-- CONHECIMENTOS ESPECÍFICOS –

Julgue os itens que se seguem, de acordo com os normativos relacionados à Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br).

51 Se, no desenvolvimento do sistema informatizado de gestão de processos e documentos de um órgão do Poder Judiciário, for constatado conflito entre um requisito não funcional de segurança e um requisito não funcional de usabilidade, então, conforme a resolução do CNJ que instituiu o MoReq-Jus, o requisito não funcional relacionado à segurança deve ser aplicado em detrimento do requisito relacionado à usabilidade.

52 Se a PDPJ-Br contratar um serviço de computação em nuvem na modalidade de integrador de nuvem (*broker*), não é necessário que o serviço tenha a capacidade de mensurar o uso dos recursos da nuvem de forma individualizada por cliente de cada serviço provido na PDPJ-Br.

53 Se um juiz auxiliar da presidência do CNJ for designado como membro do Comitê Gestor Nacional da PDPJ-Br, então, nesse caso, ele deverá presidir o Comitê.

54 Se um novo serviço for projetado para a PDPJ-Br com o uso do modelo arquitetural de microsserviços, então, conforme normativo do CNJ, na interação entre os microsserviços, deve-se adotar o modelo de coreografia, por meio de um serviço centralizado de mensageria, o que garante o desacoplamento.

Julgue os itens subsequentes, conforme as Portarias CNJ n.º 131/2021 e n.º 162/2021, e as Resoluções CNJ n.º 396/2021 e n.º 468/2022.

55 Se forem implementadas mudanças no código-fonte de uma solução disponibilizada na PDPJ-Br, o código-fonte alterado deverá ser encaminhado para análise do Grupo Revisor de Código-Fonte das soluções da PDPJ-Br e do sistema Processo Judicial Eletrônico (PJe).

56 Na estrutura organizacional de um tribunal regional, conforme a resolução que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), a estrutura de segurança da informação deverá ser subordinada diretamente à área de TIC do respectivo órgão.

57 Para fins de investigação de ilícito, os registros históricos de eventos (*logs*) devem ser armazenados pelo período mínimo de 12 meses, a fim de atender aos normativos do CNJ.

58 Na contratação relativa a desenvolvimento de *software* em órgão submetido ao controle administrativo e financeiro do CNJ, diante da dificuldade de mensurar o esforço, a adoção da métrica homem-hora somente será permitida caso haja justificativa e vinculação à entrega de produtos de acordo com prazos e qualidade previamente definidos.

De acordo com os normativos do Conselho Nacional de Justiça (CNJ), julgue os itens a seguir.

59 No âmbito da administração de sistemas judiciais, os órgãos do Poder Judiciário devem priorizar o uso de contas compartilhadas para autenticação e controle de acessos, uma vez que esse modelo é considerado o mais eficaz para assegurar rastreabilidade, responsabilização e segurança das operações realizadas por usuários internos.

60 A Resolução do CNJ que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) estabelece que os objetivos, os princípios e as diretrizes de segurança da informação devem ser alinhados às recomendações da norma NBR ISO/IEC 27001:2013, devendo a ENSEC-PJ assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e informações.

Julgue os itens a seguir, relativos a Java, Swagger, PostgreSQL e JSON.

61 O código em Java a seguir, ao ser executado, apresentará `22` como resultado.

```
public class Main {
  public static void main(String[] args) {
    Object valor = "22 TJ PA";
    if (valor instanceof String s) {
      valor = s.replaceAll("[^a-zA-Z]", "");
    }

    switch (valor) {
      case String s -> System.out.println(s);
      case Integer i -> System.out.println(i);
      default -> System.out.println(valor);
    }
  }
}
```

62 O Swagger, quando utiliza a OpenAPI 3.0, permite descrever as APIs protegidas por meio do esquema de segurança *bearer authentication*.

63 Considere o código em Java a seguir, especialmente em relação aos valores descritos na notação JSON.

```
import java.util.Arrays;
import java.util.Collections;
public class JsonSortDescendingExample {
  public static void main(String[] args) {
   String jsonString =
"{\"TJPA\":[\"Tribunal\",\"Justica\",\"Estado\"
,\"Para\"]}";
   String arrayContent =
jsonString.substring(
     jsonString.indexOf("[") + 1,
     jsonString.indexOf("]")
   );
   String[] values =
arrayContent.replaceAll("\"", "").split(",");
   Arrays.sort(values,
Collections.reverseOrder());

   // Exibindo os valores ordenados
   System.out.println("Resultado:");
   for (int i = values.length - 1; i >= 0; i--)
{
   System.out.println(values[i]);
   }
  }
}
```

Esse código, ao ser executado, apresentará o resultado a seguir.

```
Resultado:
Estado
Justica
Para
Tribunal
```

```
CREATE TABLE processos (
   idproc INT PRIMARY KEY,
   descricao VARCHAR(50),
   referencia INT REFERENCES processos(idproc)
);

INSERT INTO processos (idproc, descricao,
referencia) VALUES
(1, 'Gabinete', NULL),
(2, 'Processo A', 1),
(3, 'Processo B', 2),
(4, 'Recurso 1', 3);
```

Considerando que os comandos precedentes tenham sido executados no PostgreSQL 14, julgue o item subsequente.

64 Suponha que, no mesmo banco de dados e imediatamente após a execução dos comandos apresentados, tenha sido executado o código SQL a seguir.

```
WITH RECURSIVE processop AS (
    SELECT idproc, descricao, referencia
    FROM processos
    WHERE referencia IS NOT NULL

    UNION ALL

    SELECT p.idproc, p.descricao, p.referencia
    FROM processos p
    INNER JOIN processop pp ON p.referencia =
pp.idproc
)
SELECT distinct
    idproc,
    descricao,
    (SELECT descricao FROM processos WHERE
idproc = processop.referencia) AS
descricao_pai
FROM processop
ORDER BY idproc;
```

Nessa situação hipotética, após as referidas ações, será apresentado o resultado a seguir.

```
 idproc | descricao  | descricao_pai
--------+------------+---------------
      2 | Processo A | Gabinete
      3 | Processo B | Processo A
      4 | Recurso 1  | Processo B
```

Julgue os próximos itens, relativos a Keycloak, RabbitMQ, GitHub e Kubernetes.

65 As políticas de autorização do Keycloak, em sua versão mais recente, embora não permitam controle de acesso com referência temporal por questões de segurança, permitem o controle de acesso com base no usuário e em atributos.

66 No RabbitMQ, em sua versão mais recente, as filas de quórum devem ser utilizadas especialmente quando envolvem filas temporárias ou transitórias.

67 No GitHub, pode-se utilizar o comando `git stash` caso seja necessário mudar de *branch* por um tempo sem fazer o *commit* de um trabalho incompleto.

68 Kubernetes é uma plataforma unificada nativa que, ainda que não ofereça autenticação centralizada, permite a implantação de *bare metal* e de nuvens públicas com a utilização de contêineres.

Julgue os próximos itens, a respeito de meios de transmissão, tipos de cabeamento, tecnologias, modelos de referência e elementos de rede.

69 As fibras ópticas do tipo multimodo possuem diâmetro maior que as do tipo monomodo e podem ser usadas com equipamentos mais baratos, sendo ideais para transmissão em curtas distâncias, de até 15 km.

70 O cabo de categoria 5e suporta até 100 MHz e permite o uso do padrão Ethernet a 1 Gbps.

71 O cabeamento estruturado para *backbone* de *campus* estende-se desde os distribuidores de piso até as tomadas de telecomunicação conectadas a ele.

72 No padrão IEEE 802.11, utilizado em WLAN, as transmissões são feitas por meio de rádios de curto alcance nas bandas de 2,4 GHz (maior alcance) e 5 GHz (menor interferência).

73 Na descoberta da unidade máxima de transmissão (MTU) do caminho, o pacote é dividido em fragmentos, que seguem como pacotes independentes até o destino, onde são remontados.

74 Em redes de computadores, os roteadores operam na camada de enlace de dados, utilizando endereços IP para encaminhar pacotes.

75 Os *hubs* operam na camada física, conectam várias linhas e retransmitem sinais para todas as portas, mas sem inteligência de comutação.

Acerca de protocolos de rede e sistemas de detecção de intrusão (IDS), julgue os itens a seguir.

76 O IPv6 utiliza endereços de 32 *bits* para identificar interfaces de rede em *hosts* e roteadores, sendo compatível com os protocolos TCP e UDP, bem como com o IPv4.

77 O CIDR foi criado para resolver dois grandes problemas da Internet: o crescimento desenfreado das tabelas de roteamento e o desperdício de endereços IP no antigo sistema de classes (A, B, C).

78 Na consulta recursiva do DNS, o servidor de nomes responde com a próxima etapa e o resolvedor local continua o processo.

79 IDS são usados para identificar e combater ataques em redes e podem ser baseados em assinaturas ou em anomalias.

Em relação a serviços de nuvem, sistemas operacionais e conceitos de DevOps, julgue os itens subsequentes.

80 No modelo de nuvem privada, os recursos pertencem a um provedor terceirizado, sendo oferecidos mediante pagamento ou outros meios, como publicidade.

81 O AD DS (*Active Directory Domain Services*) do Microsoft Windows Server conta com política de senha refinada, restrita ao uso via linha de comando.

82 DevOps é um conjunto de práticas que integra desenvolvimento e operações de *software*, promovendo colaboração entre equipes para entregar aplicações e serviços de forma mais rápida, visando alinhar a área de TI com a estratégia organizacional.

Julgue os itens que se seguem, a respeito de NAT, SNMP, tipos de *backup* e servidor de aplicação IIS.

83 A NAT foi criada como solução para o esgotamento de endereços IPv4 e sua função é permitir que uma rede interna use endereços IP privados (não roteáveis na Internet) e traduza esses endereços para um IP público ao se comunicar com a Internet.

84 O SNMP é organizado em uma árvore hierárquica, com identificadores únicos denominados OID (*object identifiers*).

85 Um *backup* incremental faz cópias apenas dos dados alterados desde o último *backup* e tem como desvantagem a restauração mais demorada, requerendo todos os *backups* incrementais anteriores.

86 O servidor de aplicação IIS possui arquitetura modular, o que permite a ativação ou a desativação de funcionalidades, conforme a necessidade.

Considerando as normas da ABNT acerca de gestão da segurança e gestão de riscos de sistemas de informação, julgue os itens a seguir.

87 A NBR ISO/IEC 27002:2022 apresenta estrutura com dois aspectos complementares de organização: agrupamento de controles em domínios temáticos e aplicação de múltiplos atributos de classificação a cada controle.

88 O processo iterativo de monitoramento e análise crítica de riscos descrito na ABNT NBR ISO/IEC 27005:2022 fornece subsídios para o atendimento aos requisitos de melhoria contínua e análise crítica pela direção previstos na ABNT NBR ISO/IEC 27001:2013.

89 No escopo da ABNT NBR ISO/IEC 27005:2022, os aspectos da gestão da continuidade do negócio são abordados em dois grupos principais de controles: continuidade da segurança da informação e redundâncias suficientes para o atendimento aos requisitos de disponibilidade.

A respeito de conceitos e ferramentas relativos à segurança da informação, julgue os itens subsequentes.

90 Na arquitetura de gestão de identidades do Keycloak, a hierarquia de configuração privilegia comandos explícitos sobre definições ambientais, priorizando argumentos ou opções fornecidos diretamente na linha de comando sobre as variáveis de ambiente.

91 *Ping sweeping* é definida como uma técnica meramente defensiva implementada para a identificação de dispositivos não autorizados em redes *wireless*, como *hosts* ativos, sem deixar rastros nos *logs* de *firewall*.

92 SPF e DKIM são protocolos de análise de conteúdo que trabalham em conjunto na identificação de palavras-chave suspeitas no texto do *email*, atribuindo pontuação de risco com base no contexto semântico da mensagem.

93 Ataques de *buffer overflow* em aplicações *web* ocorrem tipicamente em componentes *server-side* desenvolvidos em linguagens de baixo nível, mediante a exploração da manipulação inadequada de limites de memória em módulos compilados do servidor para a execução do código arbitrário no sistema hospedeiro.

94 Os vírus de computador são programas autônomos que se propagam automaticamente por meio de redes sem a necessidade de ação humana, ao passo que os *worms* exigem interação do usuário para iniciar sua replicação.

Julgue os itens que se seguem, acerca de princípios e tecnologias de criptografia aplicados à segurança da informação.

95 Entre as propriedades fundamentais de uma função *hash* segura destaca-se a resistência à segunda pré-imagem, que inviabiliza, do ponto de vista computacional, a identificação de uma entrada alternativa capaz de gerar o mesmo resumo criptográfico de uma entrada específica preexistente.

96 Esquemas de assinatura digital fundamentados em criptografia de chave pública não garantem, por si mesmos, a confidencialidade da informação.

97 A autoridade certificadora do tempo (ACT) da ICP-Brasil administra os mecanismos de sincronização e adaptação temporal dos carimbos criptográficos em transações nacionais que perpassam diferentes fusos horários.

Julgue os próximos itens, no que se refere a controles de acesso, gerenciamento de identidades e serviços de autenticação no âmbito da segurança da informação.

98 O controle de acesso baseado em papéis, implantado no modelo restrito, permite que usuários tenham papéis potencialmente conflitantes em seu perfil, mas impede a ativação simultânea desses papéis durante a mesma sessão de autenticação.

99 No processo de identificação do usuário no sistema, a autorização é um mecanismo de controle de acesso colocado em prática pelo uso de validações, como credenciais secretas, *tokens* exclusivos de identificação pessoal ou características biométricas únicas.

Julgue os itens subsecutivos, em relação a vetores de ataques cibernéticos em comunicação sem fio e mensageria eletrônica.

100 Os ataques DDoS por *botnet* sem *spoofing* não utilizam técnicas como o DNS *footprinting*, mas, sim, a força bruta de múltiplos dispositivos comprometidos que enviam tráfego malicioso com seus endereços reais.

101 Quando servidores de *email* corporativo estão comprometidos por ataque de *spear phishing*, é estabelecido um canal persistente que permite ao atacante executar ataques de *whaling* automatizados sem interação com novas mensagens.

102 Uma forma usual de atuação de um *adware* é analisar o conteúdo dos *emails* para identificar termos-chave de interesse comercial, enviando esses dados para anunciantes que podem, então, enviar *emails* direcionados ao destinatário.

Julgue os itens a seguir, que versam acerca da administração do SGBD Oracle, da modelagem de dados multidimensional e do conceito de *data lake*.

103 Oracle RMAN (Recovery Manager) é uma ferramenta capaz de realizar apenas *backups* lógicos de objetos do banco de dados, como tabelas e usuários, de modo que *backups* físicos são realizados por outras ferramentas, como Data Pump.

104 O Oracle Data Guard permite a replicação síncrona e assíncrona de dados entre bancos de dados primários e de *standby*, oferecendo alta disponibilidade e recuperação de desastres.

105 Na modelagem multidimensional, a tabela fato contém os dados de medição quantitativa, está no centro do esquema estrela e tem relação direta com as tabelas dimensão.

106 O conceito de *data lake* baseia-se na estruturação rígida dos dados no momento da ingestão (*schema-on-write*), o que garante integridade imediata e desempenho otimizado em consultas transacionais.

Acerca dos tipos de aprendizado, da inteligência artificial generativa e das redes neurais, julgue os itens subsequentes.

107 O aprendizado por reforço é utilizado principalmente em tarefas de classificação supervisionada, nas quais o agente aprende com base em dados rotulados fornecidos previamente.

108 A inteligência artificial generativa inclui modelos como as redes generativas adversárias e os modelos baseados em transformadores, os quais são capazes de criar novos conteúdos, como imagens, textos ou áudios.

109 Em arquiteturas de redes neurais profundas, o uso de funções de ativação não lineares, como ReLU ou Sigmoid, é essencial para que a rede aprenda padrões complexos e não lineares.

110 Redes neurais convolucionais são utilizadas principalmente em tarefas de processamento sequencial, como tradução automática e análise de sentimentos em linguagem natural.

A respeito dos fundamentos de GPU para ambientes de alto desempenho e das aplicações práticas da CUDA, julgue os itens a seguir.

111 A utilização de GPU permite acelerar cargas de trabalho de alta complexidade, superando a capacidade de processamento de CPUs tradicionais para a execução de certas tarefas, como o treinamento de modelos de aprendizado profundo para a análise preditiva de sentenças.

112 Técnicas como AWQ (*activation-aware weight quantization*) e GGUF (*general unified format*) comprometem a precisão e a viabilidade da execução local de grandes modelos de linguagem, sendo inadequadas para aplicações como *chatbots offline*, análise de texto em tempo real ou inferência embarcada, já que essas abordagens aumentam a latência e o consumo de memória, exigindo *hardware* com alta capacidade computacional.

113 Em CUDA, a execução paralela é estruturada em *threads*, que formam *blocks*, os quais, por sua vez, compõem *grids*, podendo diferentes *blocks* dentro de um mesmo *grid* compartilhar automaticamente sua memória local e seus registradores.

114 Em uma GPU, o programador define diretamente no código quantos blocos de *threads* devem ser executados, enquanto o escalonador de blocos de *threads*, implementado em *hardware*, distribui esses blocos entre os processadores SIMD *multithreaded*.

115 No desenvolvimento de aplicações com CUDA, uma das estratégias recomendadas para a otimização de desempenho é a minimização do uso da memória compartilhada do dispositivo, priorizando-se o acesso direto à memória global, já que esta possui maior largura de banda e menor latência.

Julgue os próximos itens, em relação a cuDNN, gerenciamento de GPU com NVIDIA SMI, e infraestrutura e operação de ambientes com GPU.

116 No ambiente Windows, a instalação e o uso do cuDNN com Python é um processo complexo que exige a compilação manual do cuDNN a partir do código-fonte e a modificação direta de bibliotecas Python de baixo nível, pois os *frameworks* de *deep learning*, como TensorFlow e PyTorch, não possuem integração nativa com o cuDNN no ambiente Windows, tornando-o inviável para desenvolvedores comuns.

117 O utilitário `nvidia-smi`, integrante da SMI da NVIDIA, é restrito à função de leitura passiva de métricas da GPU em tempo real, como temperatura, uso de memória e potência, não oferecendo suporte à reconfiguração de parâmetros operacionais nem à ativação de modos persistentes, funcionalidades que dependem exclusivamente de ferramentas avançadas como o NVIDIA Control Panel.

118 O uso de resfriamento líquido direto ao *chip* em *data centers* de inteligência artificial permite a operação com temperaturas de água mais elevadas, reduzindo a dependência de *chillers* mecânicos em diversos climas, abordagem que contribui tanto para a eficiência energética quanto para a eficiência hídrica.

119 A correta execução de bibliotecas de inteligência artificial que utilizem aceleração por GPU, como TensorFlow ou PyTorch com suporte CUDA, depende da compatibilidade entre as versões da GPU NVIDIA, do *driver* instalado, do CUDA Toolkit e da biblioteca utilizada, visto que uma incompatibilidade entre esses componentes pode impedir o uso da GPU, mesmo que ela esteja fisicamente instalada e funcional.

120 A virtualização de GPU com NVIDIA vGPU permite o compartilhamento de uma única GPU física entre múltiplas máquinas virtuais ou contêineres; no caso do uso com contêiner Docker, é necessário que o *host* tenha os *drivers* NVIDIA instalados, além do NVIDIA Container Toolkit, para que os contêineres consigam acessar a GPU corretamente.

Espaço livre