

Questões comentadas – SEFAZ-RS - 2019 2

Cargo: Auditor – Assunto: Tecnologia da Informação..... 2



QUESTÕES COMENTADAS – SEFAZ-RS - 2019

CARGO: AUDITOR – ASSUNTO: TECNOLOGIA DA INFORMAÇÃO

55. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: ITIL

Em determinado órgão, foi identificada a necessidade de solucionar os seguintes problemas:

- (a) Ausência de gerenciamento dos *softwares* desenvolvidos internamente, quanto a versão, recursos e arquiteturas;
- (b) Falhas na entrega de informações que deveriam ser precisas, na perspectiva de serem corretas, para a pessoas certa, no momento certo.

De acordo com a ITIL v3, esses problemas podem ser resolvidos com a implantação

- a) Do processo gerenciamento da liberação, para ambos.
- b) Do processo gerenciamento de nível de serviço, para ambos.
- c) Da função gerenciamento de aplicativo, para (a), e do processo gerenciamento de conhecimento, para (b).
- d) Do processo gerenciamento de problemas, para ambos.
- e) Do processo gerenciamento de configuração, para (a), e da função central de serviços, para (b).

Comentário: Os problemas descritos no texto são resolvidos por uma função do estágio de operação de serviços e por um processo do estágio de transição, quais sejam:

Função: Gerenciamento de aplicativo (Operação de Serviço da ITIL) - A função responsável por gerenciar aplicativos durante os seus ciclos de vida.

Processo: Gerenciamento de conhecimento (Transição de Serviço da ITIL) - O processo responsável por **compartilhar perspectivas, ideias, experiência e informações, e por garantir que estejam disponíveis no lugar certo, no momento certo**. O processo de gerenciamento de conhecimento possibilita a tomada de decisões bem informadas e melhora a eficiência reduzindo a necessidade de redescobrir o conhecimento.

Assim, podemos marcar nossa resposta na alternativa C.

Gabarito: C

56. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: ITIL

Em auditoria externa para analisar um serviço implementado em determinado órgão, o auditor observou que esse serviço seguia inicialmente as boas práticas da ITIL, mas passou a ficar inoperante ou com baixa performance em alguns momentos, durante picos de acesso. O auditor constatou ainda, que não havia tido avaliação prévia sobre picos de demanda.

De acordo com a ITIL v3, esses problemas podem ser resolvidos com a implantação



- a) De incidentes, que, no caso descrito, ficaria limitado ao atendimento da inoperância e aos casos de baixa performance com a função central de serviços.
- b) Da demanda do estágio de estratégia que visa gerenciar os ciclos de produção dos serviços e ciclos de consumo dos serviços.
- c) De disponibilidade, especialmente no que se refere à métrica MTTR, que mede a performance dos serviços.
- d) De capacidade do estágio de transição, especialmente no que se refere a quantidade de recursos necessários para o sistema funcionar sem interrupções.
- e) De mudança no estágio de desenho, especialmente no que se refere à mensuração da capacidade prévia necessária para uso do serviço.

Comentário: Vamos analisar cada uma das alternativas:

A – Errada: Gerenciamento de incidente (Operação de Serviço da ITIL) - O processo responsável por gerenciar o ciclo de vida de todos os incidentes. O gerenciamento de incidente garante que a operação normal de um serviço seja restaurada tão rapidamente quando possível e que o impacto no negócio seja minimizado. Percebe que o incidente não trabalha com previsão de demanda futura dos serviços. Ele controla apenas o ciclo de vida da informação.

B – Certa: Gerenciamento de demanda (Estratégia de Serviço da ITIL) - O processo responsável pelo entendimento, previsão e influência da demanda do cliente por serviços. O gerenciamento de demanda trabalha com o gerenciamento de capacidade para garantir que o provedor de serviço tenha capacidade suficiente para atender à demanda exigida.

Em um nível estratégico, o gerenciamento de demanda pode envolver análise de padrões de atividade de negócio e perfis de usuário, enquanto, em nível tático, pode envolver o uso de cobrança diferenciada para estimular clientes a usar os serviços de TI em horários menos ocupados ou exigir atividades em curto prazo para responder à demanda inesperada ou à falha de um item de configuração.

C – Errada: MTTR – Mean Time to Repair - é um indicador de desempenho usado na manutenção para indicar o Tempo Médio Para Reparo de algum equipamento, componente, máquina ou sistema. Veja que esse indicador não vai resolver os problemas da demanda.

D – Errada: O gerenciamento da capacidade é um processo descrito no livro de desenho de serviço. Aqui já temos o erro na alternativa. O processo é responsável por garantir que a capacidade dos serviços de TI e a infraestrutura de TI sejam capazes de atender aos requisitos relacionados à capacidade e ao desempenho acordados de maneira oportuna e eficaz em custo.

E – Errada: O gerenciamento de mudanças está presente no estágio de transição. A alternativa afirma que é um processo de desenho. O processo responsável pelo controle do ciclo de vida de todas as mudanças, permitindo que mudanças benéficas sejam feitas com o mínimo de interrupção aos serviços de TI.

Gabarito: B



57. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: PMBOK

QUESTÃO 57

No desenvolvimento de um produto, verificou-se que não havia identificação de precedência entre algumas atividades antes do início das execuções.

De acordo com o PMBOK, a representação das relações lógicas entre as atividades do projeto é obtida com

- Ⓐ a técnica Delphi.
- Ⓑ a estrutura analítica do projeto (EAP).
- Ⓒ o diagrama de rede do cronograma do projeto.
- Ⓓ a matriz de rastreabilidade de requisitos.
- Ⓔ a linha de base do escopo.

Comentário: Vejamos as definições de cada um dos termos acima.

A – Técnica Delphi: O Método Delphi é baseado no princípio que **as previsões por um grupo estruturado de especialistas** são mais precisas se comparadas às provenientes de grupos não estruturados ou individuais.

B – Estrutura Analítica do Projeto (EAP): A EAP ou WBS, *work breakdown structure*, define as entregas do projeto e sua decomposição em Pacotes de trabalho.

C – Diagrama de rede do cronograma do projeto: Sequenciar atividades envolve identificar as atividades e marcos do projeto e colocá-los numa ordem lógica, o resultado dessa sequência pode ser analisado através do “Diagrama de Redes”. Existem vários métodos para se desenhar um diagrama de redes, atualmente o mais utilizado é o método do diagrama de precedência (MDP) ou Atividade no nó (ANN). Nesse método, os nós são usados para representar atividades, e as setas mostram as dependências entre as atividades. **Veja que essa é a resposta da nossa questão.**

D – Matriz de rastreabilidade de requisitos: Segundo o Guia PMBOK®, a matriz de rastreabilidade dos requisitos associa os requisitos às suas origens e os rastreia durante todo o ciclo de vida do projeto.



E – Linha de base do escopo: A Linha de base do escopo é composta pelos artefatos que servem para orientar a equipe do projeto em relação as entregas e o resultado esperado do projeto.

Gabarito: C

58. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: PMBOK

QUESTÃO 58

Assinale a opção que indica o documento que, no projeto de um novo serviço, é descrito na área de conhecimento integração no PMBOK e, apesar de não ser considerado um contrato, informa as necessidades do negócio, as premissas e os requisitos de alto nível do cliente.

- Ⓐ registro das mudanças
- Ⓑ estrutura analítica do projeto (EAP)
- Ⓒ plano de gerenciamento da qualidade
- Ⓓ termo de abertura de projeto
- Ⓔ plano de gerenciamento do projeto

Comentário: Essa questão se refere ao termo de abertura de projeto. Considerado um dos principais documentos elaborados durante o ciclo de vida do projeto. Vejamos o que o PMBOK fala sobre o termo de abertura segundo o PMBOK:

“Desenvolver o termo de abertura do projeto é o processo de desenvolver um documento que **formalmente autoriza a existência de um projeto** e **dá ao gerente do projeto a autoridade** necessária para aplicar recursos organizacionais às atividades do projeto. O principal benefício deste processo é um início de projeto e limites de projeto bem definidos, a criação de um registro formal do projeto, e **uma maneira direta da direção executiva aceitar e se comprometer formalmente com o projeto.**”

Gabarito: D



59. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: ITIL e PMBOK

QUESTÃO 59

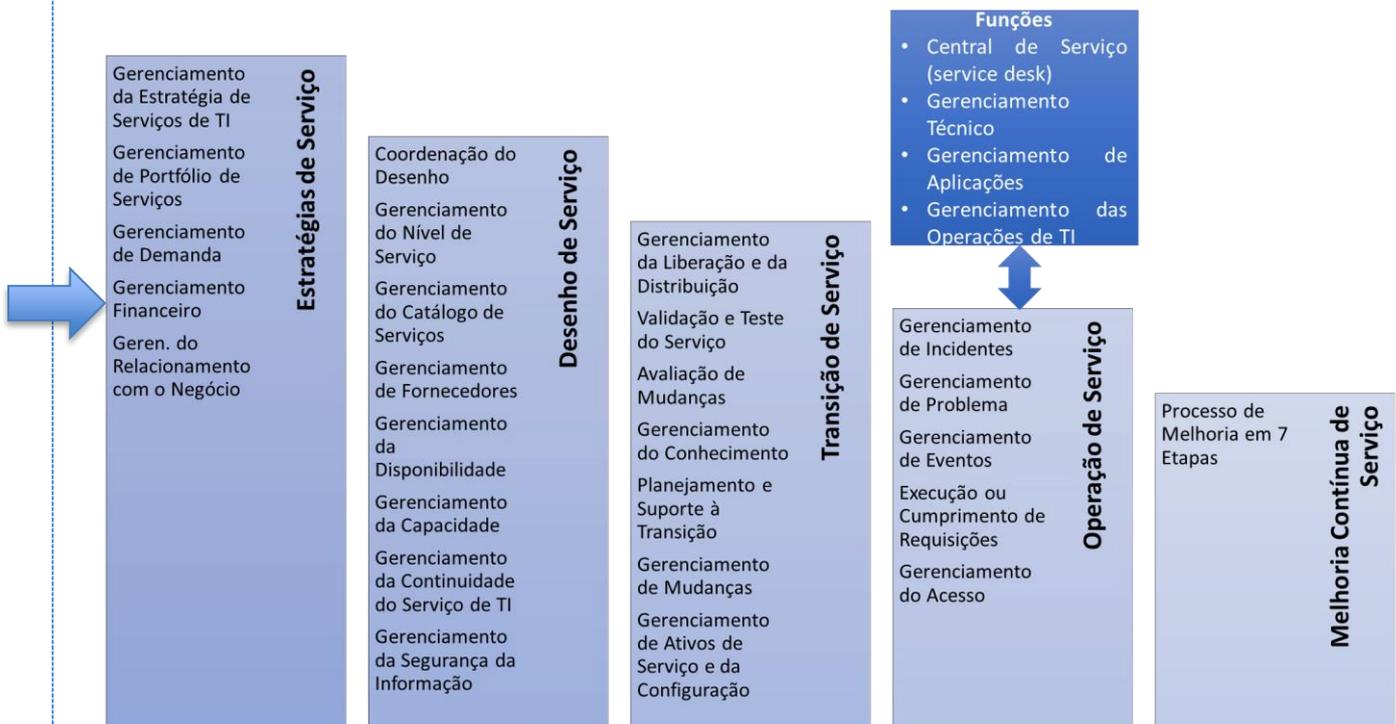
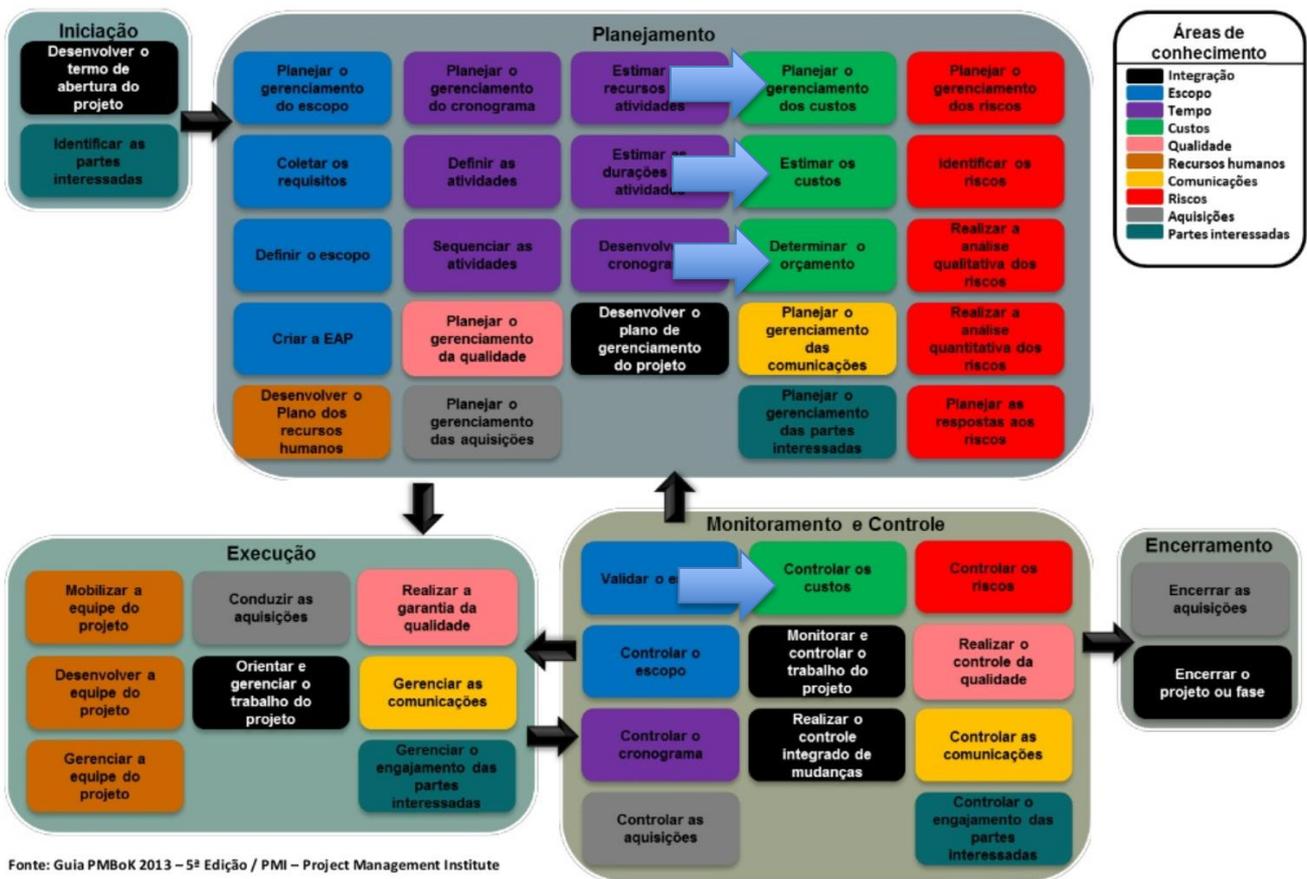
É dispensável que o gerenciamento de finanças como custos e orçamentos conste em guias e(ou) modelos de governança de TI, apesar de esse tipo de gerenciamento caracterizar ação associada à governança. Aliado ao gerenciamento de finanças, o orçamento

- Ⓐ é abordado na ITIL, no estágio estratégia, e no PMBOK, no gerenciamento de custos do projeto.
- Ⓑ é abordado no PMBOK, no gerenciamento financeiro do projeto, mas não na ITIL.
- Ⓒ é abordado na ITIL, no estágio desenho, e no PMBOK, na área de conhecimento gerenciamento do escopo do projeto.
- Ⓓ não é abordado na ITIL nem no PMBOK.
- Ⓔ é abordado na ITIL, no gerenciamento financeiro, mas não no PMBOK.

Comentário: Para responder a essa pergunta podemos olhara para duas figuras que fizeram parte do seu dia a dia de estudos para essa prova, elas definem os processos do ITIL e do PMBOK:



Grupos de Processos e Áreas de Conhecimento em Gerenciamento de Projetos



Observem que o gerenciamento financeiro aparece na estratégia de serviços do ITIL e temos 4 processos na área de conhecimento de gerenciamento de custos.

Gabarito: A



60. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: ITIL

QUESTÃO 60

Ao rever a aplicação da ITIL em determinado órgão, um auditor verificou que os processos gerenciamento da mudança e gerenciamento da configuração e de ativos de serviço atuavam em outros estágios além daquele em que se encontram organizados na ITIL v3.

À luz da ITIL v3, infere-se desse achado da auditoria

- A** irregularidade, pois somente o processo gerenciamento da configuração e de ativos de serviço pode atuar fora do seu estágio.
- B** ausência de irregularidade, pois todos os processos do estágio transição podem operar tanto nos respectivos estágios quanto no estágio operação.
- C** ausência de irregularidade, pois ambos os processos atuam em todo o ciclo de vida, apesar de descritos no estágio transição de serviços.
- D** irregularidade, pois todos os processos da ITIL atuam somente nos estágios aos quais eles pertencem.
- E** irregularidade, pois somente o processo gerenciamento da mudança pode atuar fora do seu estágio.

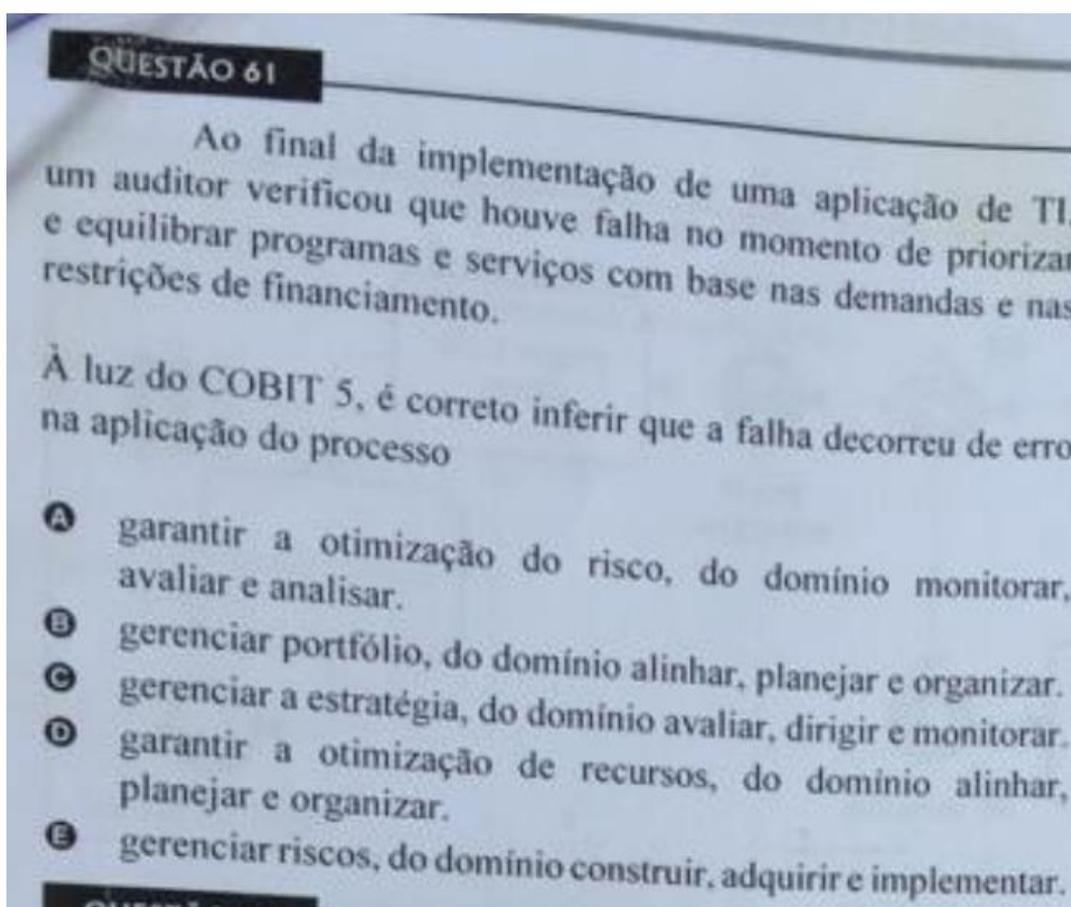
Comentário: Essa questão é interessantes e pode ser respondida com o mapa mental que apresentamos no nosso curso. Veja a parte do mapa que trata de transição de serviços:



Assim, percebemos que, embora esses 3 processos façam parte do livro de transição de serviços, eles são considerados processos genéricos, ou seja, são válidos para todo o ciclo de vida do serviço.

Gabarito: C

61. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: COBIT



Comentário: Essa questão exige que você tenha decorado os processos do COBIT para eliminar as alternativas C, D e E. Veja que gerenciar a estratégia é um processo do domínio (APO – Alinhar, Planeja e Organizar), garantir a otimização de recursos faz parte do domínio (ADM – Avaliar, Dirigir e Monitorar) e o gerenciamento de riscos faz parte do domínio (APO).

Já a alternativa A trata de otimização de riscos que não tem relação com a priorização e equilíbrio dos serviços. Quem é responsável por essas ações é justamente o gerenciamento de portfólio. Logo, temos nossa resposta na alternativa B

Gabarito: B

62. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: ITIL

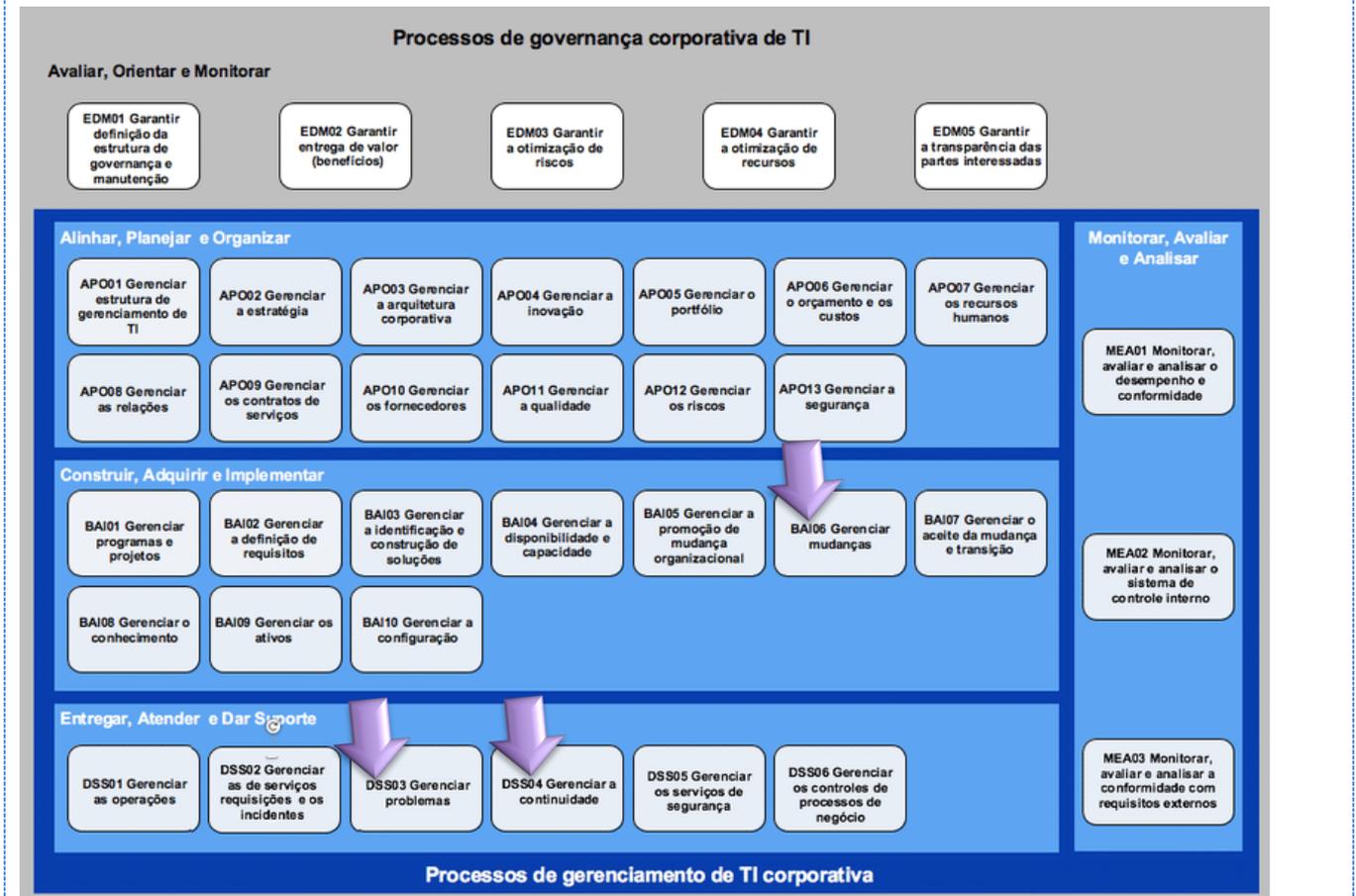
QUESTÃO 62

O diretor de TI de determinado órgão implantou, de acordo com a ITIL v3, os processos voltados para gerenciar mudanças, gerenciar problemas e gerenciar a continuidade de serviço.

Nessa situação, a implantação do COBIT 5 para as mesmas finalidades mencionadas seria

- A) inviável, pois no COBIT há somente o processo gerenciar continuidade.
- B) inviável, pois no COBIT há somente os processos gerenciar mudanças e gerenciar problemas.
- C) apropriada, pois esses processos também se encontram no COBIT.
- D) inviável, pois no COBIT há somente os processos gerenciar continuidade e gerenciar problemas.
- E) apropriada, pois o COBIT lida apenas com a governança de TI, o que não interfere nesses processos.

Comentário: Observe o mapa de processos abaixo e tente encontrar os processos descritos no enunciado:



Gabarito: C



63. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: ITIL, COBIT, PMBOK

QUESTÃO 63

No tocante à implantação de processos de governança, assinale a opção correta, acerca da gestão de recursos humanos e de pessoas, conforme as boas práticas descritas no COBIT 5, na ITIL v3 e no PMBOK.

- A Somente o guia PMBOK inclui gestão de pessoas; a ITIL, por gerenciar serviços, não aborda os recursos humanos necessários.
- B No COBIT, não há referência a gestão de pessoas; no PMBOK consta o processo gerenciamento de recursos humanos na área de conhecimento escopo do projeto.
- C Na ITIL, as pessoas são consideradas habilidades e constituem um dos 4 Ps do desenho de serviço; no PMBOK, a área de conhecimento gerenciamento das partes interessadas do projeto lida com a gestão de pessoas.
- D A ITIL lida com pessoas estritamente no estágio estratégia; o PMBOK lida com pessoas estritamente nos processos afetos à área de conhecimento integração.
- E Nem a ITIL, nem o COBIT, nem o PMBOK mencionam a gestão de pessoas: todos eles constituem guias de boas práticas para governança de TI, exclusivamente.

Comentário: Essa talvez seja uma das questões mais chatas da prova. Vamos tentar comentar rapidamente cada uma das alternativas.

A – Errado: Tanto ITIL quanto COBIT possuem alguma relação com os recursos humanos. No COBIT as pessoas aparecem como parte da lista de **habitadores** e o processo APO07 trata do gerenciamento de recursos humanos. No ITIL temos **pessoas** como um dos 4 p's do serviço e também como um recurso tangível dos ativos de serviços.

B – Errado: Vimos na alternativa anterior que o COBIT faz referência à gestão de pessoas.

C – Certo! Essa é a nossa resposta. Conforme observamos na alternativa "A", um dos 4 P's do desenho são justamente as pessoas. Já a área do conhecimento gerenciamento de recursos humanos do PMBOK trata com mais ênfase do grupo de pessoas que trabalham diariamente no projeto. Contudo, a área de gerenciamento das partes interessadas também se preocupa com a motivação e engajamento de pessoas no projeto. Logo, podemos considerar que ela também atua na gestão de pessoas.

D – **Errada**: ITIL também lida com pessoas no desenho e o PMBOK lida com pessoas nas áreas de conhecimento de RH e Partes interessadas.

E – **Errada**: Todos dos frameworks falam de gestão de pessoas e o PMBOK é aplicado a projetos de qualquer natureza, não apenas a projetos de TI.

Gabarito: C

64. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: COBIT

QUESTÃO 64

O diretor de TI de uma empresa pública de pequeno porte deseja melhorar a governança e a gestão de TI dessa empresa.

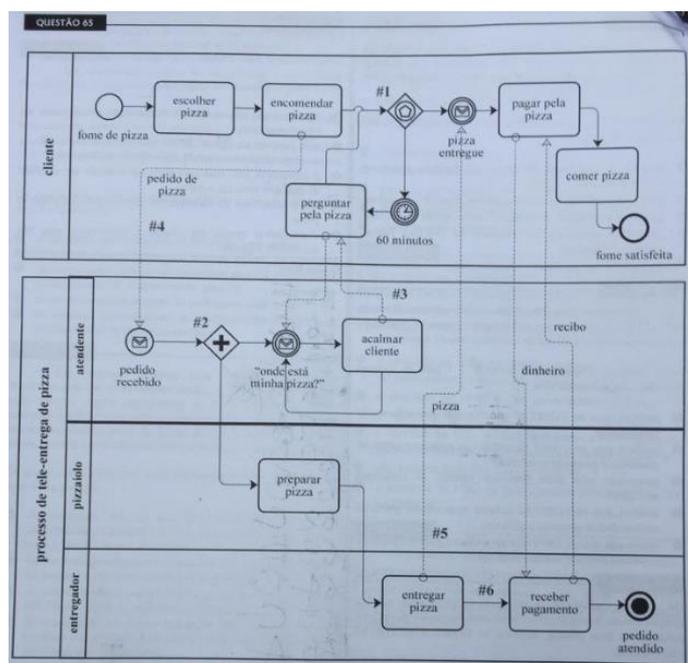
Nesse caso, a aplicação do COBIT 5

- A não é viável, pois o COBIT 5 não pode ser utilizado em empresa pública.
- B não compete ao diretor de TI, mas somente à presidência da empresa, porque alterará a governança da empresa.
- C é admissível, pois esse guia pode ser utilizado em empresa de qualquer natureza e porte.
- D não é viável, por ser incompatível com empresa de pequeno porte.
- E é admissível apenas em relação à governança, mas não em relação à gestão.

Comentário: Sabemos que o **COBIT 5** é **genérico e útil** para organizações de todos os portes, sejam comerciais, sem fins lucrativos ou públicas.

Gabarito: C

65. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: BPMN



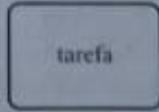
A respeito do modelo precedente, assinale a opção correta, de acordo com a BPM (*business process modeling*).

#5 ou #6 estão errados, pois dois fluxos não podem sair, ao mesmo tempo, de uma mesma tarefa. Nesse caso, o correto seria representar as saídas por meio do símbolo 

#1 indica um desvio exclusivo baseado em eventos, de modo que cada ocorrência de um dos eventos subsequentes inicia uma nova instância do processo.

#2 indica a ramificação em que se acionam todos os fluxos de saída em paralelo.

#3 está modelado de forma errada, pois a ligação entre duas raias (divisões de responsabilidade) deve ser feita, obrigatoriamente, por meio do símbolo 

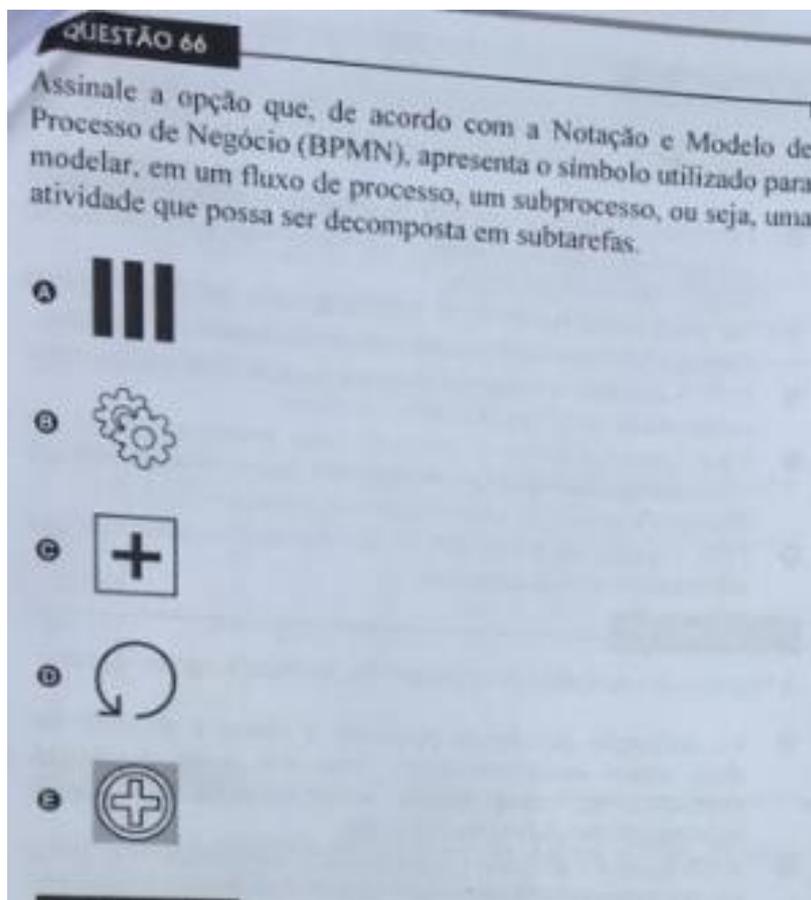
#4 não surtirá efeito, pois a ligação entre divisões é restrita a tarefas simbolizadas por 

Comentário: Vamos comentar as alternativas acima:

- A) Errada:** Não existe restrição quanto ao fato de 2 fluxos saírem da mesma tarefa. E a figura em questão apresentada determina um fluxo condicional, no qual existe uma condição associada que define se o caminho será seguido ou não.
- B) Certa:** A questão define um tipo de evento bem específico, o Desvio Exclusivo baseado em Eventos (gerador de instâncias), nele, cada ocorrência de um dos eventos subsequentes, inicia uma nova instância do processo.
- C) Errada:** Em **um ponto de ramificação** onde temos uma ativação incondicional em paralelo, todos os fluxos de saída são ativados simultaneamente. Em um ponto de convergência de fluxos, espera que todos os caminhos de entrada completem, antes de disparar o fluxo de saída. Posso estar errado, mas o CESPE vai considerar essa alternativa errada por conta da ausência da palavra **ponto**.
- D) Errada:** O desenho representado por #3 é um Fluxo de Mensagem que simboliza fluxos de informação que transpõem fronteiras internas e externas de uma organização. Podem ser conectados a Divisões, atividades ou eventos de mensagem. Logo, está modelado de forma correta.
- E) Errado:** Como visto acima, na definição de fluxo de mensagem, essa figura pode estar conectada a um evento de mensagem, que é exatamente o que acontece no diagrama.

Gabarito: B

66. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: BPMN



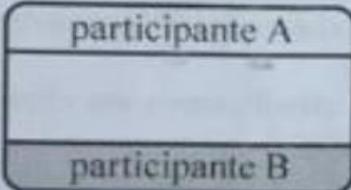
Comentário: Questão tranquila, vejamos o que cada um dos símbolos representa:

- A) Marcador de Instâncias Múltiplas em paralelo
- B) Tarefa de invocação de serviços
- C) **Marcador de subprocesso**
- D) Marcador de repetição
- E) Evento intermediário múltiplo paralelo - capturam, de uma só vez, todos os eventos de um conjunto de eventos que ocorrem em paralelo.

Gabarito: C

67. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: BPMN

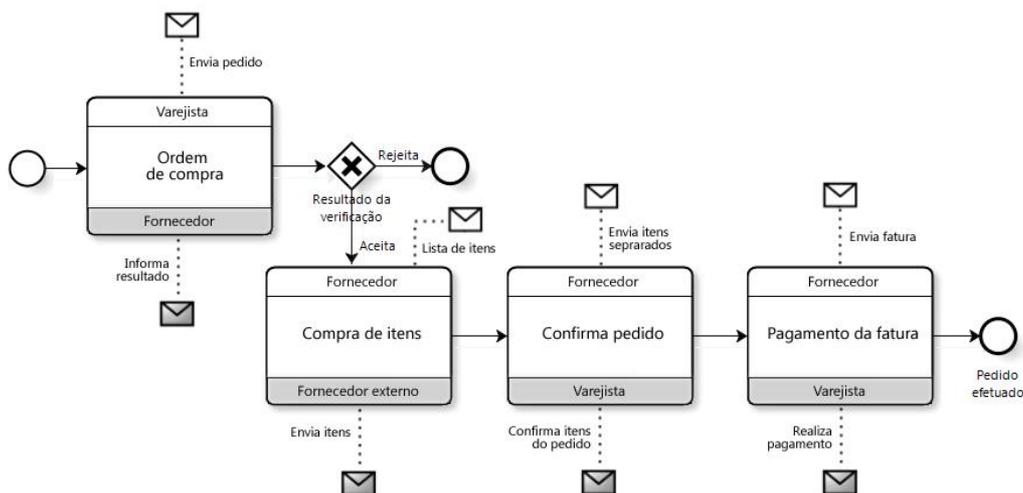
QUESTÃO 67



De acordo com a BPMN, o símbolo precedente descreve

- Ⓐ uma mudança de estado do participante A e do participante B.
- Ⓑ uma tarefa de execução de *scripts* entre dois participantes.
- Ⓒ um repositório de dados de ambos os participantes.
- Ⓓ uma transação em que as atividades do participante A estão logicamente relacionadas com as atividades do participante B.
- Ⓔ uma tarefa de coreografia que representa uma interação entre dois participantes.

Comentário: Uma Tarefa de Coreografia representa uma interação (Troca de Mensagem) entre dois Participantes. A figura abaixo representa um diagrama de coreografia, nele observamos 4 tarefas de coreografia: Ordem de compra, Compra de itens, Confirma pedido, Pagamento da fatura.



Diagramas de coreografia podem ser vistos também como um contrato de negócio entre os participantes, onde o foco está na troca de informações (mensagens), implica no envio ou recebimento de algum tipo de documento, como é o caso do diagrama acima, onde o contrato de negócio está na forma de uma ordem de compra. Este diagrama representa o Processo de Ordem de Compra, o fluxo demonstra a comunicação entre os três participantes (Varejista, Fornecedor e Fornecedor Externo).

Resumindo, podemos dizer que Diagrama de Coreografia:

- Focaliza a forma como os participantes trocam mensagens, demonstrando a comunicação entre os eles;
- É a representação dos processos e suas interações;
- Demonstra o comportamento esperado entre os participantes;
- É o contrato de negócio de interação entre os participantes.

Gabarito: E

68. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: Banco de Dados

As funções de um sistema de gerenciamento de banco de dados (SGBD) incluem

A gerenciar o becape e a recuperação dos dados, bem como o escalonamento de processos no processador por meio do banco de dados.

B gerenciar o sistema de arquivos e a segurança do banco de dados.

C gerenciar a entrada e saída de dispositivos, linguagens de acesso ao banco de dados e interfaces de programação de aplicações.

D gerenciar a integridade de dados, o dicionário e o armazenamento de dados, bem como a memória do computador enquanto o SGBD estiver em execução.

E transformar e apresentar dados, controlar o acesso de multiusuário e prover interfaces de comunicação do banco de dados.

Comentário: Dentre as alternativas acima a única que apresentam funções exclusivas do SGBD é a alternativa E. As demais alternativas tratam de aspectos associados aos **sistemas operacionais**¹: A) escalonamento de processos, B) gerenciamento do sistema de arquivos, C) gerenciamento da entrada e saída, D) Gerenciamento de memória.

Um Sistema de Gerenciamento de Banco de Dados (SGBD) é um conjunto de componentes que dão **suporte à criação, utilização e à manutenção de bancos de dados**. Inicialmente, um SGBD proporcionava armazenamento e recuperação eficientes dos dados. Devido às exigências do mercado e à inovação dos produtos, os SGBDs evoluíram e hoje fornecem uma ampla gama de recursos para **a aquisição, armazenamento, disseminação, manutenção, recuperação e formatação de dados**.

Gabarito: E

69. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: Banco de Dados

No modelo relacional, a afirmação “Duas tuplas distintas, em qualquer estado da relação, não podem ter valores idênticos para os atributos na chave” é

¹ Sistema operacional (SO) é o conjunto de programas que gerenciam recursos, processadores, armazenamento, dispositivos de entrada e saída e dados da máquina e seus periféricos. O sistema faz a comunicação entre o hardware e os demais softwares, criando uma plataforma comum a todos os programas utilizados. São exemplos de SO: Dos, Unix, Linux, Mac OS, OS-2, Windows NT.



- A uma propriedade de chave do modelo.
- B falsa.
- C uma restrição de domínio do modelo.
- D uma propriedade exclusiva do modelo objeto-relacional.
- E uma condição que deverá estar explícita na representação dos atributos de uma tupla.

Comentário: A principais propriedades das chaves são unicidade e irredutibilidade. Vejamos as definições:

Unicidade: Nenhum valor válido de relação contém duas tuplas diferentes com o mesmo valor para os atributos chave.

Irredutibilidade: Nenhum subconjunto apropriado da chave tem a propriedade de unicidade.

Veja que questão trata de unicidade, logo **uma propriedade de chave do modelo**.

Gabarito: A

70. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: Banco de dados

No modelo relacional, variável corresponde a

- A um valor variável que não possui local no tempo nem no espaço.
- B uma matriz de valores codificados e armazenados na memória.
- C um recipiente para se armazenar um valor que pode ser atualizado.
- D um valor que não admite substituição.
- E uma constante individual.

Comentário: Veja que essa questão foi totalmente inspirada no livro do CJ Date – Introdução a Sistemas de Banco de Dados.

“A primeira coisa que precisamos fazer é identificar a diferença lógica crucial e fundamental entre **valores** e **variáveis** (há uma confusão surpreendente sobre essa questão na literatura) ... adotamos as seguintes definições:

Um **valor** é uma “constante individual” – por exemplo, a constante individual que é o inteiro 3. Um valor **não possui local no tempo ou no espaço**. Contudo, os valores podem ser representados na memória por meio de alguma codificação, e tais representações, ou (nosso termo preferido) aparições, possuem locais no tempo e no espaço. Na realidade, aparições distintas do mesmo valor podem existir em vários locais distintos no tempo e no espaço, significando, informalmente, que diversas variáveis diferentes podem ter o mesmo valor, ao mesmo observe que, por definição, um valor não pode ser atualizado ; se pudesse, então, depois dessa atualização, ele não seria mais esse valor.

Uma **variável** é um recipiente para um aparecimento de um valor. Uma variável **possui um local no tempo e no espaço**. Além disso, logicamente, as variáveis, diferente dos valores,



podem ser atualizadas; ou seja, o valor atual da variável em questão pode ser substituído por outro valor, provavelmente, diferente do anterior. “

Assim, temos nossa resposta na alternativa C.

Gabarito: C.

71. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: Banco de Dados

Uma das regras de Codd para o modelo relacional consiste

A na dependência de dados físicos (mudança na memória e no método de acesso).

B na independência de distribuição.

C na presença de uma linguagem de programação no SGBD que promova interface com o banco de dados, com a segurança e com a atualização dos dados.

D na subversão das regras de integridade ou restrições quando utilizada uma linguagem de baixo nível.

E no não tratamento das atualizações de visões de dados.

Comentário: A alternativa B refere-se a 11ª regra de Codd:

Regra 11: Independência de Distribuição: A Distribuição de partes do SGBD em várias localidades deve ser transparente para os usuários do mesmo. Aplicações existentes necessitam continuar a operar com sucesso:

- quando uma versão distribuída do SGBD é introduzida pela primeira vez, e
- quando dados distribuídos existentes são redistribuídos em outras localidades físicas.

Gabarito: B

72. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: Modelagem dimensional

QUESTÃO 72

Com relação aos modelos de dados multidimensionais, assinale a opção correta.

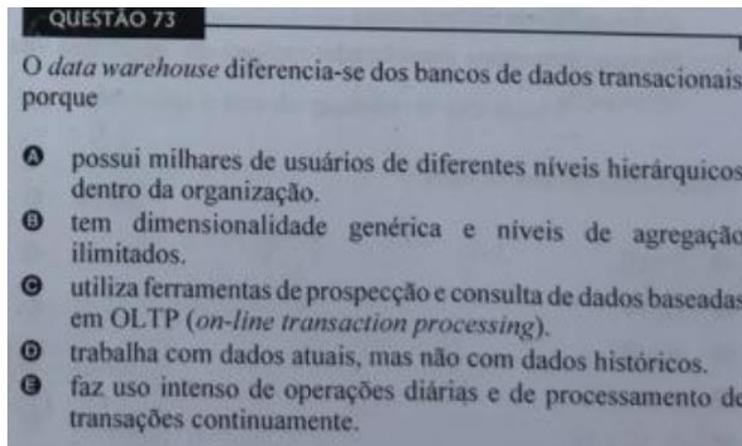
- A** Esses modelos não utilizam processos de transferência de dados, mas sim acessos nativos do próprio SGBD utilizado.
- B** A principal característica da tabela de fatos é a ausência de dados redundantes, o que melhora o desempenho nas consultas.
- C** Esses modelos são cubos de dados, sendo cada cubo representado por uma única tupla com vários atributos.
- D** Esses modelos proporcionam visões hierárquicas, ou seja, exibição *roll-up* ou *drill-down*.
- E** Os modelos de dados multidimensionais dão ênfase à coleta e às transações de dados.

Comentário: Sobre drill-down e roll-up são operações para movimentar a visão dos dados ao longo dos níveis hierárquicos de uma dimensão. A operação de drill-down o usuário navega de um nível mais alto de detalhe até um nível mais baixo (diminui-se a granularidade). Já a

operação de roll-up o usuário navega de um nível mais baixo de detalhe até o nível mais alto (aumenta-se a granularidade). Logo, temos a nossa resposta na alternativa E.

Gabarito: D

73. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: OLAP/Data Warehouse



Comentário: Observem a lista das 12 regras de Codd para avaliação de ferramentas de OLAP:

1. Visão conceitual multidimensional
2. Transparência
3. Acessibilidade
4. Desempenho de Informações consistentes
5. Arquitetura Cliente Servidor
6. **Dimensionalidade genérica**
7. Manipulação de dados dinâmicos
8. Suporte a multiusuários
9. Operações ilimitadas em dimensões cruzadas
10. Manipulação intuitiva de dados
11. Flexibilidade nas consultas
12. **Níveis de dimensão e agregação ilimitados**

Logo, podemos marcar nossa resposta na alternativa

Gabarito: B



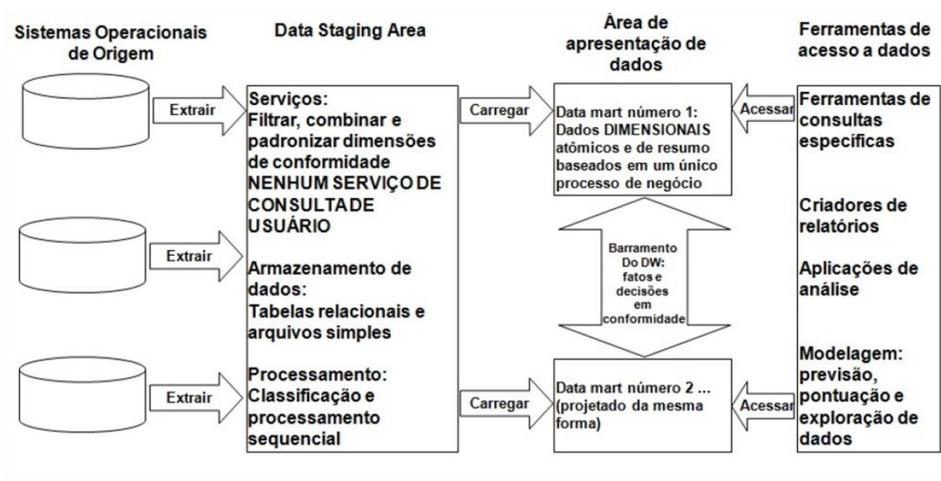
74. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: Business Intelligence

QUESTÃO 74

A respeito do BI (*business intelligence*), assinale a opção correta.

- Ⓐ O BI consiste na transformação metódica e consciente das informações exclusivamente prestadas pelos tomadores de decisão em novas formas de conhecimento, para evolução dos negócios e dos resultados organizacionais.
- Ⓑ ETL é o processo de análise de dados previsto pela arquitetura de BI.
- Ⓒ As técnicas do BI objetivam definir regras para a formatação adequada dos dados, com vista a sua transformação em depósitos estruturados de informações, sem considerar a sua origem.
- Ⓓ O repositório de dados analíticos de BI é representado pelas diversas bases de dados relacionais e por repositórios de dados que utilizem modelagens relacionais.
- Ⓔ A camada de apresentação de uma arquitetura de BI é aquela em que as informações são organizadas e centralizadas.

Comentário: Na figura abaixo observamos um fluxo dos dados entre os elementos de Business Intelligence. Perceba que a **apresentação dos dados** é o local onde os dados ficam organizados, armazenados e tornam-se disponíveis para serem consultados diretamente pelos usuários, por criadores de relatórios e por outras aplicações de análise. Kimball se refere à área de apresentação como uma série de data marts integrados. Um **Data Mart** é uma parte do todo que compõe a área de apresentação.



A banca, entretanto, apresentou a alternativa C como resposta correta. Porém eu faço algumas ressalvas a essa resposta. Depois que os dados são extraídos para o sistema ETL, há inúmeras transformações potenciais, como limpar os dados (corrigir erros de ortografia, resolver



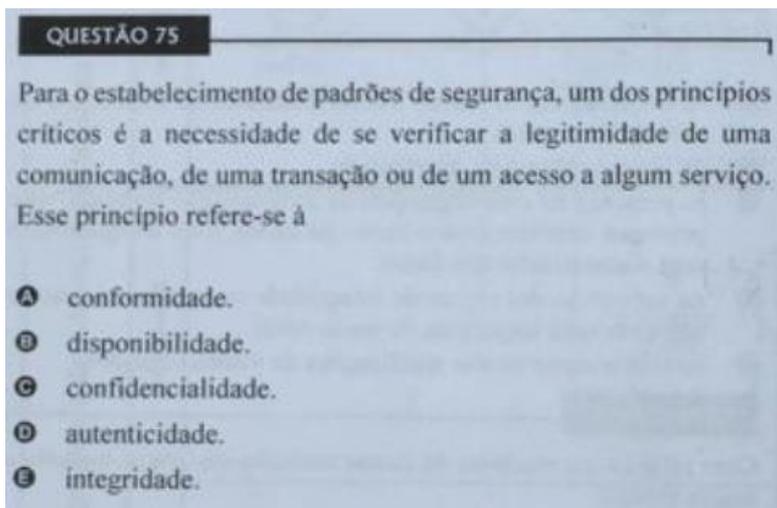
conflitos de domínio, lidar com elementos ausentes ou analisar em formatos padrão), **combinar dados de várias origens** e duplicar dados. O sistema ETL **agrega valor aos dados** com essas tarefas de limpeza e conformidade, **alterando os dados e aprimorando-os**. Além disso, essas atividades podem ser organizadas para criar metadados de diagnóstico, eventualmente levando à reengenharia de processos de negócios **para melhorar a qualidade dos dados nos sistemas de origem ao longo do tempo**. Veja que as regra de transformação se preocupam com os sistemas de origem.

Vamos agora traçar uma linha de argumentação sobre a resposta apresentada na alternativa E. O Kimball², um dos autores mais renomados no assunto de data warehouse define no seu livro uma arquitetura de DW/BI. Nesta arquitetura a **área ou camada de apresentação do DW/BI** é onde os dados são **organizados, armazenados e disponibilizados** para consultas diretas por usuários, redatores de relatórios e outros aplicativos analíticos de BI. Os dados na área de apresentação do sistema DW/BI devem ser dimensionais, atômicos (complementados por agregados que melhoram o desempenho), centrados em processos de negócios e aderir à arquitetura de barramento de data warehouse empresarial. Veja que a camada de apresentação do Kimball centraliza a informação para as consultas feitas por ferramentas de acesso aos dados.

Logo, embora a questão tenha seu referencial teórico em outro autor, existe claramente na literatura uma divergência ou incompatibilidade de nomenclatura. Sem a citação explícita da fonte não seria possível avaliar de forma consistente as alternativas. Logo, acredito que temos espaço para anulação da questão ou mudança de gabarito de C para E.

Gabarito: C/E (cabe recurso)

75. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: ITIL



Comentário: Na figura abaixo observamos um mapa mental com os princípios de segurança da informação:

² The Data Warehouse Toolkit: The Definitive Guide to Dimensional Modeling, 3rd Edition by Ralph Kimball; Margy Ross



Pela descrição observada para cada um dos princípios, aquele que se adequa corretamente à resposta é a **autenticidade**.

Gabarito: D

76. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: Segurança da informação

QUESTÃO 76

Julgue os itens a seguir, acerca de segurança da informação.

- I São exemplos de ameaças as contas sem senhas ou configurações erradas em serviços DNS, FTP e SMTP.
- II Não repúdio indica que o remetente de uma mensagem não deve ser capaz de negar que enviou a mensagem.
- III Vulnerabilidade é a fragilidade de um ativo ou de um grupo de ativos que pode ser explorada.
- IV Pessoas não são consideradas ativos de segurança da informação.

Estão certos apenas os itens

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

Comentário: Vejamos cada um dos itens que devem ser analisados:

- I. **Errada.** Neste item ele descreve vulnerabilidades e associa ao termo ameaças. Sabemos que ameaças se aproveitam das vulnerabilidades para remover, desabilitar ou destruir um recurso. Normalmente aproveitam falhas de segurança da organização.
- II. Alternativa correta! Apresenta o conceito de não repúdio ou irretratabilidade.
- III. Alternativa correta! Apresenta o conceito de vulnerabilidade.
- IV. **Errada.** Pessoas são ativos de segurança da informação.

Como II e III estão corretas, temos nossa resposta na alternativa C.

Gabarito: C

77. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: Plano de Continuidade de Negócios

QUESTÃO 77

Acerca do plano de continuidade de negócios (PCN), assinale a opção correta.

- A Os prazos decorrentes de ações realizadas por agentes externos à organização não necessitam ser considerados para elaboração do PCN dessa organização.
- B Na perspectiva do PCN, o funcionamento de uma empresa deve-se, fundamentalmente, às variáveis recursos e pessoas.
- C O PCN estabelece controles de segurança da informação como resultado de uma ampla análise de riscos.
- D Para operacionalizar o PCN de uma empresa que já foi elaborado, é altamente recomendável o desenvolvimento de um sistema de gestão de continuidade de negócios (SGCN).
- E PCN e plano de contingência são sinônimos, uma vez que contemplam os mesmos itens.



Comentário: Vamos comentar cada uma das alternativas acima:

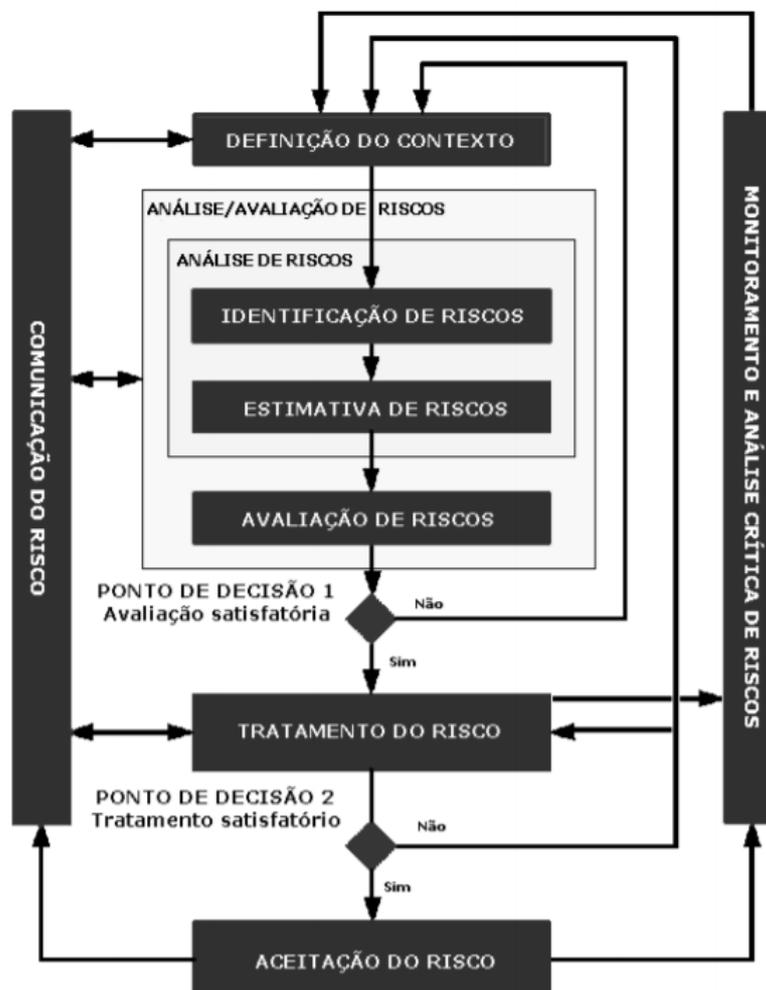
A – **Errada.** O prazo dos agentes externos impacta o PCN e devem ser conhecidos.

B – **Errada.** Sob o ponto de vista do PCN, o funcionamento de uma empresa deve-se a duas variáveis:

Processos: as atividades realizadas para operar os negócios da empresa;

Componentes: todas as variáveis utilizadas para realização dos processos: energia, telecomunicações, informática, infraestrutura, pessoas. Todas elas podem ser substituídas ou restauradas, de acordo com suas características.

C – **Errada.** (Gabarito Preliminar) A análise de riscos é definida como o uso sistemático de informações para identificar fontes e estimar o risco. Logo, seu resultado não é o estabelecimento de controles de segurança da informação como sugere questão. Veja a figura abaixo que estabelece uma visão geral do processo de gestão de riscos segundo a norma ISO 27005.



Agora se voltarmos nossa atenção para a norma 22301 que trata de plano de continuidade de negócio temos que a **avaliação (assessment) de risco** que definido como o processo global de

identificação, análise e avaliação (*evaluation*) do risco. Veja que própria norma também diferencia análise de avaliação de riscos. E a alternativa fala explicitamente de análise de riscos.

D – **Correta.** Um sistema de gestão de continuidade de negócios (SGCN) enfatiza a importância de: compreender as necessidades da organização e a necessidade de estabelecer uma política e objetivos de continuidade de negócios; implementar e operar controles e medidas para a gestão da capacidade geral de uma organização para gerenciar incidentes de interrupção; monitorar e analisar criticamente o desempenho e a eficácia do SGCN e melhorar continuamente, com base em medições objetivas.

Complementado a análise acima com o conteúdo da norma 22301, temos que:

PCN - procedimentos documentados que orientam as organizações a responder, recuperar, retomar e restaurar um nível de operação predefinido após a interrupção.

SGCN - parte do sistema geral de gestão que estabelece, implementa, opera, monitora, revisa, mantém e melhora a continuidade dos negócios. A norma sugere que a organização deve estabelecer, implementar, manter e melhorar continuamente um SGCN, incluindo os processos necessários e suas interações.

Assim, acho que a questão é passível de recurso, pela modificação do gabarito de C para D.

E – **Errada.** O plano de contingência é parte do PCN.

Gabarito: C/D (cabe recurso).

78. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: Criptografia

QUESTÃO 78

A respeito dos métodos de criptografia, assinale a opção correta.

- A Na utilização de chaves públicas, a chave é dividida em duas partes complementares, uma das quais é secreta, eliminando-se, dessa forma, o processo de geração e distribuição de chaves de cifração.
- B A cifração é suficiente para garantir a integridade dos dados que são transmitidos, por isso é dispensável o uso de chaves de autenticação e de assinaturas digitais.
- C Independentemente da técnica de criptografia empregada, a transmissão das chaves de cifração do emissor para o receptor é desnecessária.
- D Esses métodos classificam-se em cifração e decifração de chaves.
- E Na criptografia simétrica, as chaves utilizadas para criptografar uma mensagem possuem o mesmo tamanho, todavia são diferentes na origem e no destino.

Comentário: Primeira coisa importante, o CESPE considera que criptografia garante integridade e confidencialidade. Se você usa criptografia para garantir a integridade você pode dispensar outros mecanismos como chave de autenticação e assinatura digitais. Se mantiver o histórico, alinhado com alguns autores renomados a literatura de segurança da informação a resposta está na alternativa B.



Contudo, o CESPE designou como resposta da questão a alternativa A. Essa alternativa vai de encontro aos conceitos descritos no livro do Stallings³: “Há um sentimento de que a **distribuição de chave** é trivial quando se usa criptografia de chave pública, em comparação com distribuição de chave usados para a criptografia simétrica. Para a distribuição de chave usando criptografia de chave pública, é necessário alguma forma de protocolo, que frequentemente envolve um agente central, e os procedimentos envolvidos não são mais simples nem de qualquer modo mais eficientes do que os exigidos pela criptografia simétrica.” Ou seja, a distribuição da chave continua existindo. Logo, a alternativa está **incorreta, pelo menos segundo o Stallings**.

Ainda segundo Stallings, Criptografia pode ser definida da seguinte forma: “princípios, meios e métodos de disfarçar informações para garantir sua **integridade**, confidencialidade e autenticidade.” Veja que a integridade faz parte da criptografia ou cifragem. Sendo assim, acredito que seja viável a mudança de gabarito de A para B. Ou, em última instância, é possível solicitar a anulação da questão.

Gabarito: A/B. (cabe recurso)

79. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: Certificação Digital

QUESTÃO 79

Acerca de certificação digital, assinale a opção correta.

- A. Certificado digital comprado não pode ser revogado.
- B. É função da autoridade certificadora identificar e cadastrar usuários presencialmente e, depois, encaminhar as solicitações de certificados, mantendo registros das operações.
- C. No Brasil, adota-se o modelo de certificação hierárquica com várias raízes; SERPRO, SERASA e CERTISIGN são exemplos de autoridades certificadoras raiz que credenciam os participantes e auditam os processos.
- D. A utilização do certificado digital em documentos ainda não dispensa a apresentação física destes documentos no formato impresso em órgãos públicos.
- E. Normalmente, cada certificado inclui a chave pública referente à chave privada de posse da entidade especificada no certificado.

Comentário: Vamos comentar as alternativas:

- A.** Errada. Os certificados podem ser revogados, para isso existe a LCR -Lista de Certificados Revogados.
- B.** Errada. A Autoridade de Registro que é responsável pela interface entre o usuário e a Autoridade Certificadora – AC. Vinculada a uma AC, tem por objetivo **o recebimento, a validação, o encaminhamento de solicitações de emissão ou revogação de certificados digitais e identificação, de forma presencial, de seus solicitantes.** É responsabilidade da AR

³ **Segurança de Computadores, Princípios e Práticas** – Lawrie Brown, William Stallings, Tradução da 2ª edição.



manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota.

- C. Errada. A autoridade certificadora raiz é o ITI – Instituto Nacional de Tecnologia da Informação. Já as entidades listadas na questão (SERPRO, Certising e SERASA) são autoridades certificadoras de primeiro nível.
- D. Errada. Um exemplo de entrega digital de documento é o imposto de renda onde é dispensada a entrega do documento original.
- E. Correta. A figura abaixo apresenta a estrutura de um certificado digital. Nele podemos observar a presença da chave pública do dono do certificado. Uma Autoridade Certificadora é responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Tem a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves (pública/privada).



Gabarito: E

80. Ano: 2019 Banca: CESPE Órgão: SEFAZ-RS Prova: Auditor Assunto: Auditoria

QUESTÃO 80

A evidência verificável de que determinado programa de auditoria existe consiste na geração e na manutenção de registros, cujas principais categorias são

- A a documentação ostensiva e a sigilosa.
- B a documentação interna e a externa.
- C o gênero, a espécie, a tipologia e a natureza do assunto.
- D as auditorias internas e as externas.
- E a auditoria, a análise crítica do programa e a equipe de auditoria.

Comentário: Evidências de auditoria são registros, apresentação de fatos ou outras informações, pertinentes aos critérios de auditoria. A auditoria pode ser quantitativa ou qualitativa. Vamos comentar cada uma das alternativas:

- A. Errada. Há de se destacar, entretanto, que as informações públicas podem ser ostensivas, sigilosas ou pessoais.
- B. Errada. Não faz sentido falar em documentação interna e externa.
- C. **Certa.** (Considerações no final do comentário). Os **documentos de arquivo ou registros de auditoria** podem ser classificados em diferentes categorias, de acordo com suas características. Baseando-se nelas, podemos classificá-los quanto ao: **gênero, espécie, tipologia, natureza do assunto**, forma e formato.
- D. Errada. A classificação **quanto ao órgão fiscalizador/posicionamento** do auditor destaca 2 tipos de auditoria aplicados, em sua maioria, nas organizações, independente da área de atuação ou forma de abordagem. Essa terminologia é utilizada pela grande maioria dos auditores para classificar um processo de auditoria em auditorias internas e externas.
- E. ~~Errada.~~ **Certa.** Gabarito oficial preliminar. ~~Essa lista não tem relação nenhuma com o solicitado no enunciado.~~ Retiro o que eu disse! 😞 Temos que assumir nossos erros! De acordo com a ISSO 19011:

“5.5 Registros do programa de auditoria

Convém que sejam mantidos registros para demonstrar a implementação do programa de auditoria e convém que incluam o seguinte:

- a) registros relativos a **auditorias individuais**, tais como - planos de auditoria, - relatórios de auditoria, - relatórios de não-conformidade, - relatórios de ação corretiva e preventiva, e - relatórios de ações de acompanhamento de auditoria, se aplicável.
- b) resultados de **análise crítica do programa** de auditoria;
- c) registros relativos a **pessoal de auditoria**, incluindo assuntos tais como:



- **Competência do auditor e avaliação de desempenho,**
- **Seleção da equipe de auditoria, e**
- **Manutenção e aperfeiçoamento da competência.**

Convém que os registros sejam mantidos e salvaguardados adequadamente.”

Curiosamente o mesmo texto em inglês da norma 19011 publicada em 2018 apresenta uma abordagem um pouco diferente. Vejamos:

5.4.7 Managing and maintaining **audit programme records**

The person managing the audit programme should ensure that audit records are created, managed and maintained to demonstrate the implementation of the audit programme. Processes should be established to ensure that any confidentiality needs associated with the audit records are addressed. Records should include the following:

a) records related to the **audit programme**, such as:

- documented audit programme objectives and extent;
- those addressing audit programme risks;
- reviews of the audit programme effectiveness;

b) records related to **each individual audit**, such as: (letra “a” acima)

- audit plans and audit reports;
- nonconformity reports;
- corrective and preventive action reports;
- audit follow-up reports, if applicable;

c) records related to **audit personnel** covering topics such as: (letra “c” acima)

- competence and performance evaluation of the audit team members;
- selection of audit teams and team members;
- maintenance and improvement of competence.”

Segundo a própria norma:

3.1 **auditoria** - processo sistemático, documentado e independente para obter evidências de auditoria (3.3) e avaliá-las objetivamente para determinar a extensão na qual os critérios da auditoria (3.2) são atendidos.

3.11 **programa de auditoria** conjunto de uma ou mais auditorias (3.1) planejado para um período de tempo específico e direcionado a um propósito específico.

Essa questão para mim é uma das mais polêmicas da prova inteira. Primeiramente, porque o assunto “Auditoria, vulnerabilidade e conformidade” está dentro do escopo de segurança



da informação. A questão da prova cobrou uma descrição presente na ISO 19011⁴ que fornece diretrizes para usuários em todos os níveis de organizações, seja pequena, média ou grande, que venha a realizar auditorias de primeira, segunda ou terceira parte para sistemas de gestão. Além das diretrizes para auditoria, a ISO 19011 também estabelece requisitos para a competência e a avaliação de um auditor e de uma equipe auditora. Ou seja, não faz parte do conteúdo presente no edital.

Outro erro da questão é listar, na alternativa C, uma lista genérica de classificação de documentos e registros. Essa é uma classificação ampla, usada por várias áreas do conhecimento que trabalham com documentação e registros. Sendo assim, nada nos impede de afirmar que é uma lista de categorias de registros.

Sobre a alternativa dada como resposta correta, se formos analisar o texto da norma original em inglês, a primeira categoria refere-se ao programa de auditoria e não à auditoria de per si. As definições, retiradas da própria norma são apresentadas acima. Sendo assim, acho que há subsídio suficiente para solicitar a anulação da questão.

Gabarito: E (Cabe recurso)

⁴ <https://pauleyatman.net/wp-content/uploads/2016/09/ISO-19011-2011-Guidelines-for-auditing-management-systems.pdf>

