Cebraspe
Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos

TRIBUNAL DE CONTAS DO ESTADO DO MARANHÃO (TCE/MA)

CARGO 10: ANALISTA ESTADUAL DE APOIO AO CONTROLE EXTERNO
ÁREA: APOIO TÉCNICO-ADMINISTRATIVO
ESPECIALIDADE: TECNOLOGIA DA INFORMAÇÃO

Prova Discursiva – Peça técnica

Aplicação: 22/11/2026

PADRÃO DE RESPOSTA

1) ESTRUTURA DO PARECER
O texto do(a) candidato(a) deverá ser identificado como parecer (ex. Parecer n. xxx) e conter os seguintes elementos estruturais: **ementa ou assunto, análise e conclusão** (vedada qualquer forma de identificação do(a) candidato(a)).

2) ANÁLISE DOS ACHADOS 1 E 2 À LUZ DO COBIT 2019
Os achados 1 e 2 evidenciam fragilidades na governança de informação e tecnologia. No COBIT 2019, governança e gestão possuem finalidades distintas: a governança avalia necessidades, condições e opções das partes interessadas, estabelece direcionamento por meio da priorização e tomada de decisões e monitora desempenho e conformidade; a gestão planeja, constrói, executa e monitora atividades em alinhamento com a direção estabelecida pelo órgão de governança. O achado 1 relaciona-se especialmente ao EDM01 – Ensured Governance Framework Setting and Maintenance, pois revela ausência de estrutura decisória adequada e de participação sistemática da alta administração. Também alcança o EDM02 – Ensured Benefits Delivery, uma vez que os investimentos em TI não estão formalmente vinculados aos benefícios e objetivos estratégicos esperados. No achado 2, a continuidade de projetos, apesar de atrasos, aumento de custos e redução dos benefícios esperados, evidencia deficiência no EDM02. A ausência de avaliação integrada dos riscos relaciona-se ao EDM03 – Ensured Risk Optimization, enquanto a falta de análise sistemática da utilização dos recursos de TI alcança o EDM04 – Ensured Resource Optimization. Indicadores predominantemente operacionais também são insuficientes para que o órgão de governança acompanhe geração de valor, riscos e recursos. O COBIT 2019, portanto, exige que a TI seja governada sob perspectiva corporativa, orientada à geração de valor para as partes interessadas.

3) ANÁLISE DO ACHADO 3 À LUZ DA ISO/IEC 38500
O achado 3 demonstra inadequada separação entre governança e gestão. Segundo a ISO/IEC 38500, cabe ao órgão de governança exercer as funções de avaliar, direcionar e monitorar o uso atual e futuro da TI. A alta administração deve, portanto, avaliar propostas e necessidades relacionadas à tecnologia, estabelecer direcionamentos coerentes com os objetivos organizacionais e monitorar desempenho e conformidade. A delegação de decisões estratégicas à unidade técnica compromete o exercício da responsabilidade pelo órgão de governança. De forma correspondente, a participação direta da alta administração em decisões essencialmente operacionais confunde governança com gestão. Devem existir atribuições claramente estabelecidas, autoridade compatível com as responsabilidades e mecanismos de prestação de contas. Assim, a área de TI deve executar e gerenciar as ações conforme o direcionamento recebido, enquanto o órgão de governança permanece responsável por avaliar, direcionar e monitorar a utilização da tecnologia, preservando a adequada responsabilização pelas decisões.

4) CONCLUSÃO E RECOMENDAÇÕES
Conclui-se que os achados demonstram fragilidades relevantes na governança de TI da secretaria, especialmente no que concerne a participação da alta administração, alinhamento estratégico, definição de responsabilidades, acompanhamento dos benefícios, tratamento dos riscos, utilização dos recursos e monitoramento dos resultados. O tribunal de contas poderá recomendar ao órgão jurisdicionado a formalização ou revisão de sua estrutura de governança de TI; a clara separação entre responsabilidades de governança e de gestão; a participação efetiva da alta administração nas decisões estratégicas; o alinhamento dos investimentos de TI aos objetivos institucionais; e a implantação de mecanismos para avaliar e monitorar benefícios, riscos, recursos e desempenho. As providências devem favorecer uma governança de TI orientada à geração de valor, com responsabilidades definidas e mecanismos de monitoramento e prestação de contas em consonância com o COBIT 2019 e com a ISO/IEC 38500.

QUESITOS AVALIADOS

Quesito 2.1 – Estrutura do parecer
Conceito 0 – Não apresentou estrutura de parecer.

Conceito 1 – Apresentou apenas um dos elementos estruturais do parecer (identificação, ementa ou assunto, análise e conclusão).
Conceito 2 – Apresentou apenas dois dos elementos estruturais do parecer.
Conceito 3 – Apresentou apenas três dos elementos estruturais do parecer.
Conceito 4 – Apresentou os quatro elementos estruturais do parecer.

Quesito 2.2 – Análise dos achados 1 e 2
Conceito 0 – Não abordou o quesito ou o fez de forma totalmente equivocada.
Conceito 1 – Apresentou adequadamente apenas um dos seguintes aspectos: (i) análise do achado 1 à luz do COBIT 2019; (ii) análise do achado 2 à luz do COBIT 2019; (iii) distinção técnica entre governança e gestão de TI; (iv) relação das deficiências com os objetivos do domínio EDM.
Conceito 2 – Apresentou adequadamente apenas dois dos aspectos enumerados.
Conceito 3 – Apresentou adequadamente apenas três dos aspectos enumerados.
Conceito 4 – Apresentou adequadamente os quatro aspectos enumerados.

Quesito 2.3 – Análise do achado 3
Conceito 0 – Não abordou o quesito ou o fez de forma totalmente equivocada.
Conceito 1 – Apresentou adequadamente apenas um dos seguintes aspectos: (i) análise do achado 3 à luz da ISSO/IEC 38500; (ii) responsabilidade do órgão de governança pelo uso da TI; (iii) aplicação das funções de avaliar, direcionar e monitorar; (iv) adequada delimitação das responsabilidades entre o órgão de governança e a gestão.
Conceito 2 – Apresentou adequadamente apenas dois dos aspectos enumerados.
Conceito 3 – Apresentou adequadamente apenas três dos aspectos enumerados.
Conceito 4 – Apresentou adequadamente os quatro aspectos enumerados.

Quesito 2.4 – Conclusão e recomendações
Conceito 0 – Não apresentou conclusão com recomendações ou propôs recomendações totalmente impertinentes.
Conceito 1 – Apresentou conclusão, mas propôs apenas uma recomendação pertinente.
Conceito 2 – Apresentou conclusão e propôs duas recomendações pertinentes, mas de forma genérica.
Conceito 3 – Apresentou conclusão e propôs duas ou mais recomendações pertinentes.

Cebraspe
Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos

TRIBUNAL DE CONTAS DO ESTADO DO MARANHÃO (TCE/MA)

CARGO 10: ANALISTA ESTADUAL DE APOIO AO CONTROLE EXTERNO
ÁREA: APOIO TÉCNICO-ADMINISTRATIVO
ESPECIALIDADE: TECNOLOGIA DA INFORMAÇÃO

Prova Discursiva – Questão 1

Aplicação: 22/11/2026

PADRÃO DE RESPOSTA

O PDTIC é o instrumento que vincula as necessidades de TIC aos objetivos institucionais fixados no PETI e no Plano Estratégico Institucional. Sua função é garantir o alinhamento das aquisições e soluções de TI às prioridades do órgão, assegurando a racionalização de recursos, a eficiência do gasto público, a transparência e a conformidade legal (Lei n.º 14.133/2021 e normas de governança digital públicas), evitando contratações isoladas, desnecessárias ou sem previsão orçamentária. Entre as providências administrativas e normativas de adequação, das quais o(a) candidato(a) deverá citar duas, estão as seguintes: i) sobrestamento da contratação – paralisar temporariamente a fase preparatória da licitação/contratação da solução SaaS do sistema; ii) elaboração ou revisão do PDTIC – iniciar imediatamente o processo de elaboração de novo PDTIC ou de revisão extraordinária do instrumento vencido para incluir a demanda estratégica do sistema; iii) alinhamento ao PCA – compatibilizar a contratação com o Plano de Contratações Anual (PCA) do órgão; iv) aprovação formal – submeter o PDTIC revisado/elaborado à apreciação e aprovação formal pelo comitê de governança digital (ou instância equivalente) do órgão.

A gestão de riscos e os requisitos de cibersegurança devem integrar compulsoriamente a fase de planejamento da contratação, fundamentando a elaboração do estudo técnico preliminar (ETP) e do termo de referência (TR). Em soluções em nuvem (SaaS), essa incorporação é crítica para identificar vulnerabilidades da infraestrutura do provedor, ameaças à confidencialidade dos dados do cidadão e riscos operacionais de indisponibilidade ou dependência tecnológica.

No que se refere aos papéis dos agentes, conforme a LGPD (Lei n.º 13.709/2018), classifica-se o órgão público Alfa como controlador, pois é a pessoa jurídica de direito público a quem competem as decisões essenciais referentes ao tratamento dos dados pessoais dos cidadãos. O provedor SaaS, por sua vez, é classificado como operador, pois é a pessoa jurídica que realiza o tratamento de dados pessoais em nome e sob as instruções do controlador, executando o processamento e o armazenamento na solução de nuvem.

QUESITOS AVALIADOS

Quesito 2.1 – PDTIC e providências administrativas
Conceito 0 – Não abordou o quesito ou o fez de forma totalmente equivocada.
Conceito 1 – Abordou o quesito de forma superficial ou parcial, apenas citando a função do PDTIC genericamente sem explicar seu papel tático junto ao PETI/objetivos institucionais, ou apenas mencionando que o PDTIC precisava ser atualizado, sem detalhar as providências formais.
Conceito 2 – Abordou o quesito de forma incompleta, explicando adequadamente a função do PDTIC, mas citando apenas uma providência a ser tomada.
Conceito 3 – Abordou o quesito de forma completa, explicando adequadamente a função do PDTIC e citando pelo menos duas providências a serem tomadas.

Quesito 2.2 – Gestão de riscos e cibersegurança
Conceito 0 – Não abordou o quesito ou o fez de forma totalmente equivocada.
Conceito 1 – Abordou o quesito de forma vaga ou genérica, apenas mencionando que a gestão de riscos e a cibersegurança são relevantes, mas sem relacioná-las à etapa do planejamento e nem à contratação em questão.
Conceito 2 – Abordou o quesito de forma incompleta, abordando adequadamente a importância da gestão de riscos e da cibersegurança na etapa de planejamento, mas sem relacioná-las à contratação em questão.
Conceito 3 – Abordou o quesito de forma completa, abordando adequadamente a importância da gestão de riscos e da cibersegurança na etapa de planejamento e relacionando-as à contratação em questão.

Quesito 2.3 – Papéis dos agentes de tratamento de dados segundo a LGPD
Conceito 0 – Não abordou o quesito ou o fez de forma totalmente equivocada.
Conceito 1 – Identificou corretamente apenas o papel de um dos agentes.
Conceito 2 – Identificou corretamente o papel de ambos os agentes.

Cebraspe
Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos

TRIBUNAL DE CONTAS DO ESTADO DO MARANHÃO (TCE/MA)

CARGO 10: ANALISTA ESTADUAL DE APOIO AO CONTROLE EXTERNO
ÁREA: APOIO TÉCNICO-ADMINISTRATIVO
ESPECIALIDADE: TECNOLOGIA DA INFORMAÇÃO

Prova Discursiva – Questão 2

Aplicação: 22/11/2026

PADRÃO DE RESPOSTA

O paradigma adequado ao treinamento inicial do modelo em questão é o aprendizado não supervisionado. Como nenhum registro histórico está identificado como legítimo ou indevido, não é possível treinar um classificador supervisionado. O modelo deve aprender o padrão predominante dos acessos e sinalizar como atípicos aqueles que se afastam desse padrão. Entre os algoritmos aplicáveis à detecção de anomalias estão o *isolation forest*, o *local outlier factor* (LOF), o *one-class* SVM e o *autoencoder*.

A precisão (*precision*) corresponde aos verdadeiros positivos sobre o total de alertas, ou seja, 36/2.000 = 0,018 (1,8%). A revocação (*recall*) corresponde aos verdadeiros positivos sobre o total de acessos indevidos, ou seja, 36/40 = 0,90 (90%). O modelo detecta quase todos os acessos indevidos, mas 1.964 dos 2.000 alertas são falsos positivos. Elevar o limiar de decisão reduz o número de alertas. Com isso, a precisão tende a aumentar, porque permanecem sinalizados os acessos de pontuação mais extrema, enquanto o *recall* diminui ou, no máximo, se mantém, porque parte dos acessos indevidos deixa de ultrapassar o limiar. O ajuste do limiar representa um compromisso entre precisão e *recall*.

O tipo adequado é a explicação local. Cada alerta corresponde a uma decisão individual, e a equipe de segurança precisa saber quais atributos levaram aquele acesso específico a receber pontuação elevada, por exemplo horário incomum, endereço de origem novo ou quantidade de registros muito acima do habitual para o usuário. A explicação global descreve o comportamento geral do modelo e os atributos mais relevantes no conjunto dos dados, mas não justifica um caso particular. Entre as técnicas capazes de fornecer explicação local estão o SHAP (valores de Shapley) e o LIME.

QUESITOS AVALIADOS

Quesito 2.1 – Paradigma de aprendizado de máquina e algoritmos
Conceito 0 – Não abordou o quesito ou o fez de forma totalmente equivocada.
Conceito 1 – Apresentou corretamente apenas um dos seguintes elementos: (i) indicação do paradigma não supervisionado, semissupervisionado ou autossupervisionado, justificada pela ausência de dados rotulados para o treinamento; (ii) um exemplo de algoritmo aplicável à detecção de anomalias; (iii) outro exemplo de algoritmo aplicável à detecção de anomalias.
Conceito 2 – Apresentou corretamente apenas dois dos elementos enumerados.
Conceito 3 – Apresentou corretamente os três elementos enumerados.

Quesito 2.2 – Precisão, revocação e efeito do limiar de decisão
Conceito 0 – Não abordou o quesito ou o fez de forma totalmente equivocada.
Conceito 1 – Apresentou corretamente apenas um dos seguintes elementos: (i) precisão correta; (ii) revocação correta; (iii) indicação de que a elevação do limiar reduz o número de alertas; (iv) indicação de que a elevação do limiar aumenta ou tende a aumentar a precisão; (v) indicação de que a elevação do limiar reduz ou não aumenta a revocação.
Conceito 2 – Apresentou corretamente apenas dois dos elementos enumerados.
Conceito 3 – Apresentou corretamente apenas três dos elementos enumerados.
Conceito 4 – Apresentou corretamente apenas quatro dos elementos enumerados.
Conceito 5 – Apresentou corretamente os cinco elementos enumerados.

Quesito 2.3 – Tipo de explicação e técnicas de explicabilidade
Conceito 0 – Não abordou o quesito ou o fez de forma totalmente equivocada.
Conceito 1 – Apresentou corretamente apenas um dos seguintes elementos: (i) indicação da explicação local, justificada pela necessidade de compreender a decisão sobre cada alerta individual; (ii) primeiro exemplo de técnica de explicação local; (iii) segundo exemplo de técnica de explicação local.
Conceito 2 – Apresentou corretamente apenas dois dos elementos.
Conceito 3 – Apresentou corretamente os três elementos.