

De acordo com o comando a que cada um dos itens a seguir se refira, marque, na **folha de respostas**, para cada item: o campo designado com o código **C**, caso julgue o item **CERTO**; ou o campo designado com o código **E**, caso julgue o item **ERRADO**. A ausência de marcação ou a marcação de ambos os campos não serão apenadas, ou seja, não receberão pontuação negativa. Para as devidas marcações, use a **folha de respostas**, único documento válido para a correção das suas respostas.

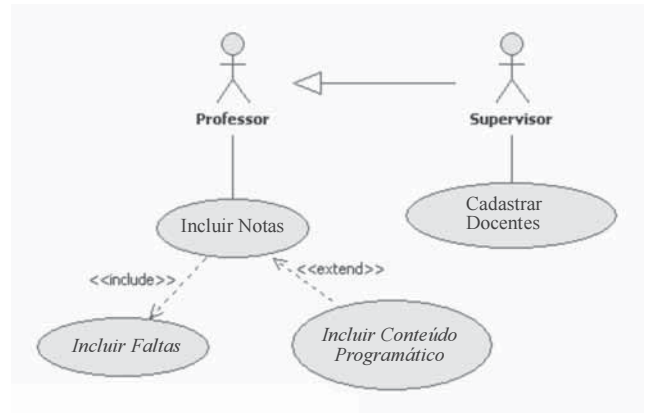
## PROVA OBJETIVA P<sub>2</sub> — CONHECIMENTOS ESPECÍFICOS

*Rational unified process* (RUP) é um processo de negócios genérico para engenharia de *software* orientada a objetos. Ele descreve uma família de processos de engenharia de *software* relacionados que compartilham uma estrutura comum, uma arquitetura de processos comum. Ele proporciona abordagem disciplinada para a atribuição de tarefas e de responsabilidades dentro de uma organização de desenvolvimento. O processo de engenharia de *software* é o processo de desenvolvimento de sistema a partir dos requisitos, sejam eles novos (ciclo de desenvolvimento inicial), ou alterados (ciclo de evolução).

Internet: <www.wthreex.com> (com adaptações).

Tendo o texto acima como referência inicial, julgue os itens a seguir.

- 101** A criação de *baselines* no RUP tem como motivação a rastreabilidade, a elaboração de relatórios e a reprodutibilidade, além de estabelecer, na fase de construção, um marco da arquitetura do ciclo de vida do projeto. Com os *baselines*, é possível desfazer mudanças caso as atualizações realizadas sejam consideradas instáveis ou não confiáveis.
- 102** No RUP, a análise estrutural, parte da análise de requisitos, constitui atividade que inclui decisões acerca de implementação da visão, arquitetura física e lógica e requisitos não funcionais do sistema. Além disso, a análise estrutural tem como finalidade definir as estratégias de reutilização e os padrões de arquitetura do sistema.



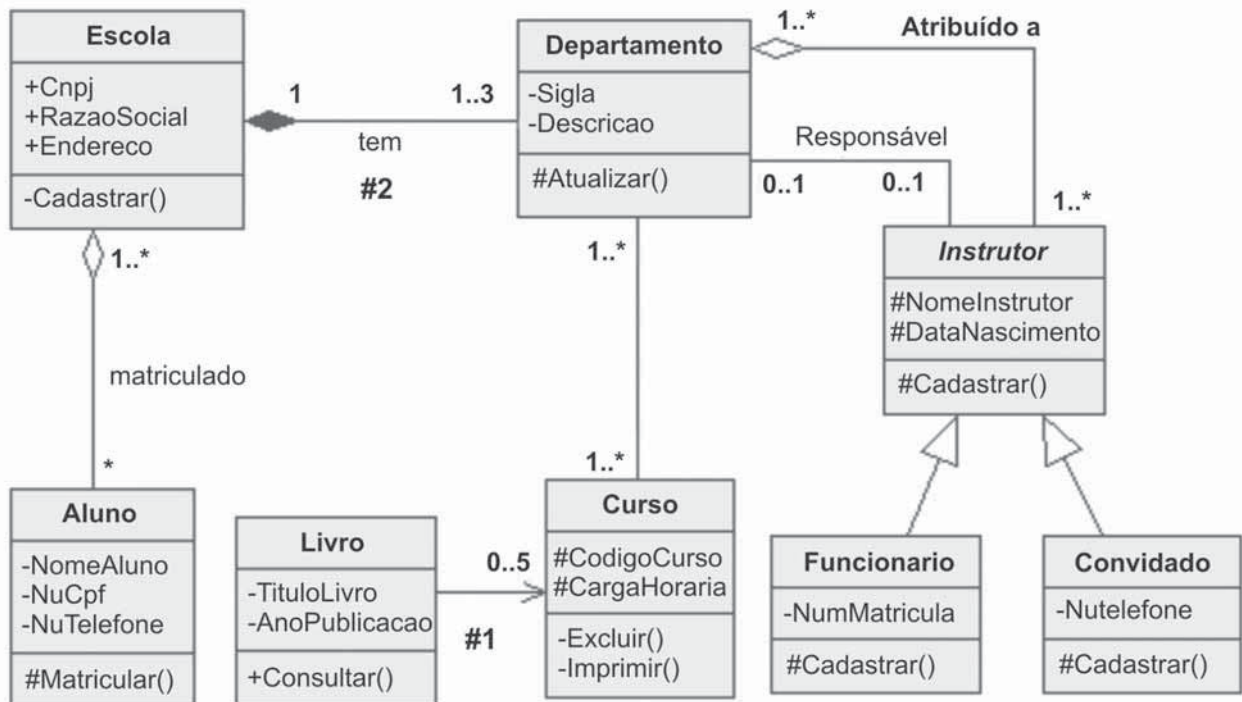
Considerando o diagrama UML acima, julgue os seguintes itens.

- 103** De acordo com o diagrama, estão corretas as seguintes afirmações: o ator Supervisor é uma especialização do ator Professor; o caso de uso *Incluir Faltas* é abstrato e pode ser acionado pelo ator Supervisor; o caso de uso *Incluir Conteúdo Programático* é abstrato e representa um segmento opcional de comportamento.
- 104** VORD (*viewpoint-oriented requirements definition*) é um *framework* para levantamento de requisitos, que consiste em realizar *brainstorm* no qual os *stakeholders* sugerem pontos de vista usando como técnica de cenários os diagramas de bolha e, para técnica de ponto de vista, os diagramas *use-case*.
- 105** Os requisitos podem ser classificados como de domínio, funcionais, não funcionais, permanentes ou consequentes. Os requisitos de domínio podem ser uma declaração explícita do que o sistema não deve fazer ou, ainda, uma característica que o mesmo tenha de ter, como, por exemplo, a de, no máximo, 100 MB de tamanho; os funcionais detalham recursos que devem ser realizados pelo sistema; os permanentes originam-se da atividade principal da orientação; os consequentes são requisitos voláteis e podem ser modificados ao longo do desenvolvimento do sistema.



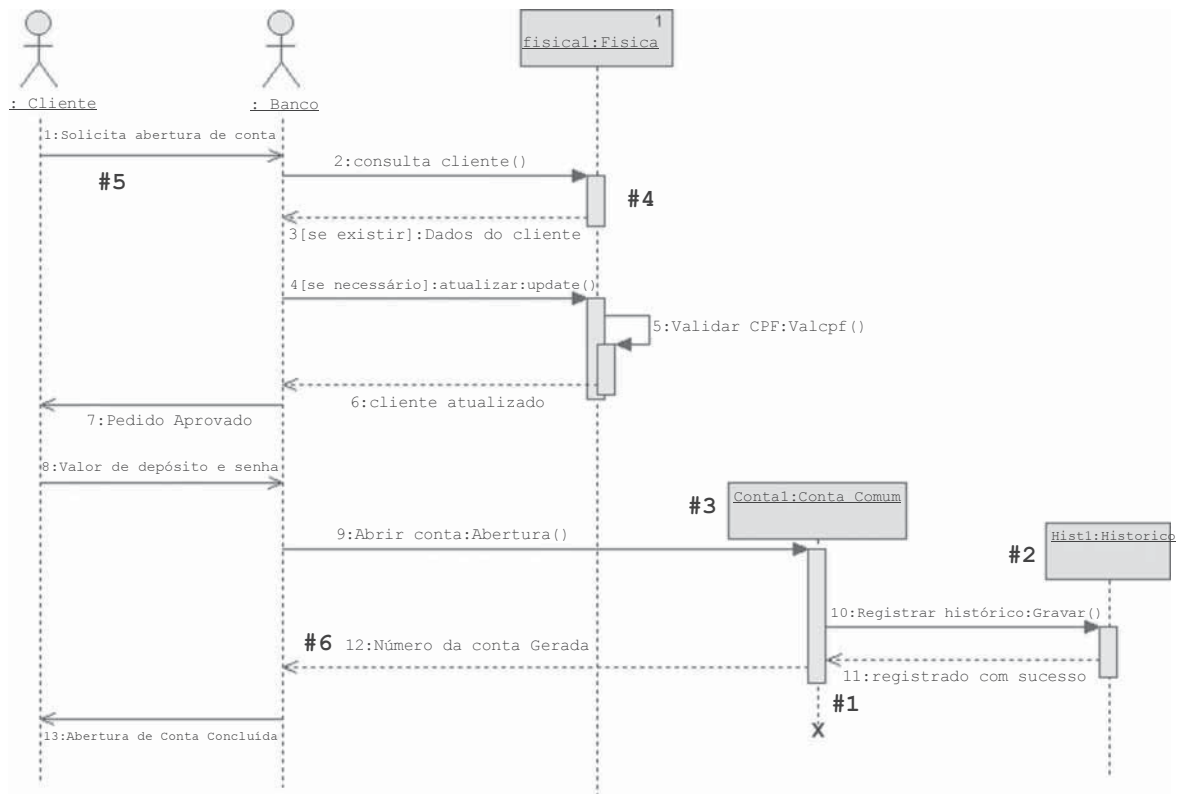
A partir da figura acima, que representa os fatores de qualidade de *software*, julgue os itens que se seguem.

- 106** A usabilidade é uma medida de qualidade de *software* a ser observada também no levantamento de requisitos, que pode ser auferida analisando-se subjetivamente as atitudes dos usuários em relação ao sistema, por exemplo, por meio de um questionário de avaliação. De acordo com a figura, a usabilidade estaria corretamente classificada se posicionada em #1.
- 107** A funcionalidade é um requisito funcional, uma característica a ser observada em um modelo de qualidade de *software*. Ela agrega subcaracterísticas como interoperabilidade, adequabilidade e acurácia. Segundo a figura, a funcionalidade estaria corretamente classificada se posicionada em #3.



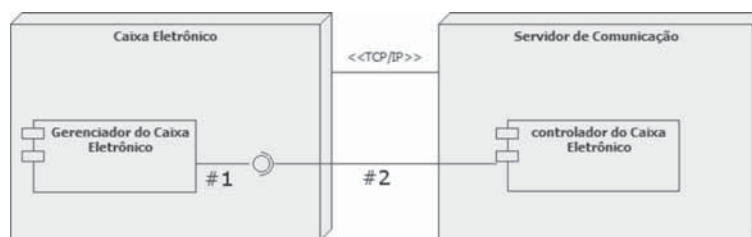
Tendo o diagrama UML da figura acima como referência, julgue os seguintes itens.

- 108** O método `#Cadastrar()` da classe *Instrutor* tem visibilidade do modo protegido tal que somente a classe possuidora *Instrutor* pode utilizá-lo.
- 109** Na associação do tipo agregação composta identificado por #2, uma instância da classe *Departamento* pertence exclusivamente a uma única instância composta em *Escola*, e um objeto da classe *Escola* pode relacionar-se com, no máximo, três objetos da classe *Departamento*.
- 110** *Instrutor* é uma superclasse abstrata; assim, o método `#Cadastrar()` oferece uma assinatura, que, no entanto, está incompleta, devendo ser implementada pelos métodos de mesmo nome nas suas classes-filhas.



Com base no diagrama UML apresentado acima, julgue os itens subsequentes.

- 111 No diagrama apresentado, #4 é um foco de controle que mostra o período durante o qual um objeto está desempenhando uma ação; #2 mostra um objeto *fisical* da classe *Fisica*; #1 representa a existência de um objeto, uma *linha de vida*, que pode ser interrompida com um x quando o objeto é destruído; #3 é um objeto que não existia no início do processo e foi criado no decorrer deste.
- 112 No referido diagrama, o número 1 no canto superior direito dentro do objeto *fisical:Fisica* indica que esse objeto é unitário tal que, em padrões de projeto, pode ser classificado como do tipo *singleton*; #6 é uma mensagem de retorno sem disparo de método; e #5 é uma mensagem simples entre atores que indica somente a ocorrência de um evento.



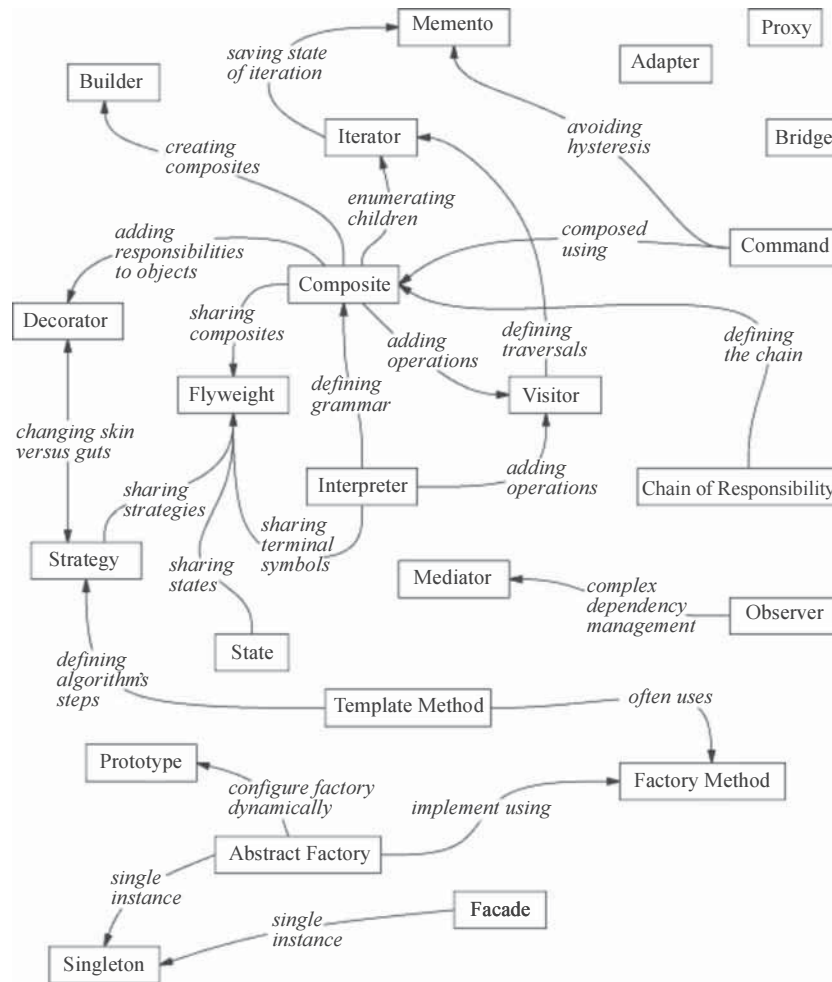
Tendo o diagrama UML acima como referência, julgue os seguintes itens.

- 113 Nesse diagrama, #1 é uma interface do tipo fornecida que descreve um serviço implementado; e #2 é uma interface do tipo requerida. Tais interfaces podem ser substituídas, sem prejuízo, pelos relacionamentos de dependência e realização, respectivamente.
- 114 Na figura, um diagrama UML de implantação é modelado juntamente com um diagrama de componentes, ambos voltados para a modelagem de aspectos físicos e estáticos de sistemas orientados a objetos.
- 115 Na UML 2.0, o diagrama de interação geral é utilizado para modelar colaborações, conjunto de instâncias que cooperam entre si para uma função específica; o diagrama de máquina de estados representa estados de um caso de uso de um subsistema ou de um sistema completo; e o diagrama de tempo demonstra a mudança de estado de um objeto, ao longo do tempo decorrente de eventos externos.

Julgue os itens subsequentes, relativos às as métricas de *software*, medições que se referem a um sistema, processo ou documentação, e que, aliadas aos padrões, auxiliam na qualidade do *software*.

**116** A medida de complexidade ciclomática avalia o número de caminhos de execução diferentes de um dado programa, sendo diretamente relacionada à facilidade de compreensão do programa. Calculada a partir da análise de um grafo dirigido, representa os possíveis caminhos de execução do programa, e desvios incondicionais contribuem para o aumento de valor desse cálculo.

**117** A métrica de acoplamento e coesão analisa o grau de dependência entre componentes de um programa. Em um projeto de *software*, buscam-se um baixo grau de acoplamento e um alto grau de coesão. A medida *fan-in*, que mede o grau de acoplamento, indica quantos módulos controlam diretamente determinado módulo; desse modo, um valor baixo de *fan-in* indica que uma função Y está estreitamente acoplada ao restante do projeto.



Os padrões de projeto podem ser vistos como heurísticas que guiam os desenvolvedores de *software* na organização do espaço de objetos de uma aplicação. Os padrões de projeto GoF (GoF *patterns*) são classificados em três tipos: de criação, de estrutura e de comportamento. Considerando esses padrões de projeto e a figura acima, julgue os itens de **118 a 120**.

**118** Se, no desenvolvimento de uma aplicação que leia documentos do tipo txt e seja capaz de converter o documento em vários formatos distintos, houver a necessidade de facilitar acréscimos de novos tipos de conversão, será mais indicado o uso do padrão de estrutura Adapter que o uso do padrão de estrutura Bridge, pois o padrão Adapter separa a construção de um objeto complexo de sua representação para criar representações diferentes com o mesmo processo.

**119** No desenvolvimento de um sistema estruturado em subsistemas para facilitar o acesso e minimizar a comunicação e dependências entre os subsistemas, o padrão de criação Factory Method, que fornece uma interface para a criação de famílias de objetos relacionados ou dependentes sem especificar suas classes concretas, é mais indicado que o padrão de criação Prototype.

**120** Caso seja verificado no desenvolvimento de um sistema forte acoplamento entre as classes, recomenda-se o uso do padrão de comportamento Factory Method, que evita o acoplamento do remetente de uma solicitação ao seu receptor, dando a mais de um objeto a oportunidade de tratar uma solicitação, mesmo nos casos em que o conjunto de objetos não seja conhecido *a priori* ou seja definido dinamicamente.

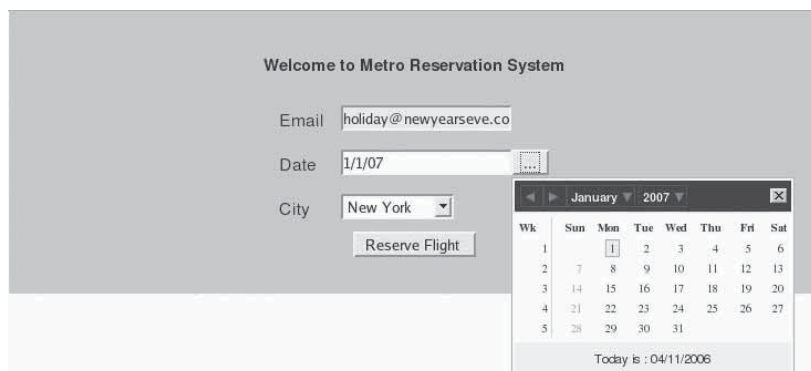
```

<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
<%@ taglib uri="http://myfaces.apache.org/tomahawk" prefix="t"%>
<html>
<head>
<title>Metro Systems </title>
<link href="css/style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="container">
<f:loadBundle basename="com.webforefront.resource.booking_messages"
var="booking_messages"/>
<f:view>
<h3> < h:outputText value="#{booking_messages['welcome']}" /> </h3>
< h:form>
<table align="center" cellpadding="5" cellspacing="5">
<tr>
<td>Email</td>
<td>< h:inputText id="email" value="#{flight.email}" />
</td>
</tr>
<tr>
<td>< h:outputText id="departure"
value="#{booking_messages['date']}" /></td>
<td>
<t:inputCalendar monthYearRowClass="yearMonthHeader" weekRowClass="weekHeader"
currentDayCellClass="currentDayCell"
value="#{flight.departure}" renderAsPopup="true"
popupTodayString="#{booking_messages['popup_today_string']}"
popupWeekString="#{booking_messages['popup_week_string']}" />
</td>
</tr>
<tr>
<td>< h:outputText value="#{booking_messages['city']}" /> </td>
<td> < h:selectOneMenu value="#{flight.city}" required="true">
<f:selectItem itemLabel="Los Angeles"
itemValue="Los Angeles"/>
<f:selectItem itemLabel="Madrid"
itemValue="Madrid"/>
<f:selectItem itemLabel="Mexico City"
itemValue="Mexico City"/>
<f:selectItem itemLabel="New York"
itemValue="New York"/>
<f:selectItem itemLabel="Paris"
itemValue="Paris"/>
</h:selectOneMenu></td>
</tr>
</table>
< h:commandButton type="submit" value="#{booking_messages['reserve']}"
action="#{flight.reserve}" />
< h:messages />
</h:form>
</f:view>
</div>
</body>
</html>

```

Com base no código acima apresentado, julgue os itens a seguir.

121 O código em questão corresponde à implementação mostrada na figura abaixo.



122 A declaração `<f: loadBundle>` fornece capacidades internacionais (i18n) à aplicação. Nessa declaração, no código apresentado, `Var` é o nome de referência para atualizar os valores dos recursos.

123 Na instrução `value="#{flight.*}"`, o nome do *backing bean* é `flight` e o segundo valor representa o nome do campo definido no *bean*.

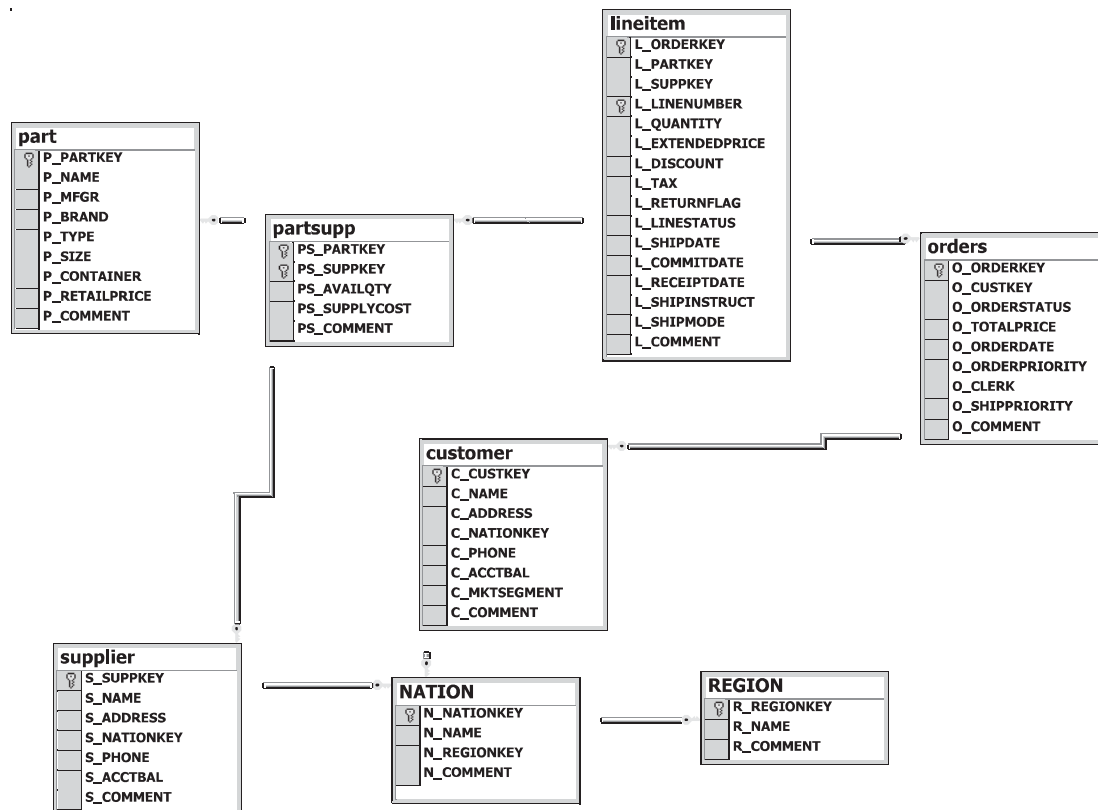


Figura I

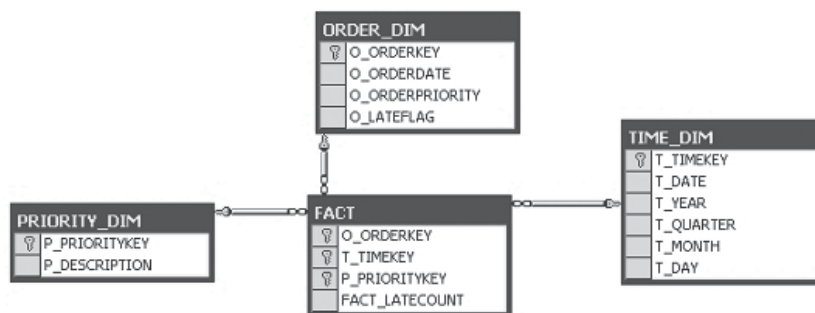


Figura II

Considerando as figuras I e II acima apresentadas, julgue os itens a seguir, a respeito de bancos de dados e bancos de dados multidimensionais.

124 O comando a seguir permite selecionar, com base na estrutura mostrada na figura I, quantas ordens foram entregues no terceiro trimestre de 1993, ordenadas por prioridade.

```
SELECT o_orderpriority, COUNT(*) AS order_count FROM orders WHERE o_orderdate >= '1993-07-01' AND o_orderdate < '1993-10-01' AND EXISTS (SELECT * FROM lineitem WHERE l_orderkey = o_orderkey AND l_commitdate < l_receiptdate) GROUP BY o_orderpriority ORDER BY o_orderpriority
```

125 Os esquemas mostrados são equivalentes, mas o da figura I corresponde a um banco de dados relacional e o da figura II corresponde a um banco de dados multidimensional.

A respeito de sistemas transacionais, julgue os itens a seguir.

126 Um escalonamento é considerado correto quando se pode encontrar um escalonamento serial que seja equivalente a ele. Dado um conjunto de transações T1, ... ,Tn, dois escalonamentos S1 e S2 são equivalentes se existe sincronização *read-write* e sincronização *write-write*.

127 No *two-phase locking*, os *locks* de dados supõem que a transação está dividida em uma fase de crescimento, na qual os *locks* são feitos, e em uma fase de encolhimento, na qual os *locks* são confirmados.

128 As transações aninhadas devem ter a propriedade de ser serializáveis em relação aos seus pares, ou seja, o acesso a recursos compartilhados entre essas transações deve obedecer as regras de sincronização de *read-write* e *write-write*.

T1	T2
lock(p1)	
read(p1)	
	lock(p1)
write(p1)	
lock(p2)	
unlock(p1)	
	read(p1)
	write(p1)
	lock(p2)
	unlock(p1)
read(p2)	
write(p2)	
unlock(p2)	
	read(p2)
	write(p2)
	unlock(p2)

Considerando as transações T1 e T2 apresentadas acima, julgue os itens subsequentes.

- 129 Na situação em questão, a transação T2 pode ver os *writes* incrementais de T1. Esse enfoque diminui a concorrência do sistema.
- 130 Se, por alguma razão, a transação T1 for abortada, o requerimento de atomicidade implicará que também sejam abortadas as transações como T2, aquelas que igualmente tenham visto os resultados de T1, transações que tenham visto os *writes* dessas transações e assim por diante. Esse problema é conhecido como *rollback* em cascata.

Com relação a conceitos de arquitetura e padrões de projeto JEE, julgue os próximos itens.

- 131 Para uma arquitetura de aplicações JEE, os padrões de projeto podem ser classificados em duas categorias: padrões de desenvolvimento geral de *software* e padrões que identificam desafios específicos J2EE.
- 132 No MVC (*model-view-controller*), um padrão recomendado para aplicações interativas, uma aplicação é organizada em três módulos separados. Um para o modelo de aplicação com a representação de dados e lógica do negócio, o segundo com visões que fornecem apresentação dos dados e *input* do usuário e o terceiro para um controlador que despacha pedidos e controle de fluxo.

Com relação a sistemas de suporte a decisão (SSD), julgue os itens seguintes.

- 133 Um SSD do tipo *model-driven* dá ênfase ao acesso e à manipulação de modelos financeiros, de otimização ou simulação. Esse tipo de SSD utiliza dados limitados e parâmetros fornecidos pelos operadores para auxiliar os desenvolvedores de sistemas na tomada de decisões.
- 134 Os SSD do tipo *Internet-driven* utilizam redes e tecnologias de comunicação para facilitar a colaboração e comunicação na tomada de decisões. Entre as ferramentas utilizadas nesses SSDs, estão *groupwares*, videoconferência e *boards* eletrônicos.

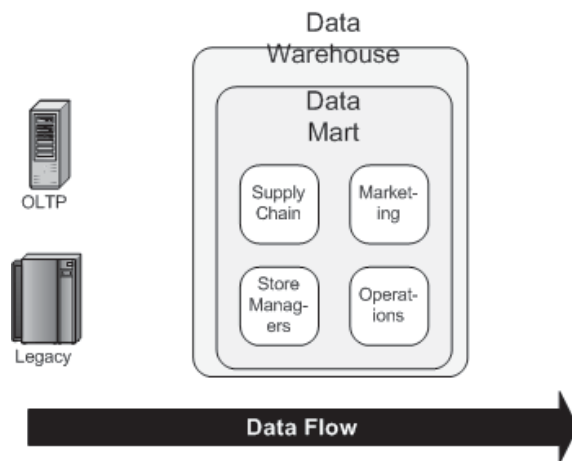


Figura I

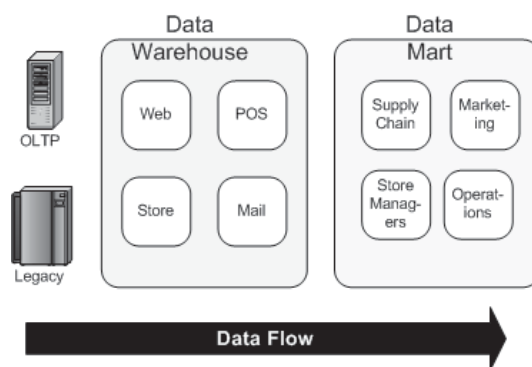


Figura II

Com base nas figuras I e II acima, e nos conceitos de *datawarehousing*, julgue os itens subsequentes.

- 135 Na figura II, que corresponde à visão de Kimball, o *datawarehousing* é visto como uma constituição de *data marts*, cujo foco é entregar objetivos do negócio para departamentos na organização.
- 136 Na figura I, o *datawarehouse* é criado com base em um enfoque *subject-by-subject*. Dessa forma, o desenvolvimento de um *datawarehouse* poderia começar com dados de uma loja *online*, por exemplo, e outros *subjects* seriam adicionados ao *datawarehouse* conforme as necessidades. Nesse enfoque, o *data mart* é a criação de uma *subject area* do *datawarehouse*.

A respeito de arquitetura de informação, julgue os itens a seguir.

- 137 Um modelo de dados de alto nível é parte de uma *information systems architecture* (ISA). Entre os componentes de uma ISA, estão os dados e os processos que manipulam os dados, estes últimos representados por DFDs e modelos de objetos.
- 138 As matrizes de planejamento proveem um enfoque explícito para descrever requerimentos do negócio e, para sua especificação, precisam que o banco de dados esteja explicitamente modelado.

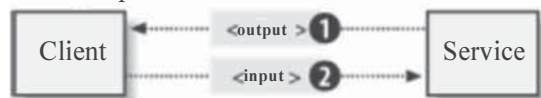
one-way



request-response



solicit-response



notification



Considerando a figura acima, julgue os itens subsequentes.

**139** Em WSDL, os elementos do tipo *types* descrevem todos os tipos de dados usados entre cliente e servidor. O WSDL está exclusivamente ligado a um sistema de tipagem específico pois utiliza, como padrão, um esquema de especificação W3C XML.

**140** Na figura mostrada, na *notification*, o serviço envia uma mensagem e a operação tem um único elemento de saída. O padrão *request-response* é pouco utilizado nos serviços SOAP.

Com relação às tecnologias de redes locais, julgue os itens a seguir.

**141** A interconexão de redes CSMA/CD, como Ethernet e IEEE 802.3, utilizando *bridges* ou *switches*, agrega os domínios de *broadcast* das redes, porém preserva seus domínios de colisão.

**142** A utilização de *switches* na interconexão de *hosts* de uma rede local embasada em CSMA/CD proporciona melhor uso da banda passante correspondente a cada *host*, além de agregar segurança, uma vez que evita a interceptação de tráfego.

**143** De maneira geral, *switches* de camada 3 são funcional e operacionalmente equivalentes a roteadores.

1. 0.285156 IP (tos 0x0, ttl 128, id 8313, offset 2944, flags [ ], proto: ICMP (1), length: 84) 10.1.1.100 > 10.1.1.200: icmp
2. 0.285156 IP (tos 0x0, ttl 128, id 8313, offset 1472, flags [+], proto: ICMP (1), length: 1492) 10.1.1.100 > 10.1.1.200: icmp
3. 0.285156 IP (tos 0x0, ttl 128, id 8313, offset 0, flags [+], proto: ICMP (1), length: 1492) 10.1.1.100 > 10.1.1.200: ICMP echo request, id 768, seq 2560, length 1472
4. 0.525390 IP (tos 0x0, ttl 250, id 9564, offset 2960, flags [ ], proto: ICMP (1), length: 68) 10.1.1.200 > 10.1.1.100: icmp
5. 0.546875 IP (tos 0x0, ttl 250, id 9564, offset 0, flags [+], proto: ICMP (1), length: 764) 10.1.1.200 > 10.1.1.100: ICMP echo reply, id 768, seq 2560, length 744
6. 0.570312 IP (tos 0x0, ttl 250, id 9564, offset 744, flags [+], proto: ICMP (1), length: 756) 10.1.1.200 > 10.1.1.100: icmp
7. 0.591796 IP (tos 0x0, ttl 250, id 9564, offset 1480, flags [+], proto: ICMP (1), length: 764) 10.1.1.200 > 10.1.1.100: icmp
8. 0.615234 IP (tos 0x0, ttl 250, id 9564, offset 2224, flags [+], proto: ICMP (1), length: 756) 10.1.1.200 > 10.1.1.100: icmp

Considerando o trecho de captura de tráfego acima apresentado, julgue os itens que seguem.

**144** Se utilizarem a mesma máscara de rede, qualquer que seja, então os *hosts* envolvidos na captura de tráfego estarão na mesma sub-rede.

**145** A chegada fora de ordem dos pacotes de resposta deve-se à retransmissão de alguns deles ao longo do percurso.

**146** É consistente com a captura que há quatro nós intermediários entre os *hosts* nela presentes.

**147** É consistente com a captura que o processo de fragmentação tenha sido aplicado mais de uma vez nos pacotes de resposta.



1. 771929 IP (tos 0x10, ttl 64, id 46018, offset 0, flags [DF], proto: TCP (6), length: 60) 192.168.1.1.5463 > 192.168.8.8.3421: S, cksum 0x1db2 (correct), 0:0(0) win 5840 <mss 1460,sackOK,timestamp 2538826 0,nop,wscale 6>
2. 1.994556 IP (tos 0x0, ttl 50, id 20037, offset 0, flags [DF], proto: TCP (6), length: 44) 192.168.8.8.3421 > 192.168.1.1.5463: S, cksum 0x9e62 (correct), 0:0(0) ack 1160318601 win 5840 <mss 1460>
3. 1.994605 IP (tos 0x10, ttl 64, id 46019, offset 0, flags [DF], proto: TCP (6), length: 40) 192.168.1.1.5463 > 192.168.8.8.3421: ., cksum 0xb61f (correct), 1:1(0) ack 1 win 5840
4. 4.909380 IP (tos 0x10, ttl 64, id 46020, offset 0, flags [DF], proto: TCP (6), length: 47) 192.168.1.1.5463 > 192.168.8.8.3421: P, cksum 0xa89d (correct), 1:8(7) ack 1 win 5840
5. 5.220509 IP (tos 0x0, ttl 50, id 20038, offset 0, flags [DF], proto: TCP (6), length: 40) 192.168.8.8.3421 > 192.168.1.1.5463: ., cksum 0xb618 (correct), 1:1(0) ack 8 win 5840
6. 5.220591 IP (tos 0x0, ttl 50, id 20041, offset 0, flags [DF], proto: TCP (6), length: 40) 192.168.8.8.3421 > 192.168.1.1.5463: F, cksum 0xae04 (correct), 2068:2068(0) ack 8 win 5840
7. 5.220607 IP (tos 0x10, ttl 64, id 46021, offset 0, flags [DF], proto: TCP (6), length: 40) 192.168.1.1.5463 > 192.168.8.8.3421: ., cksum 0xb618 (correct), 8:8(0) ack 1 win 5840
8. 5.223374 IP (tos 0x0, ttl 50, id 20040, offset 0, flags [DF], proto: TCP (6), length: 647) 192.168.8.8.3421 > 192.168.1.1.5463: P, cksum 0xe4c5 (correct), 1461:2068(607) ack 8 win 5840
9. 5.223381 IP (tos 0x10, ttl 64, id 46022, offset 0, flags [DF], proto: TCP (6), length: 40) 192.168.1.1.5463 > 192.168.8.8.3421: ., cksum 0xb618 (correct), 8:8(0) ack 1 win 5840
10. 5.229617 IP (tos 0x0, ttl 50, id 20039, offset 0, flags [DF], proto: TCP (6), length: 1500) 192.168.8.8.3421 > 192.168.1.1.5463: ., cksum 0xbf1b (correct), 1:1461(1460) ack 8 win 5840
11. 5.229632 IP (tos 0x10, ttl 64, id 46023, offset 0, flags [DF], proto: TCP (6), length: 40) 192.168.1.1.5463 > 192.168.8.8.3421: ., cksum 0xa29c (correct), 8:8(0) ack 2069 win 8760
12. 5.231280 IP (tos 0x10, ttl 64, id 46024, offset 0, flags [DF], proto: TCP (6), length: 40) 192.168.1.1.5463 > 192.168.8.8.3421: F, cksum 0xa29b (correct), 8:8(0) ack 2069 win 8760
13. 5.452312 IP (tos 0x0, ttl 50, id 20042, offset 0, flags [DF], proto: TCP (6), length: 40) 192.168.8.8.3421 > 192.168.1.1.5463: ., cksum 0xae03 (correct), 2069:2069(0) ack 9 win 5840

Com base no trecho de captura de tráfego acima, julgue os itens de **148 a 150**.

- 148** A captura em apreço apresenta uma conexão TCP completa, com todos os segmentos envolvidos no estabelecimento e encerramento da conexão.
- 149** Há elementos característicos de tráfego interativo, em que a janela deslizante não é completamente preenchida. Entretanto, há segmentos com o tamanho máximo possível.
- 150** Na captura em questão, a recepção de segmentos fora de ordem deve-se à ocorrência de retransmissão por perda de pacotes.

Com relação às tecnologias de redes de longa distância, julgue os itens seguintes.

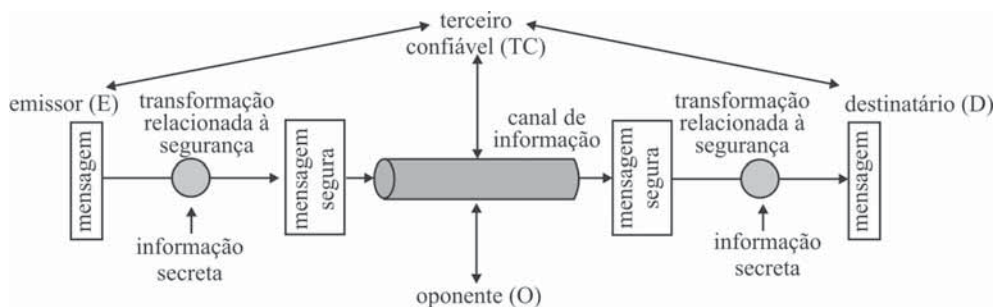
- 151** Entre outros benefícios, o uso do MPLS viabiliza a engenharia de tráfego e facilita a formação de VPNs IP, além de suportar múltiplos protocolos, tecnologias e tipos de tráfego.
- 152** A etiqueta MPLS tem comprimento de 3 *bytes*, tendo, entre outros, um campo Label (20 *bits*) e um campo TTL (8 *bits*), este último com função diferente do campo homônimo do cabeçalho IP.
- 153** O MPLS não dispõe de mecanismo de pilha da etiqueta que permita realizar uma operação hierárquica no domínio MPLS.
- 154** A etiqueta MPLS pode ser inserida tanto como informação de enlace como entre os cabeçalhos de camadas 2 e 3.

A respeito das tecnologias de redes sem fio, julgue os próximos itens.

- 155** O WPA originalmente implementou integralmente a especificação IEE 802.11i, particularmente TKIP.
- 156** O WEP, especificado no padrão IEE 802.11b e embasado na cifra de fluxo RC4, não determina como devem ser gerados os vetores iniciais, o que propicia que as implementações os reúsem, causando, assim, vulnerabilidades de segurança.
- 157** O padrão IEEE 802.1x, incorporado pelo WPA2, envolve três componentes: o suplicante, que deseja se autenticar; o autenticador, que recebe o pedido do suplicante e o repassa ao serviço de autenticação; e o servidor de autenticação, que suporta o serviço de autenticação.

Com relação aos sistemas operacionais Linux e Windows, julgue os itens a seguir.

- 158** O NTFS, como o UFS, é um sistema de arquivos hierarquizado com arquivos e diretórios, em que cada arquivo tem um proprietário, mas não pertence a um grupo. O acesso não é regulado por um conjunto de *bits* de permissão, mas por listas de acesso, implementando um modelo discricionário.
- 159** Os domínios do Windows Server 2003 operam em quatro modos: misto, nativo, .NET e .NET ínterim; os domínios em modo .NET permitem que BDCs Windows NT 4.0 participem em domínios do Windows Server 2003.
- 160** O Windows implementa o *fork* identicamente ao Unix, replicando processos já existentes.



Stallings. Criptografia e segurança de redes, Pearson, 2006.

A figura acima apresenta um modelo para segurança de rede, no qual se destacam vários elementos, individualmente nomeados. Esse modelo apresenta um conjunto de elementos que compõem soluções para o provimento de um canal de informação seguro entre o emissor (E) e o (D) destinatário, envolvendo um terceiro confiável (TC). Julgue os itens de 161 a 163, acerca das informações apresentadas e dos conceitos de ataques e dispositivos de segurança de redes de computadores e criptografia.

**161** Quando do uso de criptografia simétrica, as transformações relacionadas à segurança, realizadas nos lados do emissor (E) e do destinatário (D), devem ser efetuadas com o uso de uma informação secreta denominada chave. Essa chave pode ser permanente ou transitória, conforme o desenho dos algoritmos e protocolos de criptografia empregados. No caso do protocolo https, por exemplo, empregam-se, entre outros aspectos, dois tipos de chaves: chaves criptográficas simétricas e transitórias, bem como chaves assimétricas permanentes. Adicionalmente, chaves de ambos os tipos podem ser geradas no lado do emissor (E) ou do destinatário (D) da mensagem, bem como são trocadas com o outro lado por meio de um canal de confiança estabelecido com um terceiro confiável (TC), que é comum ao emissor e ao destinatário.

**162** Considere a seguinte situação hipotética. Um analista foi incumbido de construir um sistema de comunicações seguro baseado em uma combinação de cifragem simétrica e esteganografia no qual as mensagens trocadas entre o emissor (E) e o destinatário (D) sejam sempre de pequeno tamanho e que apenas uma pequena quantidade de mensagens seja eventualmente trocada durante todo o ciclo de vida do sistema. De acordo com os critérios de segurança do sistema, deverá ser provida absoluta confidencialidade do teor das mensagens, em detrimento de integridade e disponibilidade. Para tal tarefa, o implementador dispõe de um gerador de números aleatórios de elevadíssima qualidade, mas precisa fazer uma implementação de grande simplicidade. Esses critérios e o desenho do sistema de cifragem não são conhecidos pelo oponente (O).

Nessa situação, é mais adequado que o implementador do sistema adote um modelo com base na técnica de *one-time pad*, que utiliza uma cifra de fluxo, em vez de um modelo baseado no algoritmo DES (*data encryption standard*), que utiliza cifra de bloco.

**163** Considerando que o modelo mostrado na figura seja empregado na arquitetura de um serviço de controle de acesso baseado no Kerberos, em que existe um domínio de rede que contém um servidor Kerberos, vários servidores de recursos — destinatários (D) — e vários clientes de recursos — emissores (E), é correto afirmar que: o servidor Kerberos precisa conhecer senhas de autenticação dos clientes; o servidor Kerberos precisa compartilhar chaves criptográficas simétricas com cada servidor de recursos (D); para obter bilhetes de acesso a cada servidor de recursos (D) individual do domínio de rede, o cliente de recursos (E) precisa dialogar com o servidor Kerberos.

Durante resposta a um incidente de segurança em um ambiente de rede de computadores, um analista de segurança de tecnologia da informação (TI) precisou empregar várias técnicas e ferramentas para realizar coleta de dados em vários *hosts* e dispositivos de rede, relativas à possível presença de *malwares*. Algumas das técnicas e das ferramentas e alguns dos dados coletados foram os seguintes:

- I portas TCP/IP abertas nos computadores da rede, por meio da execução de varredura;
- II relatos de detecção de infecções por vírus, por meio de antivírus;
- III log de aplicações das regras no *firewall* da rede, por meio de inspeção;
- IV nomes e assinaturas dos processos computacionais em execução em um computador em determinado espaço de tempo, por meio de *software* apropriado.

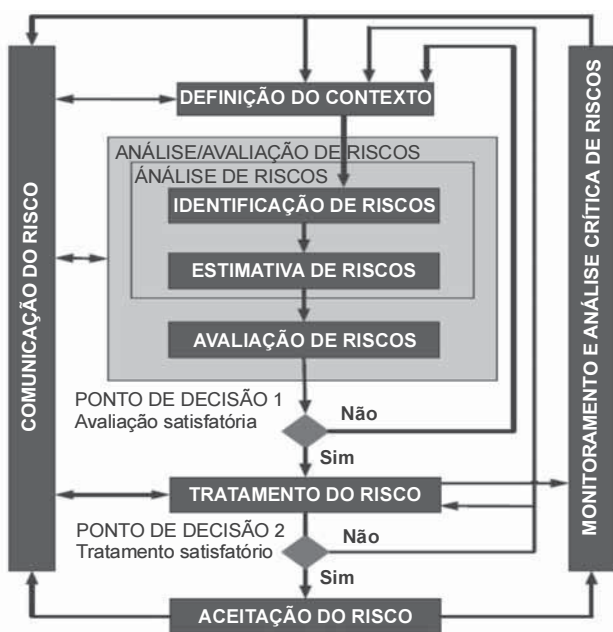
Considerando essa situação hipotética, se a comparação que o analista de segurança realizar com a última linha de base segura de determinado computador indicar que

**164** ocorreu um aumento na quantidade e qualidade de registros relativos aos aspectos I e III da linha base, mas não ao aspecto IV, então isso sugerirá a presença de *worms* e *backdoors* na rede.

**165** não há alterações junto a nenhum dos fatores I, II, III e IV, então isso evidenciará que não há infecção por *malwares*.

Acerca dos processos típicos de tratamento de incidentes de segurança, julgue o item abaixo.

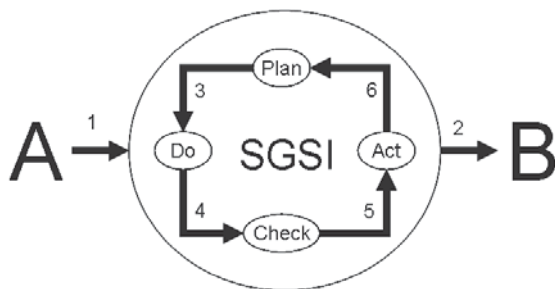
**166** O aumento do tempo decorrente entre a detecção e o fim da recuperação, nos incidentes de segurança, não aumenta necessariamente o tempo de indisponibilidade do serviço afetado.



Acerca do processo ilustrado na figura acima, que apresenta as principais atividades envolvidas na gestão de riscos, conforme a ABNT NBR ISO/IEC 27005, publicada em 2008, julgue os próximos itens.

**167** Durante o início da adoção da gestão de riscos em uma organização, a aplicação de métodos quantitativos para cálculo do nível de risco ocorre principalmente durante a estimativa de riscos e tende a oferecer resultados mais confiáveis e eficazes comparativamente ao uso de métodos quantitativos, sobretudo quando os ativos no escopo apresentam elevada intangibilidade.

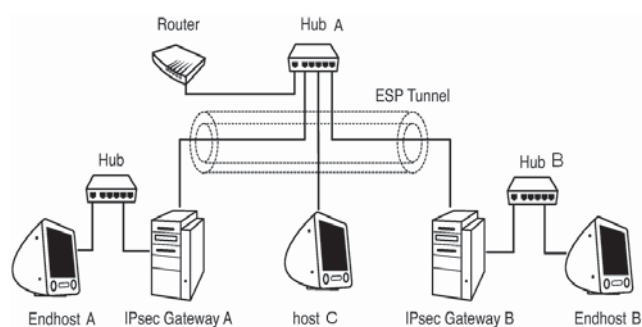
**168** A alta gestão da organização em escopo exerce maior influência sobre o ponto de decisão 1 que sobre o ponto de decisão 2, bem como contribui ativamente para prover informações quanto às fases de identificação de riscos, de definição do contexto e de análise crítica de riscos.



A respeito do diagrama acima, que apresenta um modelo conceitual sistêmico da norma ABNT NBR ISO/IEC 27001, julgue os itens **169** e **170**.

**169** No modelo em apreço, o subsistema de planejamento do SGSI possui sobreposição de atividades com a fase de definição do contexto presente na norma ABNT NBR ISO/IEC 27005 bem como produz uma informação de saída similar àquela produzida durante o processo de aceitação do risco da mesma ABNT NBR ISO/IEC 27005.

**170** Entre os documentos e registros cujo controle é demandado pela norma ABNT NBR ISO/IEC 27001, destacam-se como documentos a declaração da política de segurança, o relatório de análise/avaliação de risco e a declaração de aplicabilidade; além disso, destacam-se como registros os livros de visitantes, os relatórios de auditoria, as ocorrências de incidentes de segurança e outros registros, inclusive de não conformidade.



Internet: <www.isg.rhul.ac.uk> (com adaptações).

O modelo da figura acima apresenta elementos individualmente nomeados e presentes em uma rede hipotética, acerca dos quais é possível inferir características de protocolos de segurança. Julgue os itens seguintes, acerca das informações apresentadas e de dispositivos de segurança de redes de computadores.

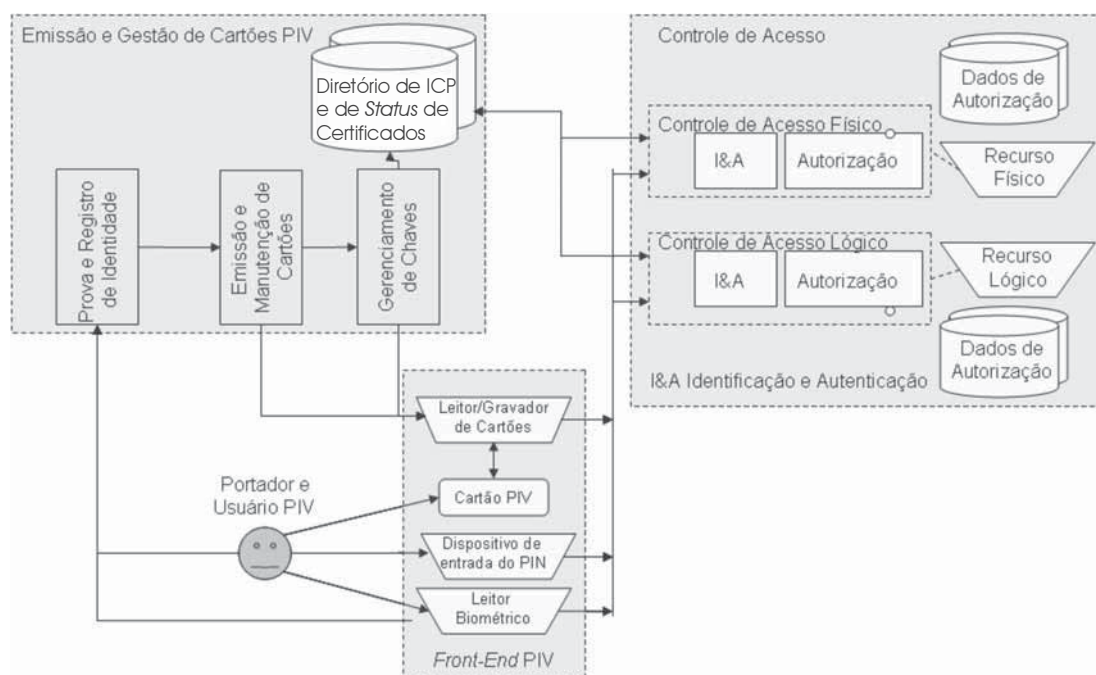
**171** Se os Endhosts A e B trocarem vários pacotes por meio de seus respectivos *gateways*, então não haverá modo fácil de o *host C* identificar quais dos pacotes IP trafegados entre os *gateways A* e *B* são relativos à comunicação entre os Endhosts A e B.

**172** Considerando a necessidade de instalar um IDS para proteger a rede A, algumas opções podem ser adotadas, entre elas a de usar um sistema passivo ou ativo, bem como a de usar um sistema baseado em *host* ou em rede. Se a solução for adotar um sistema passivo e com base em *host*, então o *host C* poderá ser uma máquina adequada para essa necessidade. Se a solução for adotar um sistema reativo e embasado na rede, então podem-se usar os *gateways A* ou *B*. Se a solução for adotar um sistema reativo e baseado em *host*, então se poderá usar o *host C*.



Considerando a figura acima, que apresenta o modelo sistêmico de gestão de continuidade de negócios proposto pelas normas ABNT NBR 15999, em que se destacam processos numerados de 1 a 6, bem como fluxos nomeados A até D, julgue os próximos itens.

- 173 A determinação de RTOs (objetivos de tempo de recuperação) ocorre apenas após a compreensão dos tempos máximos toleráveis de interrupção, sendo os RTDs insumos fundamentais para a execução de 4.
- 174 Considerando que a auditoria seja um processo sistemático, documentado e independente para obter evidências de auditoria e avaliá-las objetivamente para determinar a extensão na qual os critérios da auditoria são atendidos, é correto afirmar que evidências de auditoria são produzidas no âmbito das atividades 3, 4, 5 e 6, enquanto o processo de auditoria é realizado no âmbito da atividade 2.



Internet: <src.nist.gov> (com adaptações).

Quanto a conceitos de controle de acesso e segurança de ambientes físicos e lógicos e às informações contidas na figura acima, que apresenta um modelo arquitetural da plataforma de verificação de identidade pessoal PIV, proposta pelo órgão de padronização norte-americano NIST, julgue os itens a seguir.

- 175 A plataforma apresentada na figura suporta identificação por múltiplos fatores; contempla atribuições de autoridades de registro em modelo de infraestrutura de chaves públicas; não apresenta incompatibilidade com o uso de listas de certificados revogados (CRLs).
- 176 Não há como determinar se o modelo dessa figura emprega controle de acesso discricionário ou mandatório ou ambos.

A lista abaixo apresenta os títulos das seções da norma ABNT NBR ISO/IEC 27002 (17799), que contém um guia das melhores práticas em gestão da segurança da informação. Tais seções possuem correspondente registro no anexo A da norma ABNT NBR ISO/IEC 27001, definindo grupos de objetivos de controles e controles de segurança que podem ser implementados.

- 5 Política de Segurança
- 6 Organizando a Segurança da Informação
- 7 Gestão de Ativos
- 8 Segurança em Recursos Humanos
- 9 Segurança Física e do Ambiente
- 10 Gerenciamento das Operações e Comunicações
- 11 Controle de Acessos
- 12 Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação
- 13 Gestão de Incidentes de Segurança da Informação
- 14 Gestão da Continuidade do Negócio
- 15 Conformidade

Nos itens de **177** a **180**, julgue as propostas de associação entre conceitos ou práticas de segurança e as seções da norma ABNT NBR ISO/IEC 27002.

**177** O emprego de um ambiente computacional dedicado isolado, bem como a blindagem eletromagnética e o levantamento dos ativos envolvidos em processos críticos são abordagens diretamente associadas ao Controle de Acessos, à Segurança Física e do Ambiente e à Gestão da Continuidade do Negócio, respectivamente.

**178** Os profissionais de segurança que realizam análise crítica de logs e controle de vulnerabilidades técnicas relacionam-se mais fortemente com os aspectos de Organização da Segurança da Informação, que com a Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação.

**179** A configuração de proteções de tela bloqueadas por senha e o uso de *firewalls* e sistemas de detecção de intrusos são ações apenas indiretamente ligadas à gestão de Incidentes de Segurança da Informação e à Conformidade, respectivamente.

**180** A proteção de registros organizacionais, entre eles o registro de visitantes, constitui uma prática diretamente associada à Segurança Física e do Ambiente, embora, no caso específico do registro de visitantes, esteja prescrita visando o alcance da Segurança em Recursos Humanos.

Atualmente, existe a tendência de as organizações se adaptarem rapidamente às mudanças que ocorrem no mercado globalizado, o qual se torna cada vez mais competitivo. Isso gera necessidade de mudança mais ágil também nas estratégias das empresas, a fim de se adequarem à nova realidade. No caso das organizações públicas, a situação não é diferente. Várias delas adotam novas tecnologias e processos de trabalho, especialmente nas áreas de interface com a tecnologia da informação (TI), em aderência a modelos consagrados nos mercados privado e público internacionais. Entretanto, o ritmo de mudança em uma empresa privada, normalmente, é maior que nas públicas. A TI desempenha importante papel nessa mudança e precisa, cada vez mais, se alinhar com a estratégia organizacional.

Tendo as informações acima como referência inicial e considerando questões acerca de planejamento estratégico em conjunto com a TI, sobretudo dentro dos conceitos de gestão e governança, julgue os itens de **181** a **183**.

**181** A estratégia de TI pode ser definida como um padrão no fluxo de ações e decisões da organização, desenvolvido pelos tomadores de decisão, cujo objetivo é identificar as oportunidades nas quais os sistemas de informação existentes podem apoiar os negócios da empresa, conduzindo às mudanças e à inovação organizacional.

**182** O planejamento estratégico, um processo regularmente executado no âmbito organizacional, define a maneira pela qual a estratégia de uma organização é desenvolvida e prescreve o emprego da TI para executar o plano de ações, a fim de cumprir as metas estratégicas estabelecidas. O alinhamento entre as metas de negócio (organizacionais) e os resultados da TI pode ser calculado, segundo o modelo COBIT, por meio do mapeamento direto dos indicadores de desempenho da TI para os indicadores de meta do negócio.

**183** No processo de aumento de maturidade da TI em grandes empresas heterogêneas ou geograficamente dispersas, o estabelecimento de sistemas de informação federados, de forma geral, ocorre apenas após a adoção de modelos *adhocráticos*. Isso é especialmente verdadeiro se consideradas as oportunidades da microcomputação presentes nos anos 80 e 90 do século passado, as quais deram aos departamentos e unidades isoladas de grandes empresas a capacidade de organizarem suas soluções de TI individuais em desconformidade com os padrões estabelecidos pelo órgão central de TI, supondo-se que o mesmo era anteriormente presente.

Quanto à estrutura geral do guia PMBOK em sua terceira versão e à gestão de projetos, julgue os seguintes itens.

**184** Quando da execução de um projeto conforme o modelo PMBOK, seu gestor pode utilizar processos oriundos de cinco grupos distintos, denominados: iniciação; planejamento; monitoramento e controle; execução; e encerramento. São exemplos de características de algumas ferramentas empregadas por processos presentes em cada um desses grupos, respectivamente: basear-se no uso de opinião especializada; desenvolver simulações embasadas na técnica de Monte Carlo; atualizar contas de controle; realizar sessões de lições aprendidas; e atualizar ativos de processos organizacionais.

**185** Na disciplina de gerenciamento de aquisições, o processo denominado planejar compras e aquisições depende da estrutura analítica de projetos em maior intensidade quando comparado aos demais processos. Nessa disciplina, também existem, entre outros, os processos: solicitar respostas de fornecedores; selecionar fornecedores; e planejar contratações.

**186** Se, em um projeto, o valor agregado a um componente da estrutura analítica de projetos ou atividade do cronograma for inferior ao custo real correspondente ao elemento em foco (componente ou atividade), o índice de desempenho de custos correspondente ao elemento assumirá um valor maior que um, sinalizando que o projeto pode estar acima do orçamento.

Com relação à estrutura, aos processos e às funções do ITIL versão 3, julgue os itens que se seguem.

**187** No modelo ITIL, versão 3, o provimento de funções e os processos relacionados à gestão da segurança da informação se relacionam a mais de uma das fases do ciclo de vida de serviços de TI, pois o gerenciamento de disponibilidade e o gerenciamento de continuidade de serviços de TI são aspectos diretamente concernentes à segurança e encontram-se organizados na fase de desenho de serviço, enquanto os gerenciamentos de acessos e de incidentes, também relacionados à gestão da segurança, encontram-se organizados na fase de operação de serviços.

**188** Acerca de modelos de provisionamento de serviço de TI definidos pelo ITIL, a decisão por adotar um modelo embasado em *utility* confere maior escalabilidade às soluções de serviços de TI de uma organização, quando comparado a um modelo de serviços gerenciados. Tal decisão, embora apresente aumento de riscos de segurança no que concerne à confidencialidade, não implica, adicionalmente, o aumento de competências internas para gerenciamento de capacidade de recursos.

**189** São métricas adotadas no modelo ITIL: *mean time between failures* (MTBF), *mean time between service incidents* (MTBSI), *mean time to repair* (MTTR) e *mean time to restore service* (MTRS). O MTBSI pode ser definido como a soma do MTBF e do MTRS; e o MTRS é sempre maior ou igual ao MTTR.

**190** No desenvolvimento de uma estratégia de continuidade de serviços de TI, o uso de soluções de *cold site*, em vez de soluções de *hot stand by*, indica que o tempo máximo tolerável de interrupção dos serviços de TI é superior a 24 horas, o que não seria verdade caso a segunda solução fosse adotada.

**191** Se, em uma base de dados de erros conhecidos de uma organização que possui alto nível de maturidade no modelo ITIL, existe um número  $x$  de registros de erros, então é de se esperar que exista uma quantidade: de registros de problemas aproximadamente igual a  $x$ ;  $kx$  de registros de incidentes, em que  $k$  é um número superior a 1;  $lx$  de pacotes de *release*, em que  $l$  é um número superior a 1.

O COBIT apoia o alcance da governança de TI por meio de um *framework* que garante que a TI esteja alinhada ao negócio. Considerando o COBIT e a governança de TI, julgue os próximos itens.

**192** O gerenciamento de recursos trata do gerenciamento apropriado de recursos críticos de TI, os quais são processos, pessoas, aplicações, infraestrutura e informação.

**193** Constituem métricas que apoiam diretamente o alcance do objetivo de controle sobre processos de TI: o percentual de papéis da organização de TI com posição e responsabilidades documentadas; e a quantidade de unidades organizacionais não apoiadas pela organização de TI, mas que deveriam sê-lo, conforme apresenta a estratégia organizacional. Tal objetivo de controle pertence ao domínio de planejamento e organização do COBIT.

**194** A medição do *turnover* do pessoal de TI bem como a porcentagem de pessoas de TI certificadas conforme as necessidades do negócio constituem métricas que apoiam diretamente o alcance de objetivos de controle sobre processos de TI pertencentes ao domínio de aquisição e entrega.

A respeito da organização do modelo CMMI, julgue os itens de **195** a **197**.

**195** Seis são os níveis nos quais se pode mensurar o desempenho de metas e práticas relacionadas a uma área de processo individual, enquanto cinco são os níveis nos quais se pode mensurar o alcance de platôs evolucionários para a melhoria de processos organizacionais. A medição de capacidades de processos é requisito para a medição de maturidade organizacional.

**196** São produtos de trabalho típicos encontrados em organizações que estão no nível de maturidade 2 segundo o modelo CMMI: diagramas de causa e efeito; declarações das necessidades e objetivos dos processos da organização; listas de fontes de riscos, de origem interna e externa.

**197** Testes de cobertura de caminhos, normas e políticas organizacionais, relatórios de avaliação de produtos de *software* de prateleira (COTS) são artefatos de trabalho típicos que caracterizam uma organização que desempenha processos de validação no nível de capacidade 1.

Julgue os itens a seguir, a respeito de aspectos específicos da contratação de bens e serviços de TI.

**198** A Instrução Normativa n.º 4 SLTI/MPOG regulamenta a Lei n.º 8.666/1993 no que concerne a introduzir a obrigatoriedade de apresentação do PDTI do órgão licitante durante um certame licitatório.

**199** Quando da execução da fase de planejamento da contratação de um serviço de TI, nos moldes da Instrução Normativa n.º 4 SLTI/MPOG, o desenvolvimento de um plano de sustentação pode ser efetuado antes da definição da estratégia de contratação do órgão, e deve ser realizado pela área de TI. Em tal plano, devem estar articulados os seguintes conceitos: confidencialidade; integridade; disponibilidade; pessoas; infraestrutura; conhecimento; contratos; continuidade; e autenticidade.

**200** Nas compras públicas por meio do pregão eletrônico, em conformidade com as normas federais vigentes: o encaminhamento de lances ocorre apenas após a abertura da etapa competitiva; é possível realizar lances sucessivos, porém estes sempre devem assumir valores decrescentes; o tempo médio para encerramento da recepção dos lances é, teoricamente, de quinze minutos após o aviso de fechamento iminente.

## PROVA DISCURSIVA P<sub>4</sub>

- Nesta prova, faça o que se pede, usando os espaços para rascunho indicados no presente caderno. Em seguida, transcreva os textos para o **CADERNO DE TEXTOS DEFINITIVOS DA PROVA DISCURSIVA P<sub>4</sub>**, nos locais apropriados, pois **não serão avaliados fragmentos de texto escritos em locais indevidos**.
- Qualquer fragmento de texto além da extensão máxima de linhas disponibilizadas será desconsiderado. Será também desconsiderado o texto que não for escrito no(s) espaço(s) correspondente(s) do **caderno de textos definitivos**.
- No **caderno de textos definitivos**, identifique-se apenas no cabeçalho da primeira página, pois **não será avaliado** texto que tenha qualquer assinatura ou marca identificadora fora do local apropriado.

### QUESTÃO

Organizações bem-sucedidas compreendem os benefícios da tecnologia da informação (TI) e utilizam esse conhecimento para direcionar valor aos seus intervenientes. Elas reconhecem a dependência crítica de muitos processos de negócio relativamente à TI, bem como a necessidade de se adequarem às demandas crescentes por conformidade e os benefícios da gestão efetiva do risco.

Tendo o texto acima unicamente como motivador, e considerando a importância atribuída à adoção de modelos de governança COBIT e ITIL por órgãos de controle brasileiros, descreva algumas sobreposições e divergências de abordagem que existem entre esses dois modelos de governança de TI. Na sua descrição, indique, necessariamente:

- ▶ processos COBIT do domínio de planejamento e organização do modelo COBIT não abordados de forma sistemática pelas funções e(ou) processos do modelo ITIL, versão 3;
- ▶ funções e(ou) processos do modelo ITIL, versão 3, relacionados com o domínio de monitoramento e avaliação do modelo COBIT;
- ▶ processos e domínios do modelo COBIT relacionados ao desenho de serviços do modelo ITIL, versão 3.



**RASCUNHO – QUESTÃO**

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	

Considerando que você tenha sido encarregado de desenvolver a arquitetura de uma aplicação *web* para funcionar em ambiente de *extranet* que vise gerir informações acerca de atividades de controle externo no âmbito de todo o território nacional, redija um texto dissertativo que apresente a descrição dessa arquitetura e que aborde, necessariamente, os seguintes aspectos:

- ▶ aderência à plataforma JEE, incluindo uso de servlets, JSP, Ajax, JSF, XSL e Hibernate;
- ▶ *web services* e arquitetura orientada a serviços;
- ▶ promoção de aderência aos estágios avançados do modelo de gestão do *e-ping* no que concerne à criação e à manutenção de sítios.

**RASCUNHO – PEÇA TÉCNICA – 1/2**

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	

## RASCUNHO – PEÇA TÉCNICA – 2/2

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	