-- CONHECIMENTOS ESPECÍFICOS --

Julgue os itens a seguir, acerca de gerenciamento de projetos conforme o PMBOK 7.ª edição.

51 Em gerenciamento de projetos, método é qualquer modelo, documento, saída ou entrega de projeto.

52 *Tailoring* corresponde a adaptar os processos, a governança e a abordagem do gerenciamento de projetos visando-se à sua adequação ao contexto e à natureza do trabalho a ser realizado.

53 Considerando-se os componentes de um sistema de entrega de valor, os resultados de projetos consistem nos benefícios que são percebidos pela organização como ganhos.

54 Supervisão, controle e avaliação de valor são os componentes do sistema de entrega de valor.

55 Um escritório de gerenciamento de projetos deve promover entrega e capacidade orientadas a resultados, além de manter a perspectiva da visão real e o aprimoramento contínuo.

56 Em organizações formadas por diversos departamentos com vários projetos que entregam resultados estrategicamente importantes, recomenda-se o tipo de escritório de gerenciamento de projetos em nível empresarial.

57 Um escritório de gerenciamento de projetos deve restringir-se ao fornecimento de diretrizes, modelos e exemplos de boas práticas, com treinamento e orientação para as equipes de projetos.

58 Domínio de desempenho é um conjunto de atividades críticas e inter-relacionadas voltadas para a entrega eficaz dos produtos de um projeto.

Em relação à gestão de riscos, julgue os itens subsequentes.

59 A eliminação das ameaças é uma das formas de gerenciar os riscos.

60 O processo de avaliação de riscos é composto pelas atividades de identificação, tratamento e eliminação dos riscos.

61 A gestão de riscos compreende um conjunto de atividades coordenadas para reduzir as incertezas no alcance dos objetivos.

De acordo com o PMBOK 7.ª edição, julgue os itens que se seguem.

62 EAP é uma decomposição hierárquica do escopo total do trabalho da equipe de execução, necessária para alcançar os objetivos e entregar os produtos do projeto.

63 A equipe de gerenciamento de projetos é aquela formada por um grupo de indivíduos que executa o trabalho do projeto para alcançar os seus objetivos.

64 Os grupos de processos são fases do gerenciamento do projeto e devem ser realizados conforme a seguinte sequência: iniciação, planejamento, execução, monitoramento e encerramento.

Julgue os próximos itens, considerando a ITIL v4.

65 De acordo com a prática de gerenciamento de nível de serviço, o acordo de nível de serviço (SLA) deve ser alinhado e definido junto com o cliente final, assim como se deve definir a utilidade de um serviço, ou seja, o desempenho do serviço e o que determina se ele está adequado ou não para uso.

66 O escopo da prática de gerenciamento de incidentes inclui tanto a detecção e o registro de incidentes quanto seu diagnóstico e sua investigação, excluída, nesse caso, a revisão de incidentes, que fica a cargo da prática de gestão de problemas.

67 Os sistemas operacionais, aplicativos de *desktop* e *middleware* incluem-se no escopo da prática de infraestrutura e plataforma.

68 Não há prática na ITIL v4 diretamente afeta ao gerenciamento de segurança da informação, sendo a confidencialidade, a integridade e a disponibilidade tratadas como incidentes ou problemas quando concernentes à segurança de dados nos serviços.

69 A ITIL v4 prevê prática diretamente relacionada à gestão de projetos, incluindo tarefas como planejamento e monitoramento do projeto, com vistas a garantir que todos os projetos sejam entregues com sucesso.

Julgue os itens a seguir, referentes à ITIL v4 e ao COBIT 2019.

70 O COBIT 2019 prevê processo afeto diretamente à gestão de fornecedores, denominado terceiros gerenciados, ao passo que na ITIL v4 não há prática de gerenciamento de fornecedores, pois o prestador de serviço é gerenciado com base na prática gerenciamento de nível de serviço, na qualidade de *stakeholder* externo.

71 Tanto na ITIL v4 quanto no COBIT 2019, é prevista gestão relativa a problemas: na ITIL, a prática gerenciamento de problemas visa reduzir a probabilidade e o impacto dos incidentes, inclusive identificando as causas reais; no COBIT, o processo problemas gerenciados inclui fornecer resolução para evitar incidentes recorrentes.

72 Tanto na ITIL v4 quanto no COBIT 2019, é prevista gestão afeta ao conhecimento: na ITIL, a prática gestão do conhecimento visa manter e melhorar o uso eficaz do conhecimento em toda a organização; no COBIT, o processo conhecimento gerenciado inclui manter a disponibilidade de informações relevantes sobre conhecimento, para facilitar a tomada de decisões relacionadas à governança.

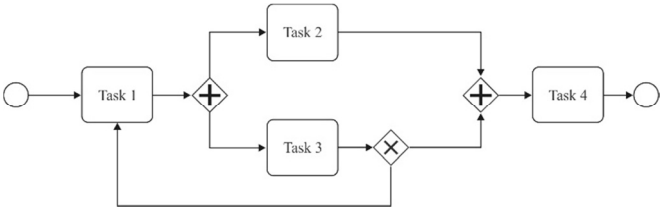
Julgue os itens que se seguem, relativos ao COBIT 2019.

73 Aspectos concernentes à entrega operacional e ao suporte de serviços de tecnologia da informação, incluída a segurança, são mais afetos ao domínio entrega, serviço e suporte (DSS) do que ao domínio alinhar, planejar e organizar (APO).

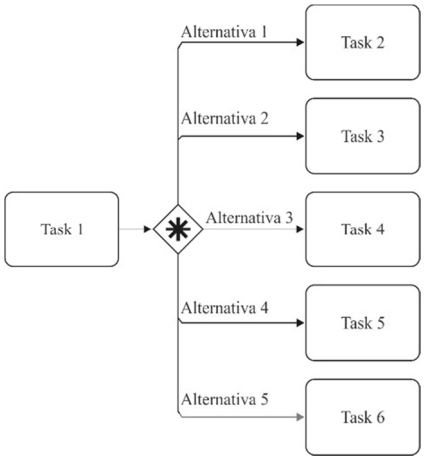
74 O COBIT 2019 é uma estrutura para organizar processos de negócios e estabelece uma distinção clara entre governança e gerenciamento.

Em relação a BPMN, julgue os itens subsequentes.

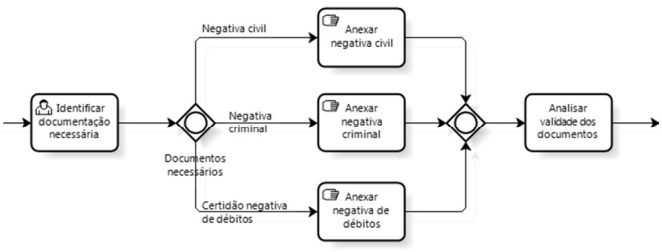
75 Com base no fluxo ilustrado a seguir, conclui-se que, após a execução da `Task 1`, será executada a `Task 2` ou a `Task 3`, mas nunca ambas em paralelo.



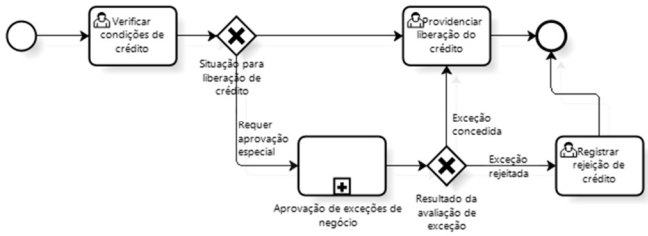
76 No fluxo representado a seguir, necessariamente as tarefas `Task 2`, `Task 3`, `Task 4`, `Task 5` e `Task 6` serão executadas em paralelo.



77 Conforme o fluxo ilustrado a seguir, necessariamente as tarefas `Anexar negativa civil`, `Anexar negativa criminal` e `Anexar negativa de débitos` devem ser concluídas para que seja executada a tarefa `Analisar validade dos documentos`.



78 No fluxo representado a seguir, `Aprovação de exceções de negócio` é um subprocesso, sendo possível realizar um detalhamento das atividades desse subprocesso com o objetivo de descrevê-lo de maneira mais minuciosa.



Em relação à gestão de segurança da informação, julgue os itens subsequentes.

79 De acordo com a NBR ISO/IEC 27001, quando uma não conformidade acontece, a organização deve, entre outras providências, avaliar a necessidade de realizar ações para a eliminação de sua causa, a fim de evitar que tal evento volte a acontecer.

80 Conforme a NBR ISO/IEC 27002, os requisitos legais, estatuários, regulamentares e contratuais constituem uma das principais fontes de requisitos de segurança da informação.

81 Segundo a NBR ISO/IEC 27001, um processo de avaliação de riscos de segurança da informação deve estabelecer e manter critérios de risco que incluam a eliminação e a avaliação dos riscos.

82 Nos controles organizacionais previstos na NBR ISO/IEC 27002, o inventário de informações e outros ativos associados abrangem as seguintes propriedades de segurança da informação: confidencialidade, integridade e disponibilidade.

A respeito da autenticação e proteção de sistemas, julgue os itens que se seguem.

83 O JSON Web Token consiste em três partes separadas por pontos: o cabeçalho, que contém informações sobre o tipo de *token* e o algoritmo de criptografia usado para assinar o *token*; o *payload*, que contém as informações do usuário; e a assinatura, usada para garantir que o *token* não tenha sido alterado.

84 O OpenID Connect é um protocolo de identidade simples, construído no protocolo do JSON Web Token, e permite que os aplicativos clientes confiem na autenticação executada por um provedor OpenID Connect para verificar a identidade de um usuário.

85 Na notificação por *push*, os métodos de autenticação de dois fatores (2FA) exigem uma senha para aprovar o acesso a um sítio ou aplicativo.

86 A biometria pode ser usada em conjunto com outros métodos de autenticação — principalmente senhas e PIN — como parte de uma configuração 2FA.

Em relação a ameaças e vulnerabilidades em aplicações, julgue os próximos itens.

87 O objetivo do ataque de LDAP *injection* é manipular as consultas LDAP, por meio da inserção de um código malicioso na consulta, que passa a ser interpretada de forma diferente do esperado.

88 XSS (*Cross-site scripting*) é um método pelo qual um invasor explora vulnerabilidades na maneira como um banco de dados executa consultas de pesquisa.

89 Um ataque de *cross-site request forgery* é aquele que induz um usuário a usar acidentalmente suas credenciais para invocar uma ação indesejada.

Acerca da segurança de aplicativos *web*, julgue os itens que se seguem.

90 Entre os riscos de segurança incluídos no relatório OWASP Top 10, a quebra de controle de acesso é um ataque contra um aplicativo *web* que analisa a entrada XML.

91 O uso de componentes com vulnerabilidades conhecidas é uma das categorias de riscos de segurança do OWASP Top 10 que resulta da desserialização de dados de fontes não confiáveis.

92 Quando um invasor encontra falhas em um mecanismo de autenticação, ele pode obter acesso às contas de outros usuários.

A respeito das características de um ataque de negação de serviço distribuído, julgue os próximos itens.

93 Um *firewall* de borda é considerado como o elemento capaz de fazer a mitigação de ataques DDoS de maneira eficiente, já que o tráfego da camada de aplicação tem que ser bloqueado na entrada da rede.

94 Em um ataque que envolve a amplificação de dados, o atacante gera uma mensagem para um elemento falho na rede e este, por sua vez, gera uma resposta que aumenta o volume de dados direcionados à vítima.

Julgue os itens a seguir, a respeito de estratégia de criptografia para dados em trânsito em uma rede de computadores.

95 O uso da última versão do TLS é recomendado para a criação de túneis de comunicação criptografados, considerando as versões de algoritmos simétricos e assimétricos seguros.

96 Como solução de verificação de integridade, o algoritmo MD5 seria uma boa escolha, já que ele é resistente a colisões e garante confidencialidade.

Acerca de assinatura e certificação digital, julgue os itens que se seguem.

97 No caso de um certificado digital com o algoritmo RSA, o tamanho adequado e seguro da chave é de 512 *bits*.

98 O algoritmo SHA512 é inseguro porque o ataque de repetição (*replay attack*) permite a colisão dos primeiros 64 *bits* de saída.

Com base na NBR ISO/IEC 27005, julgue os itens seguintes.

99 Na organização deve existir treinamento de gestores e de pessoal sobre riscos e ações de mitigação.

100 O processo de gestão de riscos deve contribuir para a identificação dos riscos de segurança da informação.

Conforme o que preconiza a LPGD para o encarregado de dados, julgue os itens subsequentes.

101 Cabe ao encarregado aceitar reclamações e comunicações dos titulares de dados.

102 A identidade e as informações de contato do encarregado de dados devem ser mantidas em sigilo, podendo ser publicadas mediante solicitação do interessado.

Julgue os itens a seguir, em relação ao processo de negociação de parâmetros criptográficos e múltiplas conexões conforme o protocolo TLS 1.3.

103 O TLS impede a abertura de múltiplas conexões HTTP paralelas.

104 O servidor processa a mensagem `ClientHello` enviada pelo cliente, entretanto, quem determina os parâmetros apropriados criptográficos para a conexão é o cliente.

A respeito do processo de gestão de riscos estabelecido pela NBR ISO/IEC 27005, julgue os seguintes itens.

105 O encerramento do processo de gestão de risco inclui decisões sobre a aceitação do risco e consequente comunicação às partes envolvidas.

106 Uma das etapas do processo de gestão de risco consiste em definir o contexto.

Em relação a ferramentas e técnicas de apoio ao gerenciamento de projetos, julgue os itens a seguir.

107 A matriz RACI é utilizada para apoiar a avaliação dos riscos que tenham impactos qualitativos no projeto, pois sua finalidade principal é manter o acompanhamento dos riscos do projeto.

108 Ao planejar um novo cronograma, caso adote o método de PERT (*program evaluation and review technique*), o gerente de projetos considerará várias incertezas e utilizará três diferentes estimativas de tempo: a otimista, a pessimista e a mais provável.

109 A técnica de valor agregado, conhecida também como EVM (*earned value management*), é um método cujo principal objetivo é mensurar a demanda de recursos humanos para o projeto.

110 O gráfico de Gantt é uma ferramenta visual que pode ser utilizada para demonstrar o cronograma de um projeto ao longo de determinado período de tempo.

111 Na fase de planejamento do projeto, pode ser utilizada a análise de SWOT, que permite identificar os pontos fortes e fracos para a entrega do projeto.

Acerca do ciclo de vida e da organização do projeto, julgue os itens seguintes.

112 As fases de um projeto são sequenciais e iterativas e devem ser controladas para que não aconteçam sobreposições.

113 Os níveis de custo e de mobilização de recursos são baixos no início do projeto e aumentam conforme o trabalho é executado.

114 Durante a fase de iniciação do projeto, a equipe deve desenvolver o plano de gerenciamento do projeto detalhado, incluindo cronograma com datas de cada entrega e orçamento, para que sirva de guia para as fases seguintes do projeto.

115 O plano de gerenciamento do escopo é o documento de entrada do processo em que se faz o controle do escopo do projeto, o qual integra a fase de encerramento do projeto.

116 O ciclo de vida do projeto pode ser influenciado por aspectos exclusivos da organização, do setor, do método de desenvolvimento ou da tecnologia utilizada.

117 Em uma estrutura genérica do ciclo de vida de um projeto, o risco é menor no início do projeto e aumenta gradativamente ao longo do tempo de desenvolvimento do projeto.

A respeito de processos de gerenciamento de projetos, julgue os itens subsecutivos.

118 As folhas de verificação, também são conhecidas como folhas de resultados, organizam fatos para a coleta de dados úteis ao processo de controlar a qualidade.

119 O registro de lições aprendidas inclui-se entre as ferramentas e técnicas do processo de validar o escopo.

120 O processo de planejar o gerenciamento dos recursos humanos tem como uma de suas saídas o termo de nomeação da equipe.

Espaço livre