-- CONHECIMENTOS ESPECÍFICOS --

A respeito dos processos de desenvolvimento de *software*, julgue os itens que se seguem.

51 A abordagem de melhoria de processos baseada em maturidade objetiva a adoção de práticas estruturadas e técnicas para elevar a qualidade do produto e a previsibilidade do processo.

52 No desenvolvimento incremental, não é exigida a entrega de cada um dos incrementos ao cliente, mas busca-se torná-los visíveis para possibilitar, sempre que viável, o *feedback* de *stakeholders*.

Com relação a práticas ágeis e ao sistema de gestão Kanban, julgue os itens subsequentes.

53 A limitação do WIP (*work in progress*) é uma prática fundamental no Kanban para apoiar a implementação do sistema puxado, no qual um novo item só é iniciado quando há capacidade disponível na equipe.

54 Um *product owner* que não aceita *feedback* do time de desenvolvimento ou dos *stakeholders* compromete a inspeção e adaptação do produto com base em colaboração, principal objetivo da *sprint review*.

55 A *daily scrum* baseada em fluxo altera o foco tradicional da reunião, o qual passa a ser as pessoas e a resolução de impedimentos dos itens de trabalho no quadro Kanban.

56 Um item de *backlog* deve ser uma história de usuário completa, não podendo ser representado por tarefas técnicas tal como, por exemplo, refatorar o código da interface com o usuário.

No que se refere a técnicas de priorização e de estimativas com *story points* e à gestão de *backlog*, julgue os itens a seguir.

57 Um *backlog* de portfólio permite o agrupamento e a organização dos itens do *backlog* em uma estrutura hierárquica, exibindo iniciativas, épicos e projetos estratégicos que orientam o trabalho da organização ao longo do tempo.

58 *Story points* são uma métrica precisa de tempo, pois refletem o esforço atual e a duração do trabalho ao considerarem fatores como complexidade, dependências, riscos e débitos técnicos.

Acerca das linguagens de programação, das linguagens de *script* e dos diferentes padrões de representação de dados, julgue os itens a seguir.

59 O Terraform e o Ansible possuem funcionalidades diferentes e, por esse motivo, não podem ser usados em conjunto para criar uma solução completa de automação de infraestrutura.

60 JSON e XML são representações usadas para a troca de dados entre aplicações, sendo o XML mais adequado para a troca de dados de forma organizada, e o JSON, quando são exigidas informações de *metadata*.

61 Quando comparada ao Python, a linguagem Java, apesar de ter uma sintaxe mais verbosa, com estrutura textual repetitiva e regras sintáticas mais rígidas, é mais adequada para aplicações que exigem alto desempenho, devido à velocidade de execução.

No que se refere ao desenvolvimento *web* e *mobile*, bem como ao desenvolvimento com contêineres, julgue os próximos itens.

62 Kubernetes é um *software* de orquestração que fornece uma API para controlar como e onde os contêineres serão executados; o uso desse *software* com o Docker pode tornar a infraestrutura mais robusta e fazer com que o aplicativo que os utiliza esteja mais disponível e mais escalonável.

63 Os padrões do W3C desempenham um papel fundamental na padronização de tecnologias, de modo a garantir acessibilidade, interoperabilidade e compatibilidade para páginas da *web* em diferentes dispositivos ou mesmo em diferentes navegadores, por meio do uso de soluções como HTML, XML e CCS3.

64 Em desenvolvimento *web*, o HTML é utilizado para estruturar páginas *web*, o CSS, para adicionar funcionalidades interativas à página e o JavaScript, para personalizar estilos da página.

No que se refere à integração de sistemas, à arquitetura de *software*, aos testes de *software* e aos bancos de dados, julgue os itens subsecutivos.

65 Os princípios FIRST orientam os testes automatizados a serem rápidos na execução, flexíveis na aplicação em diferentes contextos, independentes entre si, repetíveis consistentemente, autovalidáveis e oportunos na criação e execução.

66 *Stored procedures* em PL/SQL são estruturas armazenadas diretamente no banco de dados que permitem a execução de instruções SQL pré-compiladas, o que reduz o tráfego de rede e melhora o desempenho das aplicações.

67 RabbitMQ tem um modelo baseado em filas, tal que os produtores podem enviar mensagens para *exchanges*, que as roteiam para filas apropriadas, onde são processadas pelos consumidores, reduzindo o acoplamento entre os componentes da arquitetura e promovendo maior tolerância a falhas e escalabilidade.

68 O padrão MVC (*model-view-controller*) obriga que a visão (*view*) execute diretamente as operações de acesso e manipulação dos dados armazenados no banco de dados.

Acerca de princípios do DevOps, automação de *builds* e *deploys*, CI/CD, versionamento, *branches*, *merge* e *pipelines*, julgue os itens a seguir.

69 No Git, o *cherry-picking* permite que se adicione um *commit* de certa *branch* ao último *commit* de outra *branch*, sem que se inclua o restante dos *commits* da *branch* de origem.

70 Se a execução do comando `git blame -L 5,5 example.txt` gerasse `f4c2d3b1 (John Doe 2023-04-15 14:20:22 +0300 5)`, então o *id* do usuário que realizou o *commit* seria `f4c2d3b1`.

71 Equipes de DevOps monitoram continuamente o ciclo de vida do desenvolvimento, desde o planejamento até a implantação, e utilizam o Git para reiniciar os contêineres automaticamente em caso de falha.

A respeito de CI/CD (*continuous integration/continuous delivery*), julgue os próximos itens.

72 No trecho de arquivo `.gitlab-ci.yml`, utilizado no GitLab CI/CD para definir regras de execução de *pipelines*, só será criada a *pipeline* se as três regras de ativação do `workflow.rules` forem verdadeiras.

```
workflow:
  rules:
    -     if:     $ CI_PIPELINE_SOURCE     ==
'merge_request_event'
    - if: $ CI_COMMIT_TAG
    -      if:      $ CI_COMMIT_BRANCH      ==
$ CI_DEFAULT_BRANCH
```

73 No trecho do arquivo `.gitlab-ci.yml`, utilizado no GitLab CI/CD para definir regras de execução de *pipelines* com base em variáveis de ambiente, na execução do bloco `job2`, o valor da variável `ALL_JOBS_VAR` será `"Different value than default"`, pois variáveis definidas no nível do `job` têm precedência sobre as globais com o mesmo nome.

```
variables:
  ALL_JOBS_VAR: "A default variable"

job1:
  variables:
    JOB1_VAR: "Job 1 variable"
  script:
    - echo "Variables are '$ ALL_JOBS_VAR'
and '$ JOB1_VAR'"

job2:
  variables:
    ALL_JOBS_VAR:   "Different   value   than
default"
    JOB2_VAR: "Job 2 variable"
  script:
    - echo "Variables are '$ ALL_JOBS_VAR',
'$ JOB2_VAR', and '$ JOB1_VAR'"
```

Considere que o seguinte arquivo YAML tenha sido utilizado para criar um *deployment* no Kubernetes:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
spec:
  selector:
    matchLabels:
      app: nginx
  replicas: 2
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx
      image: nginx:1.14.2
      ports:
      - containerPort: 80
```

A partir das informações da situação hipotética precedente, julgue os itens a seguir.

74 O campo `selector` dentro do grupo `spec`, no código em apreço, é usado para encontrar os `pods` que pertencem a esse *deployment*, com base no rótulo `app: nginx`.

75 No código em questão, o campo `replicas: 2` no bloco `spec` indica que dois contêineres serão executados dentro de um único `pod` de nome `nginx`, que será ouvido na porta `80`.

Acerca do Rancher, julgue o seguinte item.

76 No arquivo `project.yaml` a seguir, utilizado para criar projetos dentro de um cluster Kubernetes gerenciado pelo Rancher, o campo `namespace` no bloco `metadata` deve ter o mesmo valor que o campo `clusterName` do bloco `spec` para que o recurso criado seja associado a um cluster específico.

```
apiVersion: management.cattle.io/v3
kind: Project
metadata:
  name: p-abc123
  namespace: local
spec:
  clusterName: local
  description: Example Project
  displayName: Example
```

Com base na Resolução CNJ n.º 522/2023, que institui o Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (MoReq-Jus), julgue os itens seguintes.

77 O programa de avaliação do grau de aderência dos sistemas ao MoReq-Jus e de atualização permanente é executado pela Secretaria Executiva do CNJ, com o apoio do Comitê do Programa Nacional de Gestão Documental e Memória do Poder Judiciário (PRONAME).

78 Os sistemas informatizados de gestão de processos e documentos utilizados em atividades judiciais e administrativas dos órgãos integrantes do Poder Judiciário deverão aderir aos requisitos do MoReq-Jus, com o objetivo de assegurar, entre outros, a confidencialidade, a integridade, a disponibilidade, a autenticidade e o não repúdio de processos e documentos do Poder Judiciário.

À luz da Resolução CNJ n.º 335/2020 e das Portarias CNJ n.º 252/2020, n.º 253/2020 e n.º 131/2021, julgue os próximos itens.

79 O grupo revisor de código-fonte das soluções da PDPJ-Br, de caráter permanente, será integrado por membros indicados pelos tribunais e pelo Departamento de Tecnologia da Informação e Comunicação do CNJ.

80 As soluções adotadas pela PDPJ-Br deverão, obrigatoriamente, abranger a autenticação uniformizada, a interoperabilidade e a usabilidade.

81 A contratação de qualquer novo sistema, módulo ou funcionalidade privados que cause dependência tecnológica do seu fornecedor poderá ensejar a responsabilização do ordenador de despesas por improbidade administrativa, sem prejuízo da comunicação da ocorrência ao respectivo tribunal de contas.

82 O processo de disponibilização de soluções para a PDPJ-Br será institucional e centralizado, limitando-se à participação de colaboradores integrantes do poder público, como medida de precaução e segurança.

83 Um representante da justiça militar, indicado pelo STM, deve integrar o Comitê Gestor Nacional da PDPJ-Br, cujo presidente deve ser um conselheiro do CNJ.

De acordo com a Resolução CNJ n.º 396/2021 e com a Portaria CNJ n.º 162/2021, julgue os itens que se seguem.

84 O protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário e o de Investigação de Ilícitos Cibernéticos do Poder Judiciário serão objeto de atualização a qualquer tempo, por indicação do Comitê Gestor de Segurança Cibernética do Poder Judiciário.

85 As ações para viabilizar a governança nacional em segurança cibernética do Poder Judiciário são coordenadas pela Secretaria de Tecnologia da Informação do Supremo Tribunal Federal.

Julgue os próximos itens, relativos a Java, API RESTful e JSON.

86 A execução do código a seguir, escrito em Java, retornará o resultado `True`.

```
package com.mcnz.recursion;

public class checkpgm {

  public static void main(String[] args) {
    boolean flag = Check("STM");
    System.out.println(flag);
  }
  public static boolean Check(String s){
    if(s.length() == 0 || s.length() == 1) {
      return true;
    }
    if(s.charAt(0) == s.charAt(s.length()-1)) {
      return Check(s.substring(1, s.length()-
1));
    }
    return false;
  }
}
```

87 No trecho de código a seguir, desenvolvido em Java, o método HTTP em questão criará um recurso novo ou um novo objeto no servidor.

```
HttpRequest              request              =
HttpRequest.newBuilder()
  .PUT(HttpRequest.BodyPublishers.ofString
(requestBody))
  .uri(URI.create("https://api.restful-
api.dev/objects/4"))
  .header("Content-Type",
"application/json")
  .build();
```

88 A execução do seguinte código, escrito em Java, resultará um código JSON válido.

```
public class CriaJson {
    public static void main(String[] args)
{
        String json = "{\n" +
                      "\"nome\":
\"Supremo\";\n" +
                      "\"nome\:
\"Tribunal\";\n" +
                      "\"nome\":
\"Militar\"\n" +
                      "}";
         System.out.println(json);
    }
}
```

A respeito de Flyway, PostgreSQL e H2 Database, julgue os próximos itens.

89 Caso o comando `flyway migrate` seja executado em um terminal de uma máquina com Flyway CLI instalado e configurado corretamente, o Flyway identificará *scripts* de migração que ainda não foram aplicados e os executará na ordem crescente de versão, atualizando o banco de dados com as alterações mais recentes definidas nos *scripts* de migração.

90 Considere que os comandos a seguir tenham sido executados no PostgreSQL 14.18.

```
CREATE TABLE IF NOT EXISTS public.servidor
(idServidor INT GENERATED BY DEFAULT AS
IDENTITY PRIMARY KEY,
nome VARCHAR(30));

CREATE TABLE IF NOT EXISTS public.magistrado
(idServidor INT GENERATED BY DEFAULT AS
IDENTITY PRIMARY KEY,
matricula int)
INHERITS (public.servidor);

INSERT INTO public.servidor (nome)
VALUES ('Pedro'), ('João');

INSERT INTO public.magistrado (nome)
VALUES ('Maria');

SELECT * FROM public.servidor;
```

Nesse caso, o comando `SELECT * FROM public.servidor;` apresentará, ao ser executado, o resultado a seguir.

```
idServidor | nome
-----------+-------
         1 | Pedro
         2 | João
         3 | Maria
-----------+-------
```

91 Ao ser executado no H2 Database, o comando `MERGE INTO SCHEMA(ID) VALUES(1, 'STM')`, em que `ID` é a coluna chave e `1` e `STM` são valores válidos no contexto, permite atualizar a linha, se existente, e inserir linhas inexistentes; se nenhuma coluna de chave for especificada, as colunas de chave primária serão usadas para encontrar a linha.

No que se refere a *single sign-on*, Git e Keycloak, julgue os itens subsequentes.

92 Keycloak é uma ferramenta *open-source* que permite, em um projeto que utilize abordagem DevSecOps, implementar com segurança CI (*continuous integration*) e CD (*continuous deployment*), automatizando etapas do ciclo de desenvolvimento de *software*, como construção, teste e implantação.

93 O comando `git fetch origin branchSTM` busca, ao ser executado, todos os dados no repositório remoto ainda não conhecidos pelo usuário, o qual poderá, depois de obter esses dados, fazer o *merge*.

94 *Single sign-on* é uma solução de autenticação que permite que os usuários façam *login* uma vez utilizando um único conjunto de credenciais e acessem várias aplicações durante a mesma sessão.

A respeito do planejamento estratégico de TIC e da governança de TIC, julgue os itens a seguir.

95 A integração das metodologias OKR, PKI e BSC no planejamento estratégico de TIC permite alinhar objetivos organizacionais com indicadores de desempenho, e a análise SWOT complementa esse processo ao identificar forças, fraquezas, oportunidades e ameaças, facilitando a tomada de decisões estratégicas.

96 O COBIT 2019 e o ITIL v4 são amplamente utilizados na gestão de TIC, sendo o primeiro voltado para o gerenciamento de serviços de TI e a melhoria contínua dos processos operacionais, e o segundo, exclusivamente para a governança, estabelecendo diretrizes estratégicas.

97 O Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) alinha as necessidades de TIC aos objetivos organizacionais, garantindo eficiência na gestão dos recursos, bem como inclui indicadores de desempenho para monitoramento contínuo.

A respeito de gerenciamento de projetos de TIC, julgue os itens que se seguem.

98 O escritório de projetos (PMO) desempenha um papel fundamental na governança de projetos, podendo atuar de forma consultiva, diretiva ou de controle, conforme o nível de influência que exerce sobre os projetos da organização.

99 O PMBOK 7.ª edição mantém a estrutura tradicional baseada em grupos de processos e áreas de conhecimento, garantindo que todas as fases do projeto sejam rigidamente seguidas conforme um modelo prescritivo, sem possibilidade de adaptação às necessidades organizacionais.

Com base nas Resoluções CNJ n.º 370/2021 e n.º 468/2022, julgue os itens subsequentes.

100 As contratações de soluções de TIC por órgãos do Poder Judiciário deverão ser precedidas da elaboração de um plano de contratações de STIC, que deve estar alinhado com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), com o planejamento estratégico institucional, com a Estratégia Nacional do Poder Judiciário e com a Estratégia Nacional de TIC do Poder Judiciário (ENTIC-JUD).

101 A Estratégia Nacional de TIC do Poder Judiciário (ENTIC-JUD) determina que o plano de transformação digital seja elaborado pela unidade competente dos órgãos, respeitadas suas especificidades, e que seja aprovado pelo Comitê de Gestão de TIC.

Acerca da gestão de riscos de TIC, julgue o seguinte item.

102 A gestão de riscos de TIC deve focar exclusivamente a mitigação de ameaças externas, como ataques cibernéticos e falhas de segurança, sem necessidade de considerar riscos internos, como erros operacionais, falhas de infraestrutura ou problemas de conformidade regulatória.

Com base na Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), julgue o próximo item.

103 A LGPD estabelece princípios fundamentais para o tratamento de dados pessoais, de forma a garantir direitos como privacidade, autodeterminação informativa e segurança de dados pessoais, e aplica-se a qualquer operação de tratamento realizada por pessoa física ou jurídica, independentemente do meio utilizado.

Julgue os itens que se seguem, relativos a ciência de dados e inteligência artificial (IA).

104 Viés algorítmico pode ocorrer quando os dados utilizados no treinamento de um sistema de IA refletem desigualdades sociais, o que pode resultar em decisões discriminatórias automatizadas.

105 *Deep learning* é um campo da IA cujos modelos conseguem reconhecer padrões de dados, tais como imagens e textos, para produzir *insights* e previsões precisas, sendo as redes neurais sua tecnologia subjacente.

106 A descentralização promovida pela tecnologia *blockchain* impede a aplicação de políticas de acesso e controle, já que todos os participantes da rede possuem os mesmos direitos sobre os dados.

107 A partir da representação de uma aplicação construída no Qlik Sense Desktop, conclui-se que essa ferramenta é compatível exclusivamente com bases relacionais estruturadas, devendo os dados estar previamente organizados em tabelas para a viabilização da visualização que ele oferece.

108 *Data marts* são bases centralizadas e corporativas que integram dados de diferentes áreas da organização, com foco em armazenamento de longo prazo e governança de dados.

109 A regressão linear é um modelo preditivo supervisionado que estabelece uma relação entre variáveis independentes e uma variável dependente de natureza contínua.

110 A técnica de validação cruzada *k-fold* contribui para a avaliação de modelos preditivos, reduzindo a variabilidade decorrente da segmentação do conjunto de dados em partes de treinamento e teste.

111 Modelos de linguagem de grande escala, como os do tipo *transformer*, são treinados exclusivamente com base em regras sintáticas explícitas extraídas de dados linguísticos anotados manualmente, o que assegura maior controle semântico.

Certa empresa brasileira de médio porte, que desenvolve soluções de *software* para o setor financeiro e armazena informações sensíveis de clientes, como dados bancários, documentos pessoais e credenciais de acesso, iniciou um processo de adequação à norma ISO/IEC 27001:2022, implementando um sistema de gestão da segurança da informação (SGSI). A equipe de segurança da empresa criou políticas para garantir confidencialidade, integridade, disponibilidade e autenticidade das informações e adotou criptografia assimétrica, controle de acesso baseado em função, e o NIST Cybersecurity Framework para resposta a incidentes. Foram identificadas vulnerabilidades de injeção SQL e a empresa sofreu um ataque DDoS que afetou a disponibilidade do sistema.

Com base na situação precedente, julgue os itens a seguir.

112 O uso de criptografia assimétrica pela empresa em apreço permite que um sistema envie dados criptografados por meio da chave privada e os decifre com a mesma chave.

113 De acordo com o NIST Cybersecurity Framework adotado pela empresa em questão, é recomendável que ações como identificação de riscos e recuperação de sistemas façam parte do processo de segurança.

114 Na implementação da ISO/IEC 27001:2022, a empresa em questão pode optar por não realizar avaliação de riscos, desde que adote integralmente todos os controles sugeridos pela norma ISO/IEC 27002:2022, pois o cumprimento completo dos controles é suficiente para demonstrar conformidade com a norma principal.

O XYZ Digital, sistema nacional de agendamento de serviços públicos, acessado via *desktop* e dispositivos móveis, que exige autenticação de cidadãos para solicitação de documentos e consultas, passou por auditoria de segurança após tentativas de acesso indevido e um incidente de autenticação indevida. Após o incidente, constatou-se a utilização de *single sign-on* (SSO – autenticação única), tendo sido providenciadas a autenticação forte com multifator (MFA) e a implementação de OpenID Connect.

A partir do caso hipotético precedente, julgue os itens subsequentes.

115 O uso de SSO pode representar um risco à segurança se não for acompanhado por mecanismos adicionais de segurança, como *logout* global e MFA.

116 A implementação de OpenID Connect no XYZ Digital permite a autenticação federada, na qual um provedor de identidade confiável autentica o usuário em nome do sistema.

117 A alteração das informações de usuário por atacantes durante o processo de autenticação no XYZ Digital representa uma violação do princípio de confidencialidade.

Julgue os seguintes itens, relativos a CSRF (*cross-site request forgery*), testes de invasão e segurança de aplicativos *web*.

118 Aplicações *web* que não implementam corretamente mecanismos de controle de sessão, como expiração de *tokens* e invalidação de sessões inativas, tornam-se vulneráveis a sequestro de sessão (*session hijacking*), mesmo que utilizem HTTPS.

119 O objetivo principal dos testes de invasão é simular falhas de desempenho de servidores, avaliando a carga sob estresse para fins de escalabilidade.

120 Em um ataque CSRF, o navegador de um usuário autenticado pode ser induzido a realizar ações maliciosas no sistema do usuário sem o conhecimento deste.

Espaço livre