-- CONHECIMENTOS ESPECÍFICOS --

A respeito de governança de TI, julgue os próximos itens.

51 No STJ, as linhas estratégicas de atuação antes previstas no Plano Estratégico de TIC deverão ser contempladas no Plano Diretor de TIC (PDTIC), com o objetivo de manter a continuidade do trabalho e o alinhamento da estratégia.

52 No COBIT 2019, o princípio Aplicar modelo único integrado estabelece que os componentes como processos, estruturas, arquiteturas e pessoas devem funcionar em conjunto para a construção de um sistema de governança eficiente.

53 O gerenciamento da demanda, da relação comercial e do portfólio de serviços são processos do ITIL v4 englobados pelo estágio Estratégia de serviços do ciclo de vida de serviços.

54 De acordo com o princípio da conformidade, as aquisições de TI devem ser feitas por razões válidas e embasadas em análises apropriadas e contínuas, com equilíbrio entre benefícios, oportunidades, custos e riscos, de curto e longo prazos.

55 As práticas de gerenciamento de serviço do ITIL v4 incluem gerenciamento de infraestrutura e de plataforma.

Em relação ao gerenciamento de projetos e à modelagem de processos de negócio, julgue os itens que se seguem.

56 Cadeia de valor é a ferramenta utilizada para modelagem corporativa que demonstra, por meio de um fluxo simples e contínuo, os processos que contribuem com a produção de valor para os clientes de uma organização.

57 Processo primário é o tipo de processo de negócio que tem como propósito medir, monitorar, controlar e administrar o presente e o futuro do negócio.

58 Caso um projeto possua um escopo sujeito a mudanças durante a sua execução, é recomendável, segundo o PMBOK, que se utilize uma abordagem de desenvolvimento do tipo preditiva.

59 Conforme o PMBOK, existem várias formas de se medirem os custos de um projeto, entre as quais o índice de desempenho de custos (IDC) é a medida de custo em que se compara o custo real de mão de obra ou de recursos com o custo estimado, sendo tal medida também conhecida como *burn rate*.

60 Segundo o PMBOK, a comunicação passiva, elemento fundamental para o engajamento das partes interessadas, é o tipo de comunicação que pode ocorrer por meio da busca por políticas ou modelos de comunicação e pesquisas em repositórios *online*, a fim de se detectarem indiretamente as preocupações dessas partes interessadas quanto ao projeto.

Com base nas Resoluções CNJ n.º 522/2023 e n.º 335/2020, relativas à Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br), julgue os itens subsequentes.

61 Entre os objetivos da PDPJ-Br está o de implantar o conceito de desenvolvimento centralizado, devendo todos os tribunais contribuir com as melhores soluções tecnológicas para aproveitamento comum.

62 Na especificação e no desenvolvimento de funcionalidade em que se identifique conflito entre requisitos, devem ser aplicados os requisitos não funcionais relacionados à segurança em detrimento de outros.

Julgue os itens seguintes de acordo com o disposto nas Portarias CNJ n.º 252/2020 e n.º 253/2020.

63 Os serviços estruturantes relacionam-se às funcionalidades essenciais básicas para um sistema de processo judicial de tramitação eletrônica, bem como àqueles serviços necessários à integração, à coreografia e à interoperabilidade entre os serviços e as soluções que compõem a PDPJ-Br.

64 O Comitê Gestor Nacional da PDPJ-Br é o responsável pela coordenação da rede de governança da plataforma.

À luz da Portaria CNJ n.º 131/2021 e da Resolução CNJ n.º 396/2021, julgue os itens que se seguem.

65 Cada tribunal, com exceção do Supremo Tribunal Federal, deve estabelecer em sua política de segurança da informação ações para realizar a gestão dos ativos de informação e da política de controle de acesso a sistemas informacionais.

66 O `merge request` será aceito se pelo menos dois tribunais, distintos daquele que houver desenvolvido a funcionalidade ou solução, aprovarem-no.

Em consonância com a Portaria CNJ n.º 162/2021, julgue os itens seguintes, relativos à Estratégia Nacional de Segurança Cibernética do Poder Judiciário.

67 O ato de desinstalar ou desabilitar *plug-ins* ou aplicações *add-on* não autorizados para navegadores *web* e clientes de *email* é uma ação associada à função de controle de segurança relativa à detecção de ameaça, ataque ou irregularidade.

68 O gerenciamento de crises cibernéticas do Poder Judiciário encontra-se dividido em três fases: planejamento, execução e melhoria contínua.

69 As funções básicas do protocolo de prevenção de incidentes cibernéticos do Poder Judiciário restringem-se a identificar, proteger, detectar e responder aos ataques ou ameaças.

Com base na Resolução CNJ n.º 468/2022, julgue os itens subsecutivos, que versam sobre diretrizes para as contratações de solução de tecnologia da informação e comunicação (TIC) pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça.

70 A equipe de gestão de contrato é composta, em regra, pelo gestor do contrato, responsável por gerir a execução contratual, e pelos fiscais demandante, técnico e administrativo, responsáveis por fiscalizar a execução contratual.

71 É facultativa a execução da fase de planejamento da contratação de solução de TIC nos casos de inexigibilidade de licitação.

72 Durante a fase de seleção do fornecedor, a equipe de planejamento da contratação é responsável por apoiar o pregoeiro ou a comissão de licitação na análise e no julgamento das propostas e dos recursos apresentados pelas licitantes, bem como na condução de eventual prova de conceito.

Em relação à linguagem de programação Java, à arquitetura distribuída de microsserviços e à biblioteca Flyway, julgue os próximos itens.

73 MapStruct é um gerador de código que simplifica a implementação de mapeamentos entre tipos de *bean* Java.

74 A solução Flyway permite que seja realizado o controle de versão de código de banco de dados, estendendo o DevOps aos bancos de dados de modo a permitir que se acompanhem as alterações e se aprimore a confiabilidade das implantações de *software*.

75 Considere o seguinte código, escrito em Java.

```
class Main {
  public static void main(String[] args) {
    int x = 11, y = -7, z = 22;
    int resultado = (x >= y) ? ((x >= z) ? x :
z) : ((y >= z) ? y : z);
    System.out.println("Resultado: " +
resultado);
  }
}
```

A partir do código precedente, é correto afirmar que a execução desse código apresentará o seguinte resultado.

```
Resultado: 22
```

76 Zuul é uma solução que permite a realização de roteamento dinâmico e monitoramento, e seus filtros são capazes de atuar na segurança por meio da identificação de requisitos de autenticação para cada recurso e da rejeição de solicitações que não os satisfaçam.

77 Swagger é uma interface API compatível com Java que permite que dois sistemas computacionais troquem informações com ausência de estado.

Julgue os próximos itens, relativos a H2, Keycloak, Webhooks, Git, *continuous delivery* e *continuous integration*.

78 *Continuous delivery* (CD) e *continuous integration* (CI) são práticas afetas ao DevOps: a primeira realiza a implantação automática no repositório da solução após o *build*; e a segunda realiza implantação automática no ambiente de produção a cada *release*.

79 O comando Git a seguir, ao ser executado, copiará todo o conteúdo do repositório local para o repositório remoto *git*, e, por padrão, fará a mesclagem com a *branch master*.

```
git clone --bare -l /home/projetox/
.git/pub/projetox
```

80 O banco de dados H2 é uma solução de persistência de dados NoSQL do tipo chave-valor.

81 O Keycloak é considerado uma pilha de *software* completa cujo objetivo principal é gerenciar a segurança em contêineres à medida que ele administra a infraestrutura de *docker*.

82 Webhooks permitem conectar aplicativos e sistemas de modo que eles compartilhem dados em tempo real, por meio de funções de retorno de chamada baseadas em HTTP que viabilizam a comunicação orientada por eventos entre os sistemas.

Acerca de cabeamento estruturado, fibras ópticas, WLAN e *jumbo frames*, julgue os itens a seguir.

83 *Jumbo frames* é um recurso que permite aumentar o tamanho dos pacotes de dados, padrão MTU, de 1.500 *bytes* para até 9.000 *bytes*, diminuindo a sobrecarga de processamento nos dispositivos de rede.

84 Cabos de par trançados são compostos por 4 pares de fios de cobre trançados entre si; cada par de fios utiliza um padrão de entrançamento diferente, com um número diferente de tranças por metro.

85 Os cabos de categorias 5 e 5e suportam taxas de transmissão de 100 *megabits* e 1.000 *megabits* e frequência de até 100 MHz, para extensão de cabo limitada a 100 m de comprimento.

86 O padrão IEEE 802.11 (WLAN) possui o protocolo CSMA/CA no nível MAC, que faz a encriptação dos dados entre o cliente e o ponto de acesso.

87 As fibras ópticas multimodo apresentam núcleo cujo diâmetro mede de 8 a 10 mícrons, e podem interligar pontos distantes em até 80 km no padrão de 10 *gigabits*.

Julgue os próximos itens, relativos a roteadores, protocolos LDAP e IMAP, mecanismo NAT e conceitos de VLAN.

88 Uma VLAN é uma rede lógica que segmenta o fluxo de informações que trafegam por uma rede corporativa, gerando mais controle de tráfego e segurança.

89 Com o NAT dinâmico, o endereço da estação de todos os acessos à rede externa será substituído pelo endereço da interface pública do servidor ou roteador em que o NAT está habilitado.

90 O roteador faz a ligação entre LANs, atuando na camada 2 do modelo de referência TCP/IP, interpreta o endereço DNS contido nos pacotes de dados e faz o envio à porta específica.

91 O LDAP utiliza como mecanismo de segurança o protocolo TLS (*Transport Layer Security*), a fim de criptografar as mensagens entre o cliente e o servidor.

92 O IMAP utiliza o UDP na camada de transporte e escuta as requisições pela porta 143.

A respeito de VPN, anti-DDoS, Nagios e *Active Directory*, julgue os itens subsequentes.

93 O arquivo `edb.log` tem como função armazenar todo o banco de dados do *Active Directory*.

94 Em uma VPN, o tráfego de dados é levado pela rede pública por meio de protocolos de criptografia por tunelamento, como o SSL, que define um tipo de cabeçalho de autenticação (AH – *authentication header*), garantindo a confidencialidade dos dados.

95 Inundação SYN é um tipo de ataque distribuído de negação de serviço (DDoS) em que um grande número de solicitações HTTP inunda o servidor, resultando na interrupção do serviço.

96 A execução do comando a seguir permite verificar a integridade da configuração do Nagios no ambiente Linux.

```
# /usr/local/nagios/bin/nagios –v
/usr/local/nagios/etc/nagios.cfg
```

97 O SNMP utiliza, no nível de transporte, o UDP para fazer o gerenciamento de equipamentos, mas apresenta deficiências em relação à segurança e à transferência eficiente de grande quantidade de informação.

Em relação à segurança da informação, julgue os itens a seguir, de acordo com as normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2022.

98 Os controles são classificados em controle de pessoas, controle físico e controle tecnológico e, quando não enquadrados em nenhum desses, devem ser categorizados como organizacionais.

99 Os controles e objetivos de controle a serem implementados para mitigar os riscos devem ser adotados em alinhamento aos termos da subseção avaliação de riscos de segurança da informação.

100 Por meio da promoção de melhoria contínua, a alta direção de uma organização demonstra sua liderança e seu comprometimento em relação ao sistema de gestão de segurança da informação.

Julgue os itens seguintes, relativos à gestão de riscos e políticas de segurança da informação.

101 As políticas de segurança da informação dentro de uma organização podem ser apoiadas por políticas específicas por tema, as quais devem, por sua vez, ser alinhadas e complementares à política de segurança da informação da organização.

102 Na segurança da informação, a autenticidade é conceituada como a propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

A respeito de gerenciamento de incidentes de segurança da informação e gestão de continuidade de negócio (GCN), julgue os itens que se seguem.

103 A GCN, ao contrário da gestão de incidentes de segurança da informação, tem a finalidade de estabelecer procedimentos para identificar, gerenciar, registrar, analisar e comunicar eventos relativos às operações e aos impactos negativos causados às operações da organização.

104 A gestão de incidentes é considerada um componente crítico da estratégia de gerenciamento de riscos das organizações porque, com tal gestão, é possível reduzir o tempo de inatividade e minimizar os impactos negativos causados por acidentes cibernéticos.

Acerca do uso do *framework* de autenticação OAuth 2.0, julgue o item subsequente.

105 O OAuth 2.0 utiliza *refresh tokens* para obter novos *tokens* de acesso, sem pedir ao usuário para fazer *login* novamente, e serve de base para o OpenID Connect, que adiciona uma camada de autenticação sobre o protocolo de autorização.

No que se refere a ataques em redes de computadores e redes *wireless*, julgue os itens subsecutivos.

106 Nos ataques do tipo *access point spoofing*, os invasores circulam fisicamente por regiões onde desejam realizar os ataques e descobrem as redes que existem por ali, bem como os equipamentos físicos através dos quais poderão realizar as invasões posteriormente.

107 O ataque DoS se caracteriza por utilizar uma única fonte de conexões, enquanto um ataque DDoS utiliza várias fontes de tráfego de ataque, muitas vezes na forma de uma *botnet*.

Julgue os itens seguintes, relativos a ameaças, ataques e protocolos de segurança de *email*.

108 O método de autenticação SPF (*sender policy framework*) permite que os proprietários de domínios assinem *emails* automaticamente a partir de seu domínio; nessa assinatura digital, é utilizada criptografia de chave pública para verificar matematicamente que o *email* veio do domínio correto.

109 O *spear phishing* tem como alvo um grupo específico ou tipo de indivíduo, como os administradores de sistema de uma empresa; já o *whaling* é um tipo de *phishing* ainda mais direcionado e geralmente tem como alvo um CEO ou CFO de um setor ou negócio específico.

Acerca de ataques de *malware*, julgue os próximos itens.

110 Ataques do tipo APT (*advanced persistent threats*) usam uma abordagem ampla e são projetados sem um alvo específico, sendo iniciados para causar danos à rede da organização-alvo, com o objetivo de se obter entrada e saída rápidas.

111 *Leakware*/*doxware* é um tipo de *ransomware* em que se ameaça destruir os dados se o resgate não for pago, havendo casos em que se destroem os dados mesmo tendo sido efetivado o pagamento do resgate.

No que diz respeito a *frameworks* de segurança da informação e segurança cibernética, julgue o item subsequente.

112 O *framework* de segurança da informação e segurança cibernética MITRE ATT&CK oferece as seguintes aplicações práticas: melhoramento do entendimento das ameaças, testes de penetração, priorização de ameaças e riscos, melhoria dos controles de segurança, caça a ameaças e resposta a incidentes, avaliação de soluções de segurança, pesquisa e desenvolvimento.

Acerca de administração de sistemas de gestão de bancos de dados (SGBD), julgue os próximos itens.

113 O Postmaster é o principal processo no PostgreSQL e controla os demais processos do SGBD.

114 No PostgreSQL, o usuário *master* também é o usuário *master* do sistema operacional.

Julgue os itens seguintes, a respeito de ciência de dados e de modelagem de dados.

115 Os sistemas de bancos de dados NoSQL baseados em documentos armazenam os dados por meio de esquemas do tipo XML.

116 Em *Big Data*, uma das propriedades ACID é a atomicidade, que garante que todas as alterações sejam efetivadas no banco de dados, sem atualização parcial da transação.

117 Quando uma tabela está na terceira forma normal (3FN), toda coluna que não é chave depende diretamente da chave primária, sem dependências indiretas.

118 A regressão linear do aprendizado de máquina busca estabelecer uma relação entre as variáveis de entrada de um algoritmo.

Julgue os itens a seguir, relativos a *business intelligence* (BI).

119 As estatísticas relacionadas a BI devem ser geradas com base nas fontes transacionais, sem que haja acréscimo de informações diretamente da base de BI.

120 Os bancos de dados dimensionais que atendem ao *data warehouse* devem ser implementados de forma normalizada.

Espaço livre