- Nesta prova, faça o que se pede, usando, caso deseje, o espaço para rascunho indicado no presente caderno. Em seguida, transcreva o texto para o **CADERNO DE TEXTO DEFINITIVO DA PROVA DISCURSIVA**, no local apropriado, pois **não será avaliado fragmento de texto escrito em local indevido**.
- Qualquer fragmento de texto além da extensão máxima de linhas disponibilizadas será desconsiderado.
- No **Caderno de Texto Definitivo**, a presença de qualquer marca identificadora nos espaços destinados à transcrição dos textos definitivos acarretará a anulação da sua prova discursiva. Caso queira assinar o texto de sua peça de natureza técnica, utilize apenas o nome **Analista de Apoio ao Controle Externo**. Ao texto que contenha outra forma de assinatura será atribuída nota zero, correspondente à identificação do candidato em local indevido.
- Na peça de natureza técnica, ao domínio do conteúdo serão atribuídos até **20,00 pontos**, dos quais até **1,00 ponto** será atribuído ao quesito apresentação (legibilidade, respeito às margens e indicação de parágrafos) e estrutura textual (organização das ideias em texto estruturado). Em cada uma das questões discursivas, esses valores corresponderão a **10,00 pontos** e **0,50 ponto**, respectivamente.

-- PROVA DISCURSIVA --

Peça técnica

Em procedimento de fiscalização realizado por certo tribunal de contas estadual em uma secretaria do mesmo estado, a equipe de auditoria avaliou a governança e a gestão de tecnologia da informação (TI), considerando a relevância dos serviços digitais para a execução das políticas públicas e a materialidade dos investimentos realizados. A fiscalização identificou os seguintes achados.

Achado 1 – As decisões relativas aos investimentos em TI são tomadas predominantemente pela unidade técnica de tecnologia, sem participação sistemática da alta administração. Embora exista Plano Diretor de Tecnologia da Informação (PDTI), não foram evidenciados mecanismos formais que demonstrem a vinculação entre os investimentos priorizados, os objetivos estratégicos institucionais e os benefícios esperados. Também não há instância colegiada responsável por avaliar prioridades, direcionar a aplicação dos recursos de TI e acompanhar os resultados obtidos.

Achado 2 – A secretaria mantém diversos contratos, sistemas e projetos de TI, porém não adota processo institucionalizado para avaliação integrada dos benefícios, riscos e recursos envolvidos nas decisões de tecnologia. Projetos relevantes continuam recebendo recursos mesmo diante de atrasos, elevação de custos e redução dos benefícios inicialmente previstos. Os relatórios encaminhados à alta administração concentram-se em indicadores operacionais, como disponibilidade de serviços e quantidade de chamados atendidos, sem indicadores relacionados à realização de benefícios, otimização de riscos e utilização dos recursos.

Achado 3 – A auditoria constatou sobreposição de atribuições entre a alta administração e a unidade de TI. Decisões de natureza estratégica são delegadas à área técnica, enquanto gestores superiores participam diretamente de decisões operacionais relativas à execução de projetos e à configuração de serviços. Não foram formalmente estabelecidos papéis, responsabilidades e mecanismos de prestação de contas relativos à governança de TI, tampouco processo periódico pelo qual a alta administração avalie, direcione e monitore o uso atual e futuro da tecnologia.

Considerando a situação hipotética apresentada, elabore, com fundamento no COBIT 2019 e na ISO/IEC 38500, parecer técnico acerca dos achados apontados pela equipe de auditoria do tribunal de contas em questão. Em seu parecer, atenda ao que se pede a seguir: (i) analise os achados 1 e 2 à luz do COBIT 2019, estabelecendo distinção técnica entre governança e gestão de TI, e relacionando as deficiências identificadas aos objetivos do domínio EDM (*evaluate, direct and monitor*) pertinentes à estrutura de governança, entrega de benefícios, otimização de riscos e otimização de recursos; (ii) examine o achado 3 à luz da ISO/IEC 38500, abordando a responsabilidade do órgão de governança pelo uso da TI e a aplicação das funções de avaliar, direcionar e monitorar, bem como a adequada delimitação das responsabilidades entre o órgão de governança e a gestão; (iii) indique as principais recomendações a serem expedidas pelo tribunal de contas ao órgão jurisdicionado, com vistas ao fortalecimento da governança, da responsabilização, do monitoramento e da geração de valor pelo uso da tecnologia da informação.

PEÇA TÉCNICA – RASCUNHO 1/2

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	

RASCUNHO

PEÇA TÉCNICA – RASCUNHO 2/2

31	
32	
33	
34	
35	
36	
37	
38	
39	
40	
41	
42	
43	
44	
45	
46	
47	
48	
49	
50	
51	
52	
53	
54	
55	
56	
57	
58	
59	
60	

RASCUNHO

Questão 1

O órgão público federal Alfa, entidade responsável pela gestão de serviços públicos essenciais de seguridade e assistência social, deu início à fase preparatória para a contratação de uma solução de *software* como serviço (*Software as a Service* – SaaS) em ambiente de nuvem. Denominada Sistema Integrado de Atendimento ao Cidadão (SIAC), a plataforma visa unificar e digitalizar o atendimento em âmbito nacional, tratando dados pessoais e dados pessoais sensíveis de cidadãos.

Na avaliação preliminar de governança e conformidade do processo administrativo, foram identificadas as seguintes inconformidades críticas:

(a) **desalinhamento estratégico e orçamentário –** a aquisição da solução SaaS/SIAC não possui previsão no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) do órgão Alfa, que se encontra vencido desde o exercício passado, inexistindo documento formal vigente aprovado pelo comitê de governança digital que respalde a necessidade da contratação;

(b) **ausência de análise de riscos e de requisitos de cibersegurança –** o processo não conta com gerenciamento de riscos da contratação na fase de planejamento. O estudo técnico preliminar (ETP) e a minuta do termo de referência (TR) omitiram a especificação de requisitos de segurança da informação, controles de cibersegurança e garantias de continuidade de negócios para o prestador de serviços em nuvem;

(c) **inconformidade com o regime de proteção de dados pessoais –** o termo de referência cita apenas de forma genérica a observância à Lei Geral de Proteção de Dados Pessoais (LGPD – Lei n.º 13.709/2018), sem delimitar os papéis operacionais dos agentes de tratamento, sem exigir o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e sem prever cláusulas específicas para a gestão de incidentes de segurança.

A partir da situação-problema apresentada, redija um texto dissertativo em atendimento ao que se pede a seguir.

1 Discorra sobre a função do PDTIC no planejamento estratégico de TI e no alinhamento das contratações aos objetivos institucionais, indicando duas providências administrativas e normativas a serem tomadas no caso apresentado diante da ausência de previsão da contratação e da desatualização do instrumento. [**valor: 3,50 pontos**]

2 Aborde a importância da gestão de riscos e da cibersegurança na etapa de planejamento da contratação em questão, explicando a criticidade da sua incorporação no caso de contratação de solução em nuvem (SaaS). [**valor: 3,00 pontos**]

3 Identifique, com base na LGPD, os papéis do órgão contratante e do provedor SaaS no tratamento dos dados pessoais, indicando a instância operadora e a instância controladora no caso apresentado. [**valor: 3,00 pontos**]

QUESTÃO 1 – RASCUNHO

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	

RASCUNHO

Questão 2

A unidade de tecnologia da informação de um tribunal de contas estadual implantou um modelo de inteligência artificial para identificar acessos atípicos ao banco de dados do sistema de processo eletrônico. A base histórica contém todos os acessos ao sistema, mas nenhum deles traz indicação de ter sido legítimo ou indevido, embora já se saiba que ocorreram consultas indevidas a processos sigilosos, realizadas com credenciais válidas. O modelo atribui a cada acesso uma pontuação de anomalia, tanto maior quanto mais atípico for o acesso, e emite um alerta quando ela ultrapassa um limiar de decisão.

Após o treinamento inicial, o modelo foi avaliado com os dados de um dia de operação, reservados para esse fim. Nesse dia, houve 500 mil acessos, e uma auditoria identificou exatamente 40 deles como indevidos. O modelo emitiu, nesse dia, 2.000 alertas, cada um referente a um acesso distinto. Desses alertas, 36 correspondiam a acessos indevidos. Os alertas são triados pela equipe de segurança, e cada um informa apenas a pontuação de anomalia, sem indicar os fatores que a determinaram.

Com base nas informações descritas na situação hipotética acima, redija um texto dissertativo atendendo, fundamentadamente, ao que se pede a seguir.

1 Indique, quanto ao uso de dados rotulados, o paradigma de aprendizado de máquina que seria adequado ao treinamento inicial do modelo em questão, e cite dois algoritmos desse paradigma aplicáveis à detecção de anomalias. [**valor: 3,00 pontos**]

2 Explique o cálculo dos indicadores *precision* e *recall* do modelo no dia de avaliação e indique o efeito esperado da elevação do limiar de decisão sobre o número de alertas e sobre cada uma dessas duas métricas. [**valor: 3,50 pontos**]

3 Indique o tipo de explicação (global ou local) mais adequado à triagem dos alertas no caso apresentado e cite duas técnicas capazes de fornecer esse tipo de explicação. [**valor: 3,00 pontos**]

QUESTÃO 2 – RASCUNHO

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	

RASCUNHO