

**QUESTÃO 63**

Com relação às ameaças à segurança da informação, assinale a opção correta.

- A A perda da confidencialidade acontece quando a informação deixa de estar acessível por quem necessita dela.
- B A perda da autenticidade e a impossibilidade de não repúdio podem ser consideradas ameaças à segurança da informação.
- C As ameaças à segurança da informação são sempre motivadas pela questão financeira.
- D A perda da integridade ocorre quando há vazamento de uma determinada informação que resulta na exposição de informações restritas que deveriam ser acessadas apenas por um determinado grupo de usuários.
- E A perda da disponibilidade acontece quando uma determinada informação fica exposta a manuseio por uma pessoa não autorizada, possibilitando que esta efetue alterações que não foram aprovadas e não estão sob o controle do proprietário da informação.

**QUESTÃO 64**

Um sistema de gestão de segurança da informação (SGSI) fornece uma abordagem sistemática na gestão de informações confidenciais da organização para mantê-la segura e tem como referências as normas ISO/IEC 27001 e 27002. Acerca desse tema, assinale a opção correta.

- A Todos os controles previstos em norma devem ser implementados para que a organização tenha a certeza de ter atingido o mais elevado nível de proteção.
- B As normas NBR ISO/IEC 27001 e 27002 dizem respeito às práticas de implementação de controles e dos requisitos para a construção de um SGSI, respectivamente.
- C Risco residual é aquele que não necessita de tratamento de riscos.
- D A implementação do SGSI garante à organização a inviolabilidade das suas informações.
- E A ISO/IEC 27001 adota o modelo conhecido como PDCA (*plan-do-check-act*), que é aplicado para estruturar os processos do SGSI.

**QUESTÃO 65**

Criptografia é uma técnica matemática capaz de transformar uma informação da sua forma original para outra forma totalmente ilegível, a partir da qual um processo inverso pode voltar a recuperar a informação para seu formato original. Acerca dessas informações, assinale a opção correta.

- A A técnica criptográfica garante os atributos de autenticidade, integridade, confidencialidade, disponibilidade e não repúdio da informação.
- B Os algoritmos de chaves simétricas e assimétricas são as categorias básicas de algoritmos criptográficos, sendo os de chaves assimétricas a base conceitual da certificação digital.
- C Os algoritmos RSA e as curvas elípticas são exemplos de algoritmos criptográficos com base em chaves simétricas.
- D Os algoritmos DES e AES são exemplos de algoritmos criptográficos com base em chaves assimétricas.
- E Quando criptografada, a informação passa a ter a garantia de nível máximo de proteção.

**QUESTÃO 66**

Como consequência das recentes notícias de vazamento de informação, as entidades públicas federais brasileiras foram informadas de que passarão a fazer uso da infraestrutura de *email* do Serviço de Processamento de Dados (SERPRO). Grandes volumes de informação estratégica trafegam em sistemas de *email*. Tendo essas informações como referência inicial e considerando aspectos relacionados ao tema, assinale a opção correta.

- A Os sistemas de *email* global, como Hotmail e Gmail, dão sempre a garantia de disponibilidade das informações aos seus usuários e também poderiam ser utilizados para trafegar informações estratégicas.
- B Autenticidade, confidencialidade, não repúdio e integridade das informações trocadas podem ser atributos atingidos tecnicamente com os usuários fazendo uso de certificação digital para assinar digitalmente e cifrar as mensagens de *email* trocadas.
- C Para o envio de uma mensagem cifrada a um destinatário de *email*, o usuário local precisa ter conhecimento da chave privada do usuário destinatário.
- D A mensagem assinada digitalmente faz uso da chave pública do usuário originador da mensagem.
- E O atributo de não repúdio de uma mensagem enviada fica garantido pelo fato de o usuário ter conhecimento e fazer uso de sua chave pública para assinar a mensagem.

**QUESTÃO 67**

Com referência à classificação e ao controle de ativos de informação, julgue os itens que se seguem.

- A O estabelecimento de controles que ajustem o nível de segurança para o tratamento da informação classificada deve ser diferenciado em função da natureza da informação quanto a valor, requisitos legais, grau de sensibilidade, grau de criticidade e necessidade de compartilhamento.
- B O uso de biometria como mecanismo de autenticação do usuário no acesso aos sistemas de informação é cada dia mais utilizado e tem a vantagem de rápida implantação com baixo custo.
- C Devido aos constantes ataques aos usuários do sistema bancário, é cada vez mais comum a adoção de mecanismos de autenticação com base em segundo fator de autenticação para o acesso bancário. Nesses casos, o usuário entra com a sua senha duas vezes consecutivas para autenticar o seu acesso.
- D Para a segurança da informação, todas as informações são igualmente importantes. A isonomia na classificação da informação garante que todas as informações devem ser protegidas.
- E Um dos controles de acesso aos sistemas de informação mais utilizados é a identificação pelo uso de *login* do tipo usuário e senha. A vantagem nesse tipo de controle de acesso relaciona-se ao seu baixo custo e à possibilidade de se garantir o não repúdio no acesso.

**QUESTÃO 68**

Tendo em vista que as preocupações da gestão de segurança da informação incluem política de segurança da informação, gestão de ativos, segurança em recursos humanos, segurança física e do ambiente, gestão das operações e comunicações, controle de acessos, aquisição, desenvolvimento e manutenção de sistemas de informação, assinale a opção correta.

- A A análise de mercado para avaliar as ameaças concorrenciais para o negócio é função direta dos gestores de segurança da informação.
- B A fusão e expansão do negócio são rotineiramente analisadas pela área de segurança da informação.
- C Os processos de inovação devem ser geridos pelos gestores de segurança da informação, tendo em vista a grande importância desses temas para a continuidade dos negócios.
- D Os elementos de gestão de incidentes de segurança da informação, gestão da continuidade do negócio e conformidade também são foco de preocupação direta da área gestão de segurança da informação.
- E O controle financeiro da organização deve ser objeto de interferência direta da gestão de segurança da informação.

**QUESTÃO 69**

Com relação à gestão de riscos, assinale a opção correta.

- Ⓐ O escopo da análise dos riscos deve sempre atuar sobre toda a organização.
- Ⓑ A NBR ISO/IEC 15999 estabelece as bases para a gestão de riscos em segurança da informação e a NBR ISO/IEC 27005 trata da gestão de continuidade de negócios.
- Ⓒ Gerenciar os riscos é um dos principais processos da gestão de segurança da informação, pois visa identificar, avaliar e priorizar riscos para, em seguida, se poder aplicar, de forma coordenada e econômica, os recursos para minimizar, monitorar e controlar a probabilidade e o impacto de eventos negativos, de modo a se reduzir o risco a um nível aceitável.
- Ⓓ No sentido de ganhar agilidade na identificação, avaliação e priorização dos riscos, o gestor de segurança da informação pode deixar de consultar a alta direção, sem que isso acarrete prejuízo à gestão de riscos.
- Ⓔ A gestão de segurança da informação pode arbitrar alguns riscos *a priori* e realizar o tratamento do risco sem prejuízo dos resultados.

**QUESTÃO 70**

Assinale a opção correta acerca das vulnerabilidades no modelo de proteção das informações de interesse nacional.

- Ⓐ Mesmo utilizando sistemas tecnológicos de segurança de fornecedores e tecnologias estrangeiras, é possível manter um nível adequado de segurança nacional, com algum nível de vazamento permitido.
- Ⓑ O sistema de regulamentação atual das telecomunicações no Brasil proporciona algumas possibilidades de exploração de vulnerabilidades, mas é suficiente para garantir o controle das comunicações no país.
- Ⓒ A aprovação do marco civil da Internet brasileira deverá elevar o nível de segurança para o cidadão e para o governo brasileiro e deverá impedir que ocorram novos vazamentos de informação.
- Ⓓ A proteção de informações estratégicas de uma nação deve ser feita por tecnologias desenvolvidas no país, sem *backdoor*, auditáveis, com uso de criptografia de estado, por empresas e recursos humanos credenciados, pela normatização e implantação de eficientes sistemas de gestão da informação nas organizações.
- Ⓔ Os atributos de confidencialidade, disponibilidade e integridade de proteção das informações de interesse nacional estão sendo atingidos, sendo os vazamentos algo comum e tolerado dentro de uma certa margem.

**QUESTÃO 71**

Acerca de redes de computadores e protocolos da família TCP/IP, assinale a opção correta.

- Ⓐ O ICMP (*Internet Control Message Protocol*), que atua tanto na camada de redes quanto na de transporte, é utilizado principalmente para detectar e corrigir erros de transmissão dos pacotes.
- Ⓑ O ARP (*Address Resolution Protocol*) permite descobrir o endereço IP a partir de um endereço Ethernet. Esse processo é realizado na camada de enlace para permitir o envio correto do pacote ao destinatário.
- Ⓒ UDP (*User Datagram Protocol*) é um protocolo da camada de transporte que, por não ser confiável, não possui *checksum* em seu cabeçalho.
- Ⓓ HTTP é um protocolo da camada de aplicação executado sobre o TCP e que, quando utiliza o método de conexões paralelas, permite enviar uma solicitação por conexão TCP e executar várias conexões em paralelo.
- Ⓔ PPP (*Point-to-Point Protocol*) é um protocolo da camada de transporte utilizado em redes de topologia em anel ou redes P2P.

**QUESTÃO 72**

Acerca de gerenciamento de redes de computadores e SNMP v3, assinale a opção correta. Nesse sentido, considere que a sigla USM, sempre que empregada, refere-se ao *user-based security model*.

- Ⓐ No USM, a autenticação permite realizar a comprovação da integridade bem como da origem de uma mensagem SNMP. Para isso, o protocolo utilizado é o CBC-DES.
- Ⓑ Com vistas a proteger-se de ataques do tipo *replay* em cada troca de mensagens SNMP, uma das partes é designada como dominante. Assim, quando a mensagem SNMP espera uma resposta, como *GetNext*, por exemplo, então o remetente dessas mensagens é o dominante.
- Ⓒ A troca de mensagens SNMP com privacidade e segurança deve, obrigatoriamente, utilizar chaves *privKey* e *authKey* diferentes, que são empregadas na VACM (*View-based Access Control Model*) para permitir a leitura das mensagens depois de serem criptografadas.
- Ⓓ O USM provê autenticação das mensagens SNMP utilizando chave de autenticação (*authKey*) e privacidade utilizando chave de privacidade (*privKey*). Ambas as chaves têm o tamanho de 16 octetos e não são acessíveis via SNMP.
- Ⓔ No USM, a utilização do protocolo HMAC-MD5-96 tem como objetivo obter privacidade nas mensagens SNMP por meio da cifragem da mensagem.

## QUESTÃO 73

Assinale a opção correta com relação a redes sem fio.

- A MIC (*Message Integrity Check*) é um protocolo na forma de mensagem no 802.x que utiliza o encadeamento de blocos de cifra de 128 bits com o algoritmo AES para criptografar as mensagens.
- B CCMP (*Counter Mode with Cipher Block Chaining Message Authentication code Protocol*) é um protocolo que verifica a autenticidade de uma mensagem a partir de uma chave de sessão, em uma comunicação WPA2.
- C Caso não haja um servidor de autenticação em uma rede doméstica, o protocolo que rege a comunicação utilizando o padrão 802.1x é o WPA2. Nesse caso, o EAP (*Extensible Authentication Protocol*) é o responsável por gerenciar a senha única compartilhada na autenticação da comunicação.
- D No *handshake*, de acordo com o padrão 802.11i, os *nonces* são algoritmos criptográficos baseados em CRC de 128 bits.
- E O WPA2, prescrito no padrão 802.11i, é um protocolo de segurança do nível de enlace de dados e visa impedir que um nó sem fio seja vulnerável a leitura por outro nó sem fio da rede.

## QUESTÃO 74

Ainda com relação a redes sem fio, assinale a opção correta.

- A O PGP (*Pretty Good Privacy*) utiliza a cifra de blocos IDEA (*International Data Encryption Algorithm*) com chave de 64 bits para prover segurança de mensagens de correio eletrônico quanto a privacidade e autenticação.
- B Em uma rede onde o protocolo de estabelecimento da comunicação utilizado é a troca de chaves *Diffie-Hellman*, a comunicação entre os nós é imune ao ataque do tipo brigada de incêndio, visto que, na composição dessas chaves, são utilizados dois números primos grandes.
- C Ao se usar o KDC (*Key Distribution Center*), uma forma de evitar o ataque por *replay* é incluir um registro de tempo ou utilizar *nonce* em cada mensagem.
- D O protocolo de autenticação de *Needham-Schroeder* é vulnerável ao ataque por *replay* porque, na composição das chaves autenticadoras, são utilizados números primos grandes predeterminados.
- E O *kerberos* é um protocolo de autenticação que possui, entre outros, os serviços AS (*Authentication Server*) e TGS (*Ticket-Granting Server*). Desses serviços, o que mais se assemelha ao KDC é o TGS.

## QUESTÃO 75

Acerca de *firewall*, assinale a opção correta.

- A Apesar de serem dependentes de aplicativos e de ignorar os endereços IPs, os *firewalls* de filtragem de pacotes são mais seguros em comparação com os do tipo *proxy*.
- B Além de controlar e conectar o tráfego entre redes, um *firewall* pode criar redes privadas virtuais (VPN), suportar varreduras de vírus no correio eletrônico e filtrar aplicativos para bloquear acesso não autorizado aos aplicativos remotos.
- C Em comparação com um *firewall* de filtragem de pacotes, os aplicativos de *firewall* e de *proxy* são mais rápidos, mais baratos e suportam o protocolo UDP.
- D Os *firewalls* do tipo filtragem de pacotes são voltados para tratamento de códigos maliciosos, como, por exemplo, cavalos de troia.
- E Os *firewalls* do tipo inspeção de pacotes com informação de estado funcionam nas camadas de 3 a 7 para proteção e tratamento de vírus de rede.

## QUESTÃO 76

Assinale a opção correta acerca de NAT (*network address translation*).

- A Apesar de não fornecer recursos de conexão de tráfego, como rastreamento de usuário, sítios ou conexões, a NAT permite que administradores de redes proibam acesso a determinados sítios.
- B O mecanismo de NAT é utilizado exclusivamente por roteadores que operam na camada 3 ou acima.
- C Na NAT do tipo dinâmica sobrecarregada vários endereços IP não registrados são mapeados para um único endereço IP registrado, utilizando diferentes portas.
- D Na NAT do tipo dinâmica sobreposta um endereço IP não registrado é mapeado para um endereço IP, registrado com uma base unívoca.
- E Em uma mesma rede, não é possível usar a NAT e o DHCP, pois eles são mutuamente exclusivos.

**QUESTÃO 77**

Assinale a opção correta acerca de criptografia.

- A Na criptografia assimétrica, a confidencialidade da mensagem é garantida de forma absoluta, uma vez que, nessa modalidade de criptografia, são utilizados pares de algoritmos na comunicação de dados.
- B Os métodos criptográficos RSA, DAS e *Diffie-Hellman* implementam criptografia de chave secreta ou única, que visa, principalmente, garantir a confidencialidade. Nesse tipo de criptografia, utiliza-se uma mesma chave tanto para codificar como para decodificar os dados.
- C O HMAC (*Hash Message Authentication Code*) pode ser considerado um suplemento do MD5, visto que se trata de um código de autenticação de mensagem criado com base em um valor-chave que é incluído no *hash*, de maneira que os dados originais e o MAC sofram *hash* na mesma resenha.
- D SHA-1 é um algoritmo voltado para criptografia de 128 bits.
- E A criptografia simétrica garante a autenticidade da mensagem, uma vez que exclusivamente o emissor, detentor de chave privada, pode criptografar uma informação que será decriptografada pela chave pública.

**QUESTÃO 78**

Acerca de VPN (*Virtual Private Network*), assinale a opção correta.

- A Uma VPN provê uma utilização do canal de comunicação mais racional, por não manter *links* permanentes entre os pontos de comunicação, mas não possui a função de autenticar pacotes de dados em relação à sua origem.
- B Funções de *hash*, MACs (*Message Authentication Codes*) e assinaturas digitais visam assegurar a integridade das mensagens em uma VPN.
- C Embora uma VPN possua maior custo do que as linhas dedicadas, ela fornece confidencialidade por meio de criptografia com chave pública ou privada.
- D RADIUS (*Remote Authentication Dial-In User Service*) e CHAP (*Challenge-Handshake Authentication Protocol*) garantem às VPNs não repúdio e disponibilidade, respectivamente.
- E Os protocolos de tunelamento são limitados às linhas dedicadas e aos circuitos virtuais permanentes e, portanto, não podem ser utilizados em VPNs.

**QUESTÃO 79**

Acerca de AD (*Active Directory*) e LDAP (*Lightweight Directory Access Protocol*), assinale a opção correta.

- A LDAP, AD e X.500 são projetados para fornecer informações de maneira compartilhada sobre a pilha de protocolos TCP/IP, permitindo que seus dados sejam replicados em florestas e possibilitando permissões de acesso aos objetos, como leitura, gravação e pesquisa somente com leitura.
- B No LDAP v3, os domínios de uma árvore possuem esquemas relacionais de dados na forma de DIT (*Directory Information Tree*). A *Global Catalog* se assemelha ao conceito de floresta no AD, ou seja, grupos de árvores que compartilham segurança, convenções e grau de confiança entre domínios, em que cada árvore possui um esquema individual.
- C O AD é compatível com o LDAP v1 e LDAP v2, mas não com o LDAP v3.
- D Uma das partes ativas do AD é a base de dados do diretório Windows 2000/2003. A base de dados do diretório contém contas de usuários e segurança da informação do domínio, em que o domínio do Windows 2000 e 2003 é uma estrutura lógica que compartilha uma central de serviços e diretórios.
- E No LDAP v2, as árvores são estruturas de hierarquia de um ou mais grupos, em que o *namespace* define os domínios e subdomínios (*child domains*). Os domínios compartilham as funções, havendo uma função para cada árvore, e cada árvore é formada por dados de objetos e recursos.

**QUESTÃO 80**

Assinale a opção correta no que se refere à virtualização.

- A Em um ambiente computacional virtual, o mestre é o sistema operacional (SO) executado diretamente sobre o *hardware*, enquanto o escravo é o SO executado sempre no SO virtualizado, não havendo limites na quantidade de escravos por mestre.
- B O *hypervisor* constitui-se dos dados a serem processados e das instruções. Em uma estrutura de virtualização monolítica, há somente um *hypervisor* por máquina física.
- C A virtualização está associada diretamente ao ambiente de OLTP, uma vez que consultas analíticas e *datawarehouse* não podem ser utilizados para prover transações em *batch*.
- D O *throughput* em virtualização está associado ao núcleo do SO, ao espaço em disco, aos controladores de *cache* e ao microcódigo. *Throughput* é composto de velocidade de I/O, de CPU, capacidade de paralelismo e eficiência do SO.
- E Em um ambiente virtualizado, cada máquina virtual possui *hard disk*, NIC (*network interface card*) e SO virtuais dependentes do SO físico. Assim, todas as máquinas compartilham o mesmo sistema de arquivos.