

## LICITAÇÃO: ANEXO Nº ETP 6/2026 - APÊNDICE VI -/2026/ASSESSOR-DITEC/DITEC

Processo nº 00100.002198/2025-02

Interessado: CGISE

### APÊNDICE VI - ESPECIFICAÇÕES TÉCNICAS

#### **SOLUÇÃO DE GERENCIAMENTO DE SERVIÇOS DE TIC E PLATAFORMA DE OBSERVABILIDADE AVANÇADA COM IA PARA OPERAÇÕES DE TI (AIOPS)**

##### **1. CONTEXTUALIZAÇÃO**

1.1. A solução de gerenciamento de serviços de TIC atualmente em uso no ITI é o Open Source Ticket Request System (OTRS), mantida pela atual equipe de operação de infraestrutura. Contudo, diante das mudanças estratégicas e operacionais, não atende por completo às áreas e às atuais demandas do ITI, fazendo-se necessária a sua substituição no âmbito da nova contratação, não se admitindo o fornecimento da solução principal de ITSM na modalidade software como serviço (SaaS), ressalvadas as soluções expressamente admitidas em modalidade SaaS neste Apêndice — notadamente a Plataforma de Orquestração de Conhecimento com LLMs em Low-Code/LLMOps (seção 4).

1.2. É de conhecimento de todos que as soluções de gerenciamento de TIC comercializadas possuem diferentes variáveis de licenciamento ou subscrição, que podem incluir o número de usuários ou o número de atendentes, por exemplo, dentre outras.

1.3. Cabe ressaltar que, para os itens de serviço constantes da presente contratação, está prevista uma equipe mínima que poderá sofrer alterações face à necessidade de cumprimento do nível mínimo de serviço exigido, impactando no número de atendentes, que inclusive podem aumentar apenas de forma sazonal, em períodos em que a CONTRATADA entender que o ajuste dos seus profissionais seja necessário para alcance do INS.

1.4. Somado a isso, há a complexidade das parametrizações, customizações e automações necessárias e que deverão ser implementadas pela CONTRATADA ao longo do Contrato, que requerem o total conhecimento e domínio técnico e comercial da ferramenta, além, é claro, das permissões de evolução tecnológica e alterações na solução, que podem depender do tipo de licenciamento ou da política do fabricante do software.

1.5. O modelo adotado atualmente, em que a CONTRATADA é responsável pelo fornecimento, manutenção e evolução da solução ITSM, facilita a gestão para o ITI, não impacta nas fronteiras de responsabilidade que ocorre nos casos de múltiplos contratos e não requer a manutenção de um contrato adicional de suporte técnico e evolução somente para a solução.

1.6. Além disso, está sendo prevista nessa contratação a integração da solução de gerenciamento de TIC com o TEAMS e a criação de *chatbots* que possibilitarão que os usuários utilizem o mesmo canal para abertura e acompanhamento de chamados, otimizando o processo de demandas. Para essa condição, além do conhecimento técnico para a integração do TEAMS com a solução, também será necessário que a CONTRATADA tenha total conhecimento das especificidades dos serviços e seus respectivos INS, bem como da dinâmica das Equipes Técnicas, corroborando para a vantajosidade da manutenção do fornecimento da ferramenta pela mesma CONTRATADA dos serviços de operação da infraestrutura.

1.7. Para o correto dimensionamento da solução de gerenciamento de serviços de TIC, no que se refere à utilização pelo ITI, deverá estar compreendido o quantitativo de usuários discriminado no "Apêndice I - Infraestrutura de TIC", compreendendo servidores, terceirizados e parceiros do ITI. Cabe ressaltar que a quantidade de usuários atendentes previstas para o ITI são complementares às licenças que a CONTRATADA deverá prever para a sua equipe.

1.8. É de responsabilidade total da CONTRATADA a identificação e fornecimento do quantitativo e tipo de licenças necessários à execução dos serviços, devendo abranger todos os usuários do ITI.

## **2. REQUISITOS DA SOLUÇÃO DE ITSM**

2.1. A solução de software de *Information Technology Service Management (ITSM)* para Gerenciamento de Serviços de TIC e Conformidade deverá estar em conformidade com pelo menos 15 (quinze) da biblioteca de boas práticas ITIL v4, com no mínimo os requisitos listados abaixo, por se tratar das práticas cuja implantação estão previstas na presente contratação.

2.2. A Solução de ITSM e CONFORMIDADE poderá ser composta por uma ou mais ferramentas, desde que totalmente integradas e compatíveis entre si, e deverão ser providenciados todos os softwares e licenças necessários à execução dos serviços e completa implantação das disciplinas ITIL. Isto significa, por exemplo, que deve ser disponibilizada pela CONTRATADA ferramenta para inventário de ativos de TIC como resultado da implantação do processo de Gerenciamento de Ativos de TI.

2.3. No que tange aos processos ITIL v4, a solução deverá permitir a implantação de todos os processos ao longo do Contrato sem necessidade de aquisição de módulos complementares.

2.4. A solução poderá ser instalada na infraestrutura de TI no ITI deverá:

- I. Os serviços cadastrados devem permitir o vínculo com ativos suportados.
- II. Os serviços cadastrados devem permitir o vínculo do Cliente demandante do serviço.
- III. Os serviços cadastrados devem permitir o vínculo com contratos.
- IV. A solução deve fornecer aplicativo móvel com suporte para sistemas operacionais android e IOS, permitindo o acompanhamento do chamados e abertura de chamados através do aplicativo móvel.
- V. O aplicativo móvel deve estar nas lojas oficiais de suporte do Sistema

operacional Android Play Store e IOS App Store.

VI. VI - Ser fornecida com licenciamento perpetuo visando a continuidade do histórico do ITI.

- 2.4.1. Deve permitir a criação de um Relatório de Causa Raiz.
- 2.4.2. O relatório de Causa Raiz deve permitir o registro técnico da ocorrência.
- 2.4.3. O relatório de Causa Raiz deve permitir o registro de uma Solução de Contorno.
- 2.4.4. Deve possuir um formulário para registro de Mudanças.
- 2.4.5. A aplicação deve possuir módulo para emissão de relatórios e dashboards com indicadores triviais para a tomada de decisão da Gestão.
- 2.4.6. Deve permitir a vinculação entre indicadores e relatórios com atualização dinâmica de resultados. Os resultados devem ser exibidos em diversos níveis de detalhamento, permitindo a análise desde o desempenho global, parcial ou individual dos indicadores.
- 2.4.7. Deve possuir relatório que aponte a quantidade de chamado atendido por cada Analista.
- 2.4.8. A aplicação deve permitir, a autenticação de usuários via SSO (Single Sing On/Login único) de forma Segura.
- 2.4.9. A aplicação deve permitir a autenticação via tecnologia oAuth2.
- 2.4.10. Deve ser permitido a autenticação com uso da tecnologia oAuth2, utilizada em sistemas como o Microsoft Office365, Google, dentre outros.
- 2.4.11. Deve ser permitido aos administradores definirem domínios válidos para a autenticação via oAuth.
- 2.4.12. Deve ser bloqueado todo e qualquer acesso não configurado pelo administrador.
- 2.4.13. O sistema deve possibilitar o envio de notificações via whatsapp para usuários sobre atualizações em seus chamados.
- 2.4.14. O sistema deve possibilitar o envio de notificações via sistema Telegram para usuários sobre atualizações em seus chamados.
- 2.4.15. O sistema deve possibilitar o envio de notificações via sistema Microsoft Teams
- 2.4.16. A SOLUÇÃO deverá ser aplicação web multiusuário e multiorganização, composta por interface de página única, camada de serviço (API) e banco de dados relacional, acessível por navegador sem instalação de cliente nas estações.
- 2.4.17. A SOLUÇÃO deverá ser instalada na infraestrutura do CONTRATANTE, próprio, com operação integral em rede fechada, sem exigir saída para a internet e sem tráfego de dados de atendimento para serviços de terceiros.
- 2.4.18. A SOLUÇÃO deverá dispor de instalador completo para sistemas operacionais Windows e macOS, contemplando aplicação, tempo de execução, banco de dados e registro dos serviços em pacote único, admitida implantação assistida em Linux ou em contêineres.
- 2.4.19. A SOLUÇÃO deverá operar, em sua totalidade, incluindo banco de dados e o componente de inteligência artificial, sobre um único servidor de porte padrão, dispensando parque dedicado de servidores.
- 2.4.20. O licenciamento da SOLUÇÃO não poderá ser vinculado à quantidade de

atendentes, agentes ou usuários nomeados, de modo que a ampliação da equipe de atendimento não implique acréscimo de valor.

2.4.21. A SOLUÇÃO não poderá depender, para seu funcionamento, de licença adicional, módulo pago à parte, complemento ou serviço em nuvem de terceiros, devendo a integração com sistemas externos ser opcional e não condicionante da operação.

2.4.22. A interface da SOLUÇÃO, suas mensagens e sua documentação deverão estar integralmente em português do Brasil.

2.4.23. A SOLUÇÃO deverá oferecer filtros globais de período e de organização aplicáveis às telas de análise, alternância entre tema claro e escuro e exportação de relatórios em formato PDF.

2.4.24. As telas de operação deverão dispor de atualização automática de dados em intervalo configurável, não superior a 30 segundos no menor intervalo disponível.

2.4.25. A SOLUÇÃO deverá registrar chamados classificados, no mínimo, como incidente e como requisição de serviço, mantendo a distinção ao longo de todo o ciclo de vida e na apuração contratual.

2.4.26. A prioridade do chamado deverá ser calculada automaticamente pelo cruzamento de urgência e impacto em matriz 5x5, vedada a digitação direta do campo prioridade pelo usuário.

2.4.27. A SOLUÇÃO deverá aceitar a abertura de chamados por, no mínimo, quatro canais: console do atendente, portal de autoatendimento, mensagem de correio eletrônico e rotina programada, todos alimentando a mesma fila e sujeitos às mesmas regras.

2.4.28. A SOLUÇÃO deverá permitir o anexo de imagens, vídeos e documentos na abertura e durante o atendimento, com controle de acesso ao download.

2.4.29. A SOLUÇÃO deverá permitir o agendamento de data e hora desejadas para o início do atendimento no momento da abertura.

2.4.30. O ciclo de vida do chamado deverá contemplar, no mínimo, os estados novo, em atendimento, aguardando atendimento, pendente, encaminhado a fornecedor, solucionado e fechado, com transições controladas pela própria SOLUÇÃO, vedado o salto de etapas.

2.4.31. A SOLUÇÃO deverá dispor de mecanismo de captura que impeça o atendimento simultâneo do mesmo chamado por mais de um atendente, com possibilidade de devolução do chamado à fila.

2.4.32. O chamado deverá manter registro segregado de acompanhamentos, tarefas, solução, anexos e histórico, sendo o histórico imutável e integralmente auditável.

2.4.33. A SOLUÇÃO deverá oferecer modelos de acompanhamento que padronizem as respostas ao solicitante.

2.4.34. A SOLUÇÃO deverá permitir o escalonamento do chamado entre níveis de atendimento, no mínimo primeiro, segundo e terceiro níveis, especialista e coordenação, com motivo obrigatório, troca de grupo responsável e registro em linha do tempo.

2.4.35. O "pendenciamento" de chamado deverá exigir justificativa, permitir lembrete de retomada e suspender a contagem do prazo de nível de serviço enquanto perdurar a pendência.

2.4.36. A SOLUÇÃO deverá permitir o encaminhamento do chamado a fornecedor externo, com registro do protocolo do terceiro e status próprio visível na fila.

2.4.37. O encerramento técnico do chamado deverá exigir o registro da solução, com classificação do tipo de solução e evidências, facultada a publicação do conteúdo na base de conhecimento.

2.4.38. Após a solução, a SOLUÇÃO deverá abrir prazo para avaliação e reabertura pelo solicitante, com fechamento automático ao término do prazo, tudo registrado na linha do tempo.

2.4.39. A SOLUÇÃO deverá medir separadamente o tempo ativo e o tempo suspenso de cada chamado, refletindo a segregação nos indicadores e na apuração contratual.

2.4.40. A SOLUÇÃO deverá controlar, no mínimo, dois prazos por chamado: tempo para primeiro atendimento e tempo para resolução.

2.4.41. A SOLUÇÃO deverá diferenciar acordos de nível de serviço firmados com o contratante, acordos internos entre equipes e acordos de apoio firmados com fornecedores.

2.4.42. As metas de prazo deverão ser parametrizáveis por prioridade e por item do catálogo de serviços, admitida meta específica por organização contratante, com precedência sobre o padrão do catálogo.

2.4.43. A SOLUÇÃO deverá suportar regime de cobertura ininterrupta e regime de horário útil, este último apoiado em calendário com faixas de expediente por dia da semana, fuso horário e cadastro de feriados.

2.4.44. A contagem do prazo deverá ser suspensa enquanto o chamado depender de terceiro, retomando a contagem na volta ao atendimento.

2.4.45. A SOLUÇÃO deverá sinalizar o risco de descumprimento do prazo em faixas objetivas e utilizar o mesmo critério de cálculo em painéis de operação, painéis gerenciais e apuração contratual.

2.4.46. Ao esgotar-se o prazo de resolução, a SOLUÇÃO deverá elevar automaticamente o chamado ao nível de atendimento seguinte, notificar os canais configurados e registrar o evento de forma durável.

2.4.47. A SOLUÇÃO deverá dispor de motor de regras próprio, configurável por administrador sem desenvolvimento, com condições sobre título, descrição, organização, origem, requerente, localidade e setor, admitidos operadores de conteúdo, igualdade, prefixo e expressão, combináveis por conjunção e disjunção.

2.4.48. As regras deverão poder definir categoria, prioridade, tipo, grupo técnico, nível de atendimento, acordo de nível de serviço e responsável pelo chamado.

2.4.49. A SOLUÇÃO deverá permitir ordenar a avaliação das regras, interromper o processamento a partir de determinada regra e restringir o escopo de aplicação por unidade organizacional.

2.4.50. A SOLUÇÃO deverá dispor de simulador que permita testar as regras configuradas sem criar chamado real.

2.4.51. A SOLUÇÃO deverá permitir a abertura automática de chamados em periodicidade programada, com frequência diária, semanal ou mensal, hora definida e exibição da próxima execução.

2.4.52. A SOLUÇÃO deverá abrir chamados automaticamente a partir de caixa

de correio eletrônico monitorada e converter em acompanhamento a resposta que contenha o número do chamado.

2.4.53. A SOLUÇÃO deverá notificar as movimentações do chamado por correio eletrônico, por ferramenta corporativa de mensageria e por aviso interno, com roteamento por nível de atendimento.

2.4.54. A SOLUÇÃO deverá encerrar automaticamente o chamado solucionado cujo prazo de manifestação do solicitante tenha decorrido, registrando o fechamento.

2.4.55. A SOLUÇÃO deverá dispor de gestão de problemas, com registro de causa raiz, erro conhecido e solução de contorno, controle de estados até a eliminação definitiva e vínculo bidirecional com os incidentes de origem.

2.4.56. A SOLUÇÃO deverá dispor de gestão de mudanças, com classificação em normal, padrão e emergencial, planos de implantação e de reversão obrigatórios e vínculo aos itens de configuração afetados.

2.4.57. As mudanças deverão submeter-se a comitê de aprovação, com quórum mínimo parametrizável, sem o qual a mudança não avança.

2.4.58. A SOLUÇÃO deverá dispor de gestão de liberação, com versão, janela e lista de verificação, admitindo na composição do pacote apenas mudanças previamente aprovadas pelo comitê.

2.4.59. A SOLUÇÃO deverá registrar a implantação por ambiente, no mínimo desenvolvimento, homologação, pré-produção e produção, com status e reversão registrados por ambiente.

2.4.60. A SOLUÇÃO deverá apurar a disponibilidade por serviço e por item de configuração, calculando percentual de disponibilidade, número de falhas, tempo indisponível, tempo médio entre falhas e tempo médio de recuperação, com registro das janelas de indisponibilidade e emissão de relatório do período.

2.4.61. A SOLUÇÃO deverá dispor de catálogo de serviços organizado por grupos, contendo por oferta a categoria, o tipo, o acordo de nível de serviço aplicável e a elegibilidade de nível de atendimento, com roteamento automático da solicitação.

2.4.62. A SOLUÇÃO deverá permitir a criação de modelos de chamado com campos pré-preenchidos, obrigatórios e ocultos, aplicáveis por precedência entre categoria, perfil, unidade e padrão geral.

2.4.63. A SOLUÇÃO deverá registrar oportunidades de melhoria contínua, com origem rastreada, prioridade, responsável, benefício esperado quantificado e fluxo de status até a conclusão.

2.4.64. A SOLUÇÃO deverá manter cadastro de fornecedores e de contratos de apoio, com vigência e valor mensal, e controle de licenças de software vinculadas aos ativos.

2.4.65. A SOLUÇÃO deverá registrar riscos do serviço, avaliados por probabilidade e impacto, com tratamento e acompanhamento.

2.4.66. A SOLUÇÃO deverá manter inventário de itens de configuração com tipo, fabricante, número de série, número de Patrimônio, localidade e contrato.

2.4.66.1. A SOLUÇÃO deve permitir atrelar o contrato ao item/ativo registrado, permitir gerar QR CODE com identificação para cada item registrado de forma individual, permitindo controle e abertura de chamado através do QR CODE do dispositivo.

2.4.66.2. Deve ser permitido impressão da tag individual ou em massa, para ser inserido no ativo físico.

2.4.67. Os itens de configuração deverão ter ciclo de vida controlado, contemplando ao menos os estados novo, em uso, em estoque, em reparo e baixado.

2.4.68. A SOLUÇÃO deverá registrar relacionamentos entre itens de configuração, contemplando ao menos as relações de dependência, conexão, execução, hospedagem e composição, para avaliação de impacto.

2.4.69. Cada item de configuração deverá possuir linha do tempo com histórico de eventos, incluindo as indisponibilidades registradas.

2.4.70. A SOLUÇÃO deverá vincular itens de configuração a chamados, problemas e mudanças.

2.4.71. A SOLUÇÃO deverá dispor de base de conhecimento com fluxo de aprovação em três estados, organização por categoria, busca, contador de visualizações e marcação de conteúdo público para o portal.

2.4.72. A SOLUÇÃO deverá permitir a publicação de artigo na base de conhecimento diretamente a partir do registro de solução do chamado.

2.4.73. A SOLUÇÃO deverá registrar a aprovação, pelo CONTRATANTE, dos procedimentos operacionais publicados, servindo o registro como evidência de homologação.

2.4.74. A SOLUÇÃO deverá dispor de painel de monitoração contínua que exiba apenas os chamados que demandam ação, segregados em recortes de aguardando captura, prazo vencido, prazo em iminência de vencimento, prazo em alerta e prazo suspenso.

2.4.75. O painel de monitoração deverá dispor de modo de exibição em tela cheia para projeção na central, atualização automática e busca por número, organização ou responsável.

2.4.76. O painel de monitoração deverá dispor de alerta sonoro para novos eventos críticos, destinado à operação em regime de plantão.

2.4.77. A SOLUÇÃO deverá dispor de quadro visual de fluxo de trabalho, organizado por estado, com limite de trabalho em andamento configurável por coluna, sinalização de excedente e movimentação do cartão por arrastar e soltar.

2.4.78. A SOLUÇÃO deverá calcular métricas de fluxo, contemplando ao menos tempo total de atendimento, tempo sob responsabilidade da equipe e eficiência de fluxo, apresentando média e mediana.

2.4.79. A fila de chamados deverá dispor de painel de acompanhamento calculado sobre todo o conjunto filtrado e de filtros por estado, tipo, prioridade, organização, responsável e período.

2.4.80. A SOLUÇÃO deverá dispor de painel executivo consolidado, contendo ao menos volume, chamados em aberto, tempo médio de primeiro atendimento, tempo médio de resolução, cumprimento de prazo, satisfação e tendência de abertos contra resolvidos.

2.4.81. A SOLUÇÃO deverá dispor de painel operacional com indicadores-chave, feed de alertas com registro de escalonamento, visão consolidada por organização e controle do prazo de resolução.

2.4.82. Os indicadores apresentados nos painéis deverão ser navegáveis, permitindo abrir a relação dos chamados que compõem cada número.

- 2.4.83. A SOLUÇÃO deverá apresentar o desempenho do atendimento por prioridade, por nível de equipe, por atendente e por satisfação do solicitante, com evolução mensal contra a meta.
- 2.4.84. A SOLUÇÃO deverá apresentar a distribuição da demanda no tempo, contemplando o envelhecimento dos chamados em aberto por faixa de espera, o volume resolvido por semana e a concentração por dia da semana e hora do dia.
- 2.4.85. A SOLUÇÃO deverá permitir a análise individual do atendente, com tempos de atendimento, proporção entre tempo ativo e suspenso e distribuição por prioridade, admitida a comparação entre atendentes com correção estatística por volume de amostra.
- 2.4.86. A SOLUÇÃO deverá apresentar, por organização contratante, o volume e a qualidade do atendimento confrontados com o custo apurado e a receita do contrato, com classificação automática da saúde contratual.
- 2.4.87. A SOLUÇÃO deverá apurar o custo do atendimento a partir de custo cadastrado por nível de atendimento e de custo individual por atendente, prevalecendo o custo individual quando existente.
- 2.4.88. A SOLUÇÃO deverá permitir a parametrização, por administrador e sem desenvolvimento, das faixas que classificam a carga de trabalho do atendente.
- 2.4.89. A SOLUÇÃO deverá oferecer análise de correlação entre as séries históricas da operação e representação gráfica dos relacionamentos entre chamados, organizações, atendentes, ativos e serviços.
- 2.4.90. A SOLUÇÃO deverá emitir relatórios em formato PDF, em modelo institucional, respeitando os filtros de período e organização aplicados na tela.
- 2.4.91. A SOLUÇÃO deverá calcular e apresentar, no mínimo, os indicadores de chamados em aberto, tempo médio de primeiro atendimento, tempo médio de resolução, cumprimento de prazo, satisfação, envelhecimento, volume resolvido, tempo total, tempo sob responsabilidade da equipe, eficiência de fluxo, disponibilidade e tempo suspenso.
- 2.4.92. A SOLUÇÃO deverá dispor de instrumento de medição de resultado nativo, com indicadores configuráveis por contrato, contemplando ao menos cumprimento do prazo de solução, cumprimento do prazo de resposta, chamados em aberto, satisfação e tempo médio de resolução.
- 2.4.93. Cada indicador do instrumento de medição deverá admitir meta e peso, devendo a soma dos pesos totalizar cem por cento.
- 2.4.94. A SOLUÇÃO deverá calcular o desconto por descumprimento a partir de faixas parametrizáveis por indicador, apresentando a glosa ponderada, o valor do desconto e o valor líquido a pagar na competência.
- 2.4.95. A apuração deverá ser calculada diretamente sobre os chamados efetivamente registrados na competência, vedada a alimentação manual dos resultados.
- 2.4.96. A SOLUÇÃO deverá admitir modelo alternativo de apuração por pontuação de ocorrências de inadimplemento, com conversão em percentual de desconto, teto configurável e fatores de aplicação progressiva em período de estabilização.
- 2.4.97. A medição da competência deverá ser exportável em formato PDF, apta a instruir o processo de pagamento.
- 2.4.98. A SOLUÇÃO deverá registrar Ordens de Serviço por contrato, com controle de status até o faturamento.

- 2.4.99. A SOLUÇÃO deverá suportar a medição por resultado e a fiscalização contratual nos termos da Lei nº 14.133/2021 e da IN SGD/ME nº 94/2022, registrando a execução e mantendo trilha para prestação de contas.
- 2.4.100. A SOLUÇÃO deverá dispor de perfis de uso distintos, contemplando ao menos administração, atendimento pleno, atendimento com escopo reduzido, consulta gerencial, gestão pelo contratante e solicitante.
- 2.4.101. Além do perfil de uso, a SOLUÇÃO deverá permitir a composição de perfis de acesso por página, devendo a restrição ser aplicada também na camada de serviço, de modo que o acesso negado não possa ser obtido por endereço direto.
- 2.4.102. A SOLUÇÃO deverá restringir a visibilidade dos dados por organização e por unidade organizacional, admitindo visão consolidada apenas aos perfis autorizados.
- 2.4.103. A SOLUÇÃO deverá suportar autenticação em dois fatores, com códigos de recuperação.
- 2.4.104. A SOLUÇÃO deverá exigir a troca de senha no primeiro acesso do usuário.
- 2.4.105. As credenciais de integração com sistemas externos deverão ser armazenadas de forma cifrada.
- 2.4.106. A SOLUÇÃO deverá manter trilha de auditoria das ações administrativas, classificada por sensibilidade e consultável por período, usuário e tipo de ação.
- 2.4.107. O histórico de cada chamado deverá ser imutável, complementando a trilha de auditoria da plataforma.
- 2.4.108. Em ambiente que atenda a mais de uma organização, a SOLUÇÃO deverá isolar os dados de cada uma em base própria.
- 2.4.109. A SOLUÇÃO deverá dispor de fluxo de solicitação de acesso pelo próprio interessado, submetido a aprovação do administrador, com vinculação à organização correta e senha temporária de exibição única.
- 2.4.110. A SOLUÇÃO deverá permitir a marcação do chamado que contenha dados pessoais, com registro da base legal e da finalidade do tratamento.
- 2.4.111. A SOLUÇÃO deverá registrar e controlar as solicitações de titular de dados previstas no art. 18 da Lei nº 13.709/2018, com controle do prazo legal de resposta.
- 2.4.112. A SOLUÇÃO deverá executar a anonimização de chamados encerrados, preservando o registro operacional necessário à estatística contratual.
- 2.4.113. A SOLUÇÃO deverá dispor de política de retenção e identificar os registros elegíveis a expurgo.
- 2.4.114. O tratamento dos dados deverá ocorrer exclusivamente na infraestrutura do CONTRATANTE, sem transferência de conteúdo de atendimento a terceiros, inclusive quanto a recursos de inteligência artificial.
- 2.4.115. A SOLUÇÃO deverá oferecer assistente de consulta em linguagem natural, em português, disponível ao atendente em qualquer tela do console e ao solicitante no portal.
- 2.4.116. O processamento do assistente deverá ocorrer na infraestrutura do CONTRATANTE, sem envio de conteúdo de chamados a serviços externos e sem cobrança por consulta.
- 2.4.117. O assistente deverá permanecer operante em ambiente sem saída para a internet.

- 2.4.118. A SOLUÇÃO deverá dispor de portal de autoatendimento apartado do console de atendimento, no qual o solicitante abra, acompanhe, avalie e reabra seus chamados.
- 2.4.119. O portal deverá permitir a abertura de chamado por texto livre e por seleção de oferta do catálogo de serviços, com anexo de arquivos.
- 2.4.120. O portal deverá restringir a visibilidade dos chamados ao próprio solicitante, admitida visão de todos os chamados da organização ao perfil de gestão do CONTRATANTE.
- 2.4.121. O portal deverá disponibilizar consulta à base de conhecimento pública e emissão, pelo próprio solicitante, de relatório de seus chamados no período.
- 2.4.122. O portal deverá permitir a avaliação do atendimento em escala numérica e a reabertura do chamado dentro do prazo definido, alimentando o indicador de satisfação do contrato.
- 2.4.123. A SOLUÇÃO deverá importar o histórico de chamados de ferramenta anterior a partir de arquivos em formato CSV, XLS ou XLSX, com mapeamento de colunas conferível e pré-visualização antes da gravação.
- 2.4.124. A importação deverá preservar a data original de abertura e o número de origem de cada chamado.
- 2.4.125. A importação deverá normalizar estado, prioridade e tipo, tornando o histórico pesquisável e integrado aos indicadores desde a entrada em produção.
- 2.4.126. Os dados deverão residir em banco sob guarda do CONTRATANTE, com exportação em formato estruturado, vedada qualquer forma de retenção que dificulte a substituição da SOLUÇÃO.
- 2.4.127. A SOLUÇÃO deverá dispor de painel de conformidade que relacione as práticas de gestão de serviços adotadas e as normas de governança de referência, apontando, para cada item, a tela que comprova o atendimento.
- 2.4.128. O painel de conformidade deverá contemplar, no mínimo, as referências ITIL 4, ISO/IEC 20000, COBIT, práticas de fluxo enxuto, gestão de conhecimento centrada em solução, ISO 9001 e ISO/IEC 27001 e 27701, além das normas de contratação pública aplicáveis.
- 2.4.129. A CONTRATADA deverá entregar documentação de uso completa, em português, cobrindo todos os módulos da SOLUÇÃO, do primeiro acesso à apuração contratual, com indicação do caminho de menu e do passo a passo de cada tarefa.
- 2.4.130. A CONTRATADA deverá capacitar as equipes de atendimento de primeiro a terceiro nível e disponibilizar o portal aos solicitantes na entrada em produção, com operação assistida no período inicial.
- 2.4.131. A CONTRATADA deverá realizar prova de conceito na infraestrutura do CONTRATANTE, por período determinado, com dados reais de contrato ou área piloto, previamente à aceitação definitiva.
- 2.4.132. A documentação deverá contemplar as rotinas operacionais recomendadas em periodicidade diária, semanal e mensal, incluindo o fechamento da competência para fins de medição.
- 2.4.133. A sustentação da SOLUÇÃO, compreendendo suporte, correção de defeitos e disponibilização de novas versões, deverá ser de responsabilidade da CONTRATADA, sem transferência a comunidade de usuários ou a terceiros.
- 2.4.134. A SOLUÇÃO deve disponibilizar painéis de monitoramento de status de chamado para monitoria e acompanhamento, com indicadores e alertas, permitindo

interação direto pela pagina de monitoria.

### **3. PLATAFORMA DE MONITORAMENTO AVANÇADO COM IA PARA OPERAÇÕES DE TI - DISPOSIÇÕES GERAIS**

3.1. A solução deverá ser implantada em ambiente de nuvem pública, privada ou híbrida, sob responsabilidade da CONTRATANTE, devendo:

- I. Suportar arquitetura distribuída e escalável horizontalmente (scale-out), com balanceamento automático de carga entre componentes;
- II. Garantir isolamento lógico e segurança dos dados, independentemente do modelo de implantação;
- III. Permitir operação em ambientes híbridos, com coleta e processamento de dados provenientes de múltiplas regiões e provedores;
- IV. Suportar alta disponibilidade nativa, com mecanismos de failover automático entre instâncias;
- V. Garantir continuidade operacional mesmo em caso de falha de componentes individuais da plataforma.
- VI. Admitir a implantação em rede fechada, sem saída para a internet, hipótese em que a coleta e a execução remota se darão por componente instalado no ambiente da CONTRATANTE.

#### **3.2. Escalabilidade e Performance**

- I. Suportar crescimento progressivo do volume de dados (métricas, logs, eventos e traces) sem degradação perceptível de desempenho;
- II. Permitir expansão de capacidade de processamento e armazenamento sem necessidade de interrupção do serviço;
- III. Operar com baixa latência na ingestão e análise de dados, permitindo processamento em tempo real ou próximo ao tempo real;
- IV. Garantir desempenho consistente mesmo sob cenários de alta volumetria de eventos e métricas.

#### **3.3. Licenciamento e Componentes**

- I. Todos os módulos, componentes, conectores, agentes, APIs e funcionalidades necessárias ao pleno atendimento dos requisitos desta especificação deverão estar contemplados na proposta técnico-financeira
- II. Não será admitida a necessidade de aquisição adicional de módulos, plugins ou extensões para atendimento dos requisitos técnicos descritos;
- III. A solução deverá possuir modelo de licenciamento unificado, evitando fragmentação entre componentes;
- IV. Eventuais limitações técnicas decorrentes de licenciamento deverão ser explicitadas na proposta.

#### **3.4. Controle de Acesso e Perfis**

- I. Prover acesso simultâneo a, no mínimo:
  - 100 (cem) usuários finais;
  - 20 (vinte) usuários com perfil de operação, administração ou resolução;
  - 05 (cinco) usuários com perfil analítico avançado.

- II. Permitir licenciamento não nominal, possibilitando o remanejamento dinâmico de usuários;
- III. Implementar controle de acesso baseado em papéis (RBAC), permitindo granularidade na definição de permissões;
- IV. Permitir segregação de funções entre usuários, garantindo aderência a boas práticas de governança;
- V. Registrar logs de auditoria detalhados de acesso, incluindo:
  - a) identificação do usuário;
  - b) data e hora;
  - c) ações realizadas

### 3.5. **Interface e Experiência de Uso**

- I. Possuir interface 100% web, acessível via navegador, sem necessidade de instalação de componentes locais;
- II. Ser compatível com os principais navegadores de mercado;
- III. Permitir operação responsiva, com adaptação a diferentes resoluções de tela;
- IV. Disponibilizar interface no idioma português brasileiro;
- V. Permitir personalização de dashboards, painéis e visualizações por perfil de usuário;
- VI. Permitir navegação entre diferentes níveis de informação (visão executiva → técnica → detalhada), com suporte a drill-down.

### 3.6. **Segurança da Informação**

- I. Garantir criptografia de dados em trânsito e em repouso;
- II. Permitir integração com mecanismos de autenticação corporativa (ex: LDAP, Active Directory, SSO);
- III. Suportar autenticação multifator (MFA);
- IV. Garantir proteção de credenciais utilizadas na coleta de dados (ex: discovery, integrações);
- V. Manter trilha de auditoria completa das ações realizadas na plataforma;
- VI. Permitir configuração de políticas de retenção de dados conforme requisitos da CONTRATANTE.

### 3.7. **Integração e Interoperabilidade**

- I. Disponibilizar APIs abertas para integração com sistemas externos;
- II. Permitir ingestão de dados provenientes de múltiplas fontes (on-premise e cloud);
- III. Suportar integração com ferramentas de monitoração, automação e segurança;
- IV. Permitir exportação de dados para ferramentas analíticas externas;
- V. Garantir consistência e integridade dos dados integrados.

### 3.8. **Observabilidade e Inteligência Operacional**

- I. Operar como plataforma unificada de observabilidade, integrando métricas, eventos, logs e rastreamento de transações;
- II. Permitir correlação automática entre dados de diferentes camadas (infraestrutura, aplicação e serviço);
- III. Suportar análise em tempo real e histórica;
- IV. Integrar-se com mecanismos de inteligência artificial para análise preditiva, detecção de anomalias e automação de resposta;
- V. Garantir atualização contínua das informações monitoradas

### 3.9. **Ingestão e Deduplicação de Alertas**

- a) A solução deverá receber alertas provenientes de múltiplas fontes de monitoramento por meio de webhooks HTTP, suportando, no mínimo, os formatos: Grafana Alert Manager, Prometheus Alert Manager, PagerDuty Events API e Zabbix Webhooks.
- b) A solução deverá suportar ingestão de pacotes enriquecidos contendo alertas correlacionados, inventário de hosts afetados, topologia de serviços e histórico de alterações recentes.
- c) A solução deverá implementar mecanismo de deduplicação de alertas com mesma origem e identificador, recebidos dentro de uma janela temporal configurável, de modo a evitar abertura duplicada de incidentes.
- d) A solução deverá suportar ingestão do tipo pull-based (polling) a partir de plataformas externas de AIOps por meio de adaptadores configuráveis.
- e) A solução deverá criar incidentes automaticamente a partir dos alertas recebidos, atribuindo severidade, hosts afetados e contexto extraído do payload do alerta.
- f) A solução deverá manter separados, em registros distintos, a caracterização do evento e a decisão de acionamento correspondente, de modo que cada decisão possa ser auditada independentemente do evento que a originou.
- g) A solução não deverá basear a decisão de acionamento exclusivamente em rótulo de severidade ou em nome de grupo atribuídos pela fonte, devendo considerar, no mínimo: desvio em relação à linha de base observada, especificidade do alvo, correlação com sinal interno e evidência de falha do controle.
- h) A solução não deverá realizar supressão silenciosa de eventos, devendo todo evento suprimido ser registrado com o critério que fundamentou a supressão.
- i) A solução deverá apurar e disponibilizar as taxas de supressão e de acionamento por fonte e por período, para verificação da efetividade da triagem.

### 3.10. **Gestão de Incidentes**

- a) Cada incidente deverá possuir ciclo de vida definido contemplando, no mínimo, os estados: detecção, investigação, aguardando aprovação, investigado, resolvido e encerrado, com possibilidade de transição para estado de escalção a qualquer momento.
- b) A solução deverá classificar incidentes por severidade em pelo menos cinco níveis: Crítico, Alto, Médio, Baixo e Informativo.

- c) A solução deverá atribuir número sequencial por organização para referência humana dos incidentes.
- d) A solução deverá permitir listagem de incidentes com filtros por status, severidade, fonte, período, hosts afetados e equipe responsável.
- e) A solução deverá exibir linha do tempo (timeline) completa de cada incidente, incluindo alertas recebidos, ações executadas, resultados das verificações, decisões do agente de IA e interações humanas.
- f) A solução deverá suportar investigação automática de incidentes com base em critérios de severidade configuráveis pelo administrador.
- g) A solução deverá distinguir o estado 'investigado' (agente concluiu a análise) do estado 'resolvido' (problema confirmado como solucionado), admitindo que a transição entre eles seja realizada pelo operador humano ou de forma automática, a partir do evento de mudança de status emitido pela solução de ITSM integrada.

### 3.11. **Investigação Autônoma por Agente de Inteligência Artificial**

- a) A solução deverá executar ciclo iterativo de raciocínio, ação e observação de forma autônoma para investigar incidentes, selecionando e invocando capacidades apropriadas com base no contexto do incidente.
- b) A solução deverá suportar a execução de ações sobre a infraestrutura, incluindo: execução de comandos em hosts afetados, consulta de métricas em fontes de dados, consulta de logs, verificação de conectividade e abertura de chamados na solução de gestão de serviços (ITSM) por webhook autenticado por chave de API, com correlação por identificador externo.
- c) A solução deverá respeitar níveis de risco configuráveis para execução de ações, de modo que: ações de baixo risco sejam executadas automaticamente; ações de risco médio sejam executadas com registro detalhado; ações de alto risco e críticas exijam aprovação humana prévia.
- d) A solução deverá implementar critérios de parada automáticos para o ciclo de investigação, incluindo: número máximo de iterações configurável, ausência de progresso detectada em iterações consecutivas, atingimento de limiar de confiança e timeout global configurável.
- e) A solução deverá registrar cada decisão, raciocínio, ação executada e resultado observado pelo agente, garantindo auditabilidade e reprodutibilidade das investigações.
- f) A solução deverá suportar, no mínimo, três modos de operação: autônomo (agente investiga e resolve sem intervenção humana, exceto ações destrutivas); assistido (agente investiga e sugere ações, operador decide); e manual (agente atua como assistente via chat, operador conduz).
- g) A solução deverá permitir a definição do grau de autonomia por classe de ação e por ambiente, de modo que uma mesma ação possa ser executada automaticamente em um ambiente e estar sujeita a aprovação humana em outro, sem necessidade de desenvolvimento, devendo toda ação automática registrar o procedimento de reversão aplicável.

### 3.12. **Orquestração Multi-Agente**

- a) A solução deverá suportar planejamento de investigações complexas como grafo acíclico dirigido (DAG), permitindo que passos independentes sejam executados em paralelo.

- b) O planejador de execução paralela deverá ser acionado por meio de modelo de linguagem, gerando automaticamente o plano com as dependências entre as etapas de investigação.
- c) A solução deverá suportar hooks configuráveis em pontos críticos do fluxo de execução, incluindo antes do uso de ferramenta, após geração do plano e ao acionar subagentes.

### 3.13. **Conjunto de Capacidades Nativas**

3.13.1. A solução deverá prover conjunto de capacidades nativas que o agente de IA poderá acionar durante investigações, incluindo no mínimo:

- Execução de comandos em hosts remotos via SSH e em ambientes isolados (sandbox);
- Consulta de métricas, dashboards e regras de alerta em plataformas de monitoramento (ex.: Grafana, Prometheus);
- Consulta a fontes de dados heterogêneas (ex.: ClickHouse, PostgreSQL, Elasticsearch) por meio de SQL ou linguagens de consulta nativas;
- Abertura de chamados, registro de acompanhamentos e encerramento na solução de ITSM integrada;
- Envio de notificações por múltiplos canais (ex.: Slack, Microsoft Teams, Telegram, e-mail);
- Verificação de conectividade de serviços por meio de probes HTTP/HTTPS, TCP, DNS, SSL/TLS, ICMP e SMTP;
- Geração de documentos técnicos a partir de modelos (templates) pré-definidos;
- Análise de métricas históricas e calibração automática de limiares de alerta;
- Consulta a inventário e topologia de configuração de serviços.

3.13.2. A execução de comandos em hosts remotos deverá implementar pipeline de segurança multicamadas, contemplando: decomposição de comandos compostos, validação de redirecionamentos para caminhos protegidos, classificação de risco por padrões de comandos, restrições por ambiente (desenvolvimento, homologação, produção) e classificação contextual por modelo de linguagem para comandos ambíguos.

3.13.3. A solução deverá permitir habilitação e desabilitação granular de cada capacidade por organização/tenant.

3.13.4. A solução deverá registrar métricas de uso por capacidade: total de execuções, taxa de sucesso, latência média e custo estimado em tokens.

### 3.14. **Interface Conversacional com Agente de IA**

- a) A solução deverá oferecer interface de chat com o agente de IA em dois modos: (a) vinculado a um incidente específico, com acesso a toda a linha do tempo, evidências, hosts afetados e aos dados do chamado correlacionado na solução de ITSM, recebidos por evento de integração; e (b) assistente geral de infraestrutura com acesso às capacidades e integrações configuradas.
- b) O chat deverá suportar transmissão de respostas em tempo real (streaming), exibindo ao operador o raciocínio do agente, o início e o resultado de cada ação executada, solicitações de aprovação humana e mensagens de erro.

- c) O chat deverá suportar retomada de sessão após desconexão, reconstruindo o contexto a partir do histórico de mensagens armazenado.
- d) A solução deverá aplicar controles de uso configuráveis por organização, incluindo: limite de mensagens por minuto, limite de execuções de capacidades por minuto, número máximo de conversas simultâneas e orçamento de tokens por conversa e por turno.
- e) O estilo de saída do agente deverá ser configurável em ao menos três níveis hierárquicos — organização, usuário e conversa —suportando modos como conciso, normal, detalhado e estruturado.

### 3.15. **Automações Programadas**

- a) A solução deverá suportar criação de rotinas automatizadas com frequência configurável, incluindo: execução manual, horária, diária, em dias úteis, semanal, mensal e cron customizado.
- b) As rotinas deverão ser definidas por meio de descrição em linguagem natural, com suporte a referências inline a capacidades e agentes disponíveis.
- c) A solução deverá permitir ativação, desativação e pausa de rotinas, registrando histórico de execuções com data, hora, duração, status (sucesso ou falha) e sumário do resultado.
- d) As rotinas deverão suportar execução via orquestração multi-agente paralela e memória episódica para aprendizado com execuções anteriores.

### 3.16. **Geração Automatizada de Documentos**

- a) A solução deverá suportar geração de documentos técnicos a partir de modelos (templates) com resolução automática de variáveis a partir de fontes como: dados do incidente, métricas coletadas, dados do chamado correlacionado na solução de ITSM (número, título, organização, prioridade, status e nível de atendimento) e consultas a fontes de dados externas.
- b) A solução deverá disponibilizar, no mínimo, os seguintes tipos de documento nativos: análise de causa raiz (RCA), relatório de incidente, relatório de desempenho de aplicações, relatório de calibração de alertas e planejamento de capacidade.
- c) Os documentos gerados deverão possuir ciclo de vida com os estados: rascunho, revisão, aprovado e publicado, com suporte a versionamento e histórico de alterações.
- d) A solução deverá suportar exportação dos documentos no formato PDF.
- e) A solução deverá suportar agendamento de geração periódica de documentos com entrega automática por e-mail e por canais de mensageria configurados.

### 3.17. **Dashboard Operacional**

- a) A solução deverá disponibilizar painel central de operações com atualização em tempo real, exibindo: total de incidentes ativos e tendência, tempo médio de resolução (MTTR), taxa de automação (percentual de incidentes resolvidos sem intervenção humana) e aprovações pendentes.
- b) O painel deverá exibir tabela de incidentes com filtros por severidade, status, equipe e período.

- c) O painel deverá exibir feed de atividade ao vivo com eventos do agente, das integrações e das ações dos operadores.
- d) O painel deverá exibir status de saúde das integrações configuradas.

### 3.18. **Aprovações e Escalações**

- a) A solução deverá suportar fluxo de aprovação humana para ações de risco elevado, com notificação ao aprovador pelo canal configurado (ex.: Slack, Teams, e-mail).
- b) A solução deverá suportar regras de escalação configuráveis, incluindo: timeout de aprovação, escalação automática e cadeia de escalação (operador, líder, gestor).
- c) A solução deverá cancelar automaticamente operações cujo timeout de aprovação expire, adotando comportamento fail-closed (operação não realizada em caso de ausência de resposta).

### 3.19. **Integrações com Sistemas Externos**

3.19.1. A solução deverá suportar integração nativa com, no mínimo, as seguintes categorias de sistemas:

- Gestão de Serviços de TI (ITSM): integração por interface de programação de aplicações (API) e por webhook autenticado por chave, com abertura e encerramento de chamados e correlação bidirecional por identificador externo;
- Monitoramento: Grafana, Prometheus, Zabbix;
- Fontes de dados: ClickHouse, PostgreSQL, Elasticsearch;
- Notificação: Slack, Microsoft Teams, Telegram, e-mail (SMTP);
- Execução remota: SSH (hosts Linux/Unix) e Kubernetes.

3.19.2. Todas as integrações deverão implementar mecanismos de retry com backoff exponencial, circuit breaker por provedor, timeout configurável, rate limiting e verificação periódica de saúde (health check).

3.19.3. A solução deverá suportar troca de integrações sem necessidade de reinicialização do serviço (hot-swap).

3.19.4. A solução deverá suportar modo de execução remota para ambientes sem acesso direto de rede, por meio de agente instalado no ambiente do cliente que se comunica com a plataforma via protocolo seguro.

3.19.5. A solução deverá admitir coletores distribuídos por região, cada um com identificação única, sem exposição de portas de rede e com criptografia ponta a ponta entre o coletor e a plataforma.

### 3.20. **Integração com Gestão de Serviços de TI (ITSM)**

- a) A solução deverá abrir chamados na solução de ITSM automaticamente após a conclusão de investigações, com base em severidade mínima configurável, convertendo a severidade do incidente em urgência e impacto, de modo que a prioridade do chamado seja derivada da matriz da própria solução de ITSM.
- b) A solução deverá acompanhar o status dos chamados abertos e encerrar incidentes automaticamente quando o chamado correspondente for fechado na solução de ITSM, admitido o acompanhamento por evento emitido pela solução de ITSM a cada mudança de status do chamado.

- c) A solução deverá manter rastreabilidade bidirecional entre incidentes e chamados da solução de ITSM, por identificador externo persistido no próprio chamado.

### 3.21. **Base de Conhecimento**

- a) A solução deverá suportar cadastro e gestão de entradas de conhecimento, com busca por similaridade semântica (busca vetorial) para enriquecer o contexto do agente durante investigações.
- b) O agente deverá consultar a base de conhecimento durante investigações, alcançando os artigos, erros conhecidos e soluções de contorno registrados na solução de ITSM, e incorporar as soluções conhecidas ao raciocínio e às recomendações geradas.

### 3.22. **Execução em Ambiente Isolado**

- a) A solução deverá disponibilizar ambiente de execução isolado (sandbox) onde o agente possa executar comandos sem acesso ao ambiente de produção, com restrições de sistema de arquivos, rede, privilégios e recursos computacionais.
- b) A solução deverá disponibilizar terminal interativo no ambiente isolado, acessível via interface web em tempo real.
- c) A solução deverá suportar provisionamento e desprovisionamento dinâmico dos ambientes isolados com escalonamento automático baseado na demanda.

### 3.23. **Orquestração de Modelos de Linguagem**

- a) A solução deverá registrar, de forma auditável, todas as chamadas realizadas a sistemas externos, incluindo: método, URL, corpo da requisição e resposta (sanitizados), status HTTP, decomposição de latência e contagem de tentativas.
- b) A solução deverá registrar cada iteração do ciclo de investigação do agente, incluindo: número da iteração, fase, raciocínio, ação executada, parâmetros utilizados, resultado observado e duração.
- c) O roteamento dos modelos deverá ser configurável por tipo de atividade, permitindo definir qual modelo será utilizado para cada contexto (investigação de incidentes, geração de documentos, chat, sumarização, entre outros).
- d) O módulo de orquestração de LLMs deverá permitir a definição de orçamento mensal por organização e por finalidade, com alerta em percentual configurável e comportamento definido para o esgotamento do orçamento, contemplando, no mínimo, as opções de bloqueio, degradação para modelo de menor custo ou continuidade com registro, conforme configuração da CONTRATANTE.

### 3.24. **Observabilidade da Plataforma**

- a) A solução deverá registrar, de forma auditável, todas as chamadas realizadas a sistemas externos, incluindo: método, URL, corpo da requisição e resposta (sanitizados), status HTTP, decomposição de latência e contagem de tentativas.
- b) A solução deverá registrar cada iteração do ciclo de investigação do agente,

incluindo: número da iteração, fase, raciocínio, ação executada, parâmetros utilizados, resultado observado e duração.

- c) A solução deverá registrar cada chamada realizada a modelos de linguagem, incluindo: provedor, modelo, tokens de entrada e saída, custo estimado, latência e motivo de encerramento.
- d) Todos os eventos de observabilidade deverão ser disponibilizados em tempo real na interface da plataforma, permitindo filtro por investigação.
- e) A solução deverá suportar rastreamento distribuído aderente ao padrão OpenTelemetry, permitindo visibilidade end-to-end desde a ingestão do alerta até a resolução do incidente.
- f) O registro de observabilidade deverá permitir reconstituir integralmente a decisão automatizada a partir dos dados persistidos, incluindo: entrada, raciocínio, ação executada, parâmetros utilizados, resultado observado e modelo utilizado, de modo que a fiscalização possa auditar a decisão sem depender de nova execução.

### 3.25. **Identidade e Controle de Acesso**

- a) A solução deverá implementar controle de acesso baseado em papéis (RBAC), com isolamento completo de dados entre organizações (multi-tenant).
- b) A solução deverá suportar, no mínimo, os seguintes papéis: administrador, líder técnico (SRE Lead), operador, visualizador e aprovador.
- c) A solução deverá suportar os seguintes métodos de autenticação: usuário e senha com token JWT, Single Sign-On (SSO) via OIDC (ex.: Google Workspace, Azure AD, Okta) e SAML 2.0 para integração corporativa.
- d) A solução deverá suportar autenticação multifator (MFA) com TOTP e WebAuthn/FIDO2, configurável como obrigatório por organização.
- e) A solução deverá suportar autenticação por chaves de API para integrações máquina-a-máquina.
- f) A solução deverá implementar isolamento de dados no nível de banco de dados (Row Level Security) para garantir que cada organização acesse exclusivamente seus próprios dados.

### 3.26. **Requisitos Não Funcionais**

- a) Desempenho: o tempo entre o recebimento do alerta e o início da primeira ação de investigação deverá ser inferior a 30 (trinta) segundos.
- b) Disponibilidade: a solução deverá garantir disponibilidade mínima de 99,5% (noventa e nove vírgula cinco por cento) ao longo do período contratual.
- c) Segurança: credenciais armazenadas deverão ser criptografadas com algoritmos de padrão industrial (ex.: AES-256); chaves de API deverão ser armazenadas somente como hash irreversível; toda operação sensível deverá gerar registro de auditoria imutável; containers de execução deverão operar sem privilégios elevados.
- d) Escalabilidade: a arquitetura deverá suportar expansão horizontal de componentes sem interrupção do serviço.
- e) Dados: todas as informações armazenadas são de propriedade exclusiva da CONTRATANTE e deverão ser disponibilizadas em sua integralidade por, no mínimo, 120 (cento e vinte) dias após o encerramento do contrato.

- f) Atualizações: a versão ofertada deverá ser a mais recente e estável disponível, e o fornecedor deverá prover atualizações corretivas e evolutivas durante toda a vigência contratual.
- g) Sincronização de horário: todos os componentes da solução deverão sincronizar o horário automaticamente com a Hora Legal Brasileira (Observatório Nacional).

### 3.27. **Módulo de Discovery / Inventário de Ativos de TI**

- a) A solução deverá ser capaz de realizar a descoberta de uma ampla variedade de dispositivos, incluindo licenças de software, servidores físicos e virtuais, storages, dispositivos de rede, buckets de armazenamento em nuvem, containers (Kubernetes, OpenShift, Rancher, Docker, AWS ECS, Azure AKS, Oracle OKE, entre outros) e demais ativos existentes no parque tecnológico, suportando relacionamentos muitos-para-muitos ou pai-filho entre os itens descobertos, incluindo nuvens públicas (AWS, Azure, Huawei, Oracle, Google, VMware, entre outras), ambientes virtualizados e infraestruturas distribuídas.
- b) A solução deverá manter as funcionalidades essenciais de gestão de configuração (CMDB) na solução de ITSM, contemplando criação, leitura, atualização e desativação de itens de configuração (ICs), bem como as funcionalidades essenciais de gestão de ativos de TI, admitida a carga do inventário descoberto por importação a partir da ferramenta de descoberta.
- c) A solução deverá entender e interpretar os diferentes modelos de serviço em nuvem, como IaaS (Infrastructure as a Service) e PaaS (Platform as a Service), com suporte à descoberta de recursos em várias regiões, proporcionando visão consolidada de ambientes distribuídos geograficamente.
- d) A solução deverá realizar a descoberta utilizando método sem agente instalado nos alvos (agentless), podendo complementar com método baseado em agente para descoberta em tempo real, desde que não afete o desempenho dos alvos.
- e) A solução deverá notificar os responsáveis imediatamente sobre a descoberta de dispositivos não autorizados e, ao identificá-los, ser capaz de bloqueá-los ou isolá-los mediante integração com ferramentas de segurança.
- f) A solução deverá manter agenda de execução da descoberta em intervalos regulares, garantindo a integridade dos dados do CMDB, com possibilidade de definir e personalizar o escopo da descoberta (segmentos de rede, tipos de IC e de ativo a incluir ou excluir).
- g) A solução deverá suportar uso de protocolos de descoberta como, no mínimo: SNMP, WMI e SSH, garantindo que a descoberta seja realizada de forma segura, com proteção de credenciais e adesão às melhores práticas de segurança.
- h) A solução deverá apresentar mapa de relacionamentos e dependências em visualização gráfica ou diagramas interativos, atualizado em tempo real, com suporte a tipos de relacionamento como “é parte de”, “é conectado a”, “depende de” e “é usado por”, independente da camada representada (serviço, aplicação, infraestrutura).
- i) A solução deverá criar automaticamente versões do mapa de relacionamentos e dependências, mantendo histórico de versões anteriores,

com rastreabilidade de alterações ao longo do tempo.

- j) A solução deverá realizar auditorias automáticas para verificação da existência e conformidade dos ICs no parque tecnológico, identificando não conformidades e sugerindo correções.
- k) A integração do módulo de Discovery com a solução de ITSM deverá ocorrer por interface de programação de aplicações (API), contemplando a importação do inventário descoberto e a atualização dos itens de configuração no CMDB.
- l) A solução deverá realizar a descoberta e a classificação automática de ativos nas camadas física e lógica, construindo topologia e mapa de dependências que contemplem, no mínimo: equipamentos de armazenamento, empilhamento de comutadores, telefonia sobre IP e demais elementos de rede, bem como componentes de nuvem pública, apresentados no mesmo grafo de dependências que os ativos locais.
- m) O componente instalado nos ativos monitorados deverá ser único para as funções de monitoração e de inventário e não poderá exigir a exposição de porta de serviço em escuta no ativo, de modo que a monitoração não amplie a superfície de ataque do parque tecnológico.
- n) A solução deverá reconciliar os registros provenientes de fontes distintas de descoberta e inventário, deduplicando por precedência configurável entre fontes, de modo que o mesmo ativo descoberto por mais de um método resulte em um único item de configuração, com registro da fonte que prevaleceu em cada atributo.

### 3.28. **Módulo de AIOps - Requisitos Complementares**

- a) A solução de AIOps deverá possuir capacidades avançadas de inteligência artificial para identificar automaticamente a causa raiz dos eventos, sem necessidade de configurações manuais prévias, aprendendo continuamente com cada evento para melhorar a precisão das suas previsões e recomendações.
- b) A solução deverá exibir visualmente a topologia de serviços com base nas dependências entre componentes de infraestrutura (ICs), mostrando os impactos de um chamado em um serviço mapeado pela ferramenta de descoberta, e integrar-se à solução de ITSM para automação do fluxo de resolução de incidentes, desde a abertura até o encerramento do chamado.
- c) A solução deverá ter capacidade de integração com sistemas de monitoramento de nuvem, para captura de eventos das soluções CloudWatch da AWS, Azure Monitor, Google Cloud Monitoring e OCI Monitoring da Oracle, fornecendo visão unificada de problemas ocorridos em nuvem e no on-premise.
- d) A solução deverá ser capaz de rastrear o impacto na disponibilidade de um item de configuração com base em dados do mapa de relacionamento, incidentes e problemas causados por alterações anteriores, identificando a causa raiz como erro conhecido registrado na solução de ITSM e aplicando a solução de contorno nele mapeada.
- e) A solução deverá ser capaz de configurar limites de performance para itens de configuração com flexibilidade para diferentes cenários e períodos (sazonalidade), identificando redução de qualidade/performance do serviço em virtude de tempo de resposta elevado, mesmo que não afete a disponibilidade contratada.

- f) A solução deverá possuir recursos de inteligência artificial para propor possíveis diagnósticos ou resoluções para chamados, a partir da análise dos dados do chamado e do conhecimento acumulado na solução de ITSM (base de conhecimento, chamados anteriores, mudanças, itens de configuração e eventos), cabendo ao motor de regras da solução de ITSM o direcionamento do chamado no fluxo de trabalho definido.
- g) A solução deverá estar preparada para ativação de recursos de IA Generativa, oferecendo interface conversacional em linguagem natural para usuários finais e equipes de TI, gerando respostas automatizadas e contextualizadas para incidentes, solicitações de serviço e perguntas frequentes.
- h) A solução deverá ser flexível e conectável a LLMs de mercado (como OpenAI, entre outros) via API, possibilitando personalização e alternância entre modelos.
- i) Toda a arquitetura, inclusive o AIOps, deverá ser instalada de modo que todos os seus dados sejam processados e armazenados dentro da infraestrutura da CONTRATANTE, com modelo de licenciamento unificado para toda a plataforma.

### 3.29. **Módulo de Gestão de Eventos**

- a) A solução deverá ser capaz de detectar anomalias e picos de eventos, agrupando e relacionando eventos e alertas, e abrir chamados automaticamente na solução de ITSM a partir de um evento, iniciando o fluxo de gestão de incidentes conforme critérios definidos pela CONTRATANTE e o conteúdo do evento, com deduplicação por identificador externo e admitida a reclassificação do chamado para requisição de serviço, problema ou mudança na própria solução de ITSM.
- b) A solução deverá executar ações corretivas automatizadas para os eventos identificados e ser capaz de avaliar a série histórica do item de configuração e projetar horizonte de evolução, identificando proativamente risco de descumprimento da disponibilidade acordada e recomendando a ação de ajuste correspondente, com registro da projeção e do seu fundamento, observado o grau de autonomia definido pela CONTRATANTE, nos termos do item 3.11, registrando a ação executada no chamado correspondente na solução de ITSM, que dará origem ao registro de mudança quando aplicável.
- c) A solução deverá ter capacidade de integração com ferramentas essenciais de monitoramento e operações como Zabbix, Prometheus e VMware Aria Operations para sincronização de eventos e topologia (ICs), além de integração com sistemas de monitoramento de nuvem (CloudWatch, Azure Monitor, Google Cloud Monitoring e OCI Monitoring da Oracle).
- d) A solução deverá ser capaz de receber evento de normalização do objeto do incidente e realizar automaticamente os procedimentos de encerramento adequados conforme regra de negócio definida pela CONTRATANTE, bem como medir a disponibilidade efetiva de um IC/Serviço e informar ao módulo de gestão de níveis de serviço da solução de ITSM para aferição do indicador.

### 3.30. **Módulo de Monitoramento de Performance de Aplicações (APM)**

- a) A solução deverá permitir o monitoramento de transações de aplicações em tempo real, contemplando, no mínimo: tempo de resposta, volume de transações (throughput) e taxa de erro, possibilitando análise detalhada do

comportamento das aplicações.

- b) A solução deverá realizar rastreamento distribuído (distributed tracing) de transações ponta a ponta, identificando automaticamente o caminho completo de uma requisição entre múltiplos serviços, APIs e componentes, e identificar gargalos de desempenho ao longo da execução, indicando o ponto exato de degradação.
- c) A solução deverá identificar automaticamente as dependências entre componentes de aplicação e entre aplicações e infraestrutura, permitindo visualização da topologia lógica e técnica das aplicações monitoradas, com correlação entre dados de aplicação, infraestrutura, eventos e métricas em visão unificada. A topologia de aplicação deverá ser reconciliada com o inventário e o mapa de dependências produzidos pelo módulo de descoberta (item 3.27), de modo que aplicação e infraestrutura sejam representadas no mesmo grafo de dependências.
- d) A solução deverá definir automaticamente um baseline de comportamento das aplicações com base em dados históricos, detectando anomalias de performance por desvios do comportamento esperado e gerando alertas automaticamente quando houver degradação significativa, mesmo sem violação de thresholds previamente definidos.
- e) A solução deverá operar em ambientes distribuídos e baseados em microsserviços, incluindo integração com plataformas de orquestração de containers (ex.: Kubernetes), e permitir armazenamento de dados históricos de performance para análise retrospectiva, identificação de tendências e suporte à tomada de decisão para otimização de desempenho.

### 3.31. **Módulo de Disponibilidade e Capacidade**

- a) A solução deverá medir a disponibilidade efetiva de um IC/Serviço, considerando a agenda de disponibilidade contratada (regime de produção) e agrupamentos de serviço, apresentando a disponibilidade por meio de diversas métricas como MTBF, MTRS, número de serviços impactados, tempo total de indisponibilidade por período e tempo mínimo entre falhas.
- b) A solução deverá calcular disponibilidade end-to-end do serviço sob a perspectiva do usuário final, considerando toda a cadeia de dependências, identificar proativamente ameaças à meta de disponibilidade e avaliar a série histórica do item de configuração e projetar horizonte de evolução, recomendando (via AIOps) a ação de ajuste necessária para prevenir o descumprimento da disponibilidade ou da capacidade acordada, com registro da projeção e do seu fundamento, observado o grau de autonomia definido pela CONTRATANTE, nos termos do item 3.11.
- c) A solução deverá permitir o registro da capacidade total e utilizada dos recursos de TI (CPU, memória, armazenamento em disco, taxas de transferência de rede, latência de resposta, entre outros), fornecendo visão consolidada de capacidade por Segmento Tecnológico e Tipo de Ativo, com armazenamento de dados históricos para análise retrospectiva e tendências.
- d) A solução deverá suportar a criação de Acordo de Nível de Serviço (ANS) padrão aplicável a todos os serviços e fluxos, registrando os períodos regulares de aferição dos níveis de serviço acordados, com possibilidade de fracionamento sob demanda, e notificando os responsáveis sobre proximidade de quebra e violação efetiva de ANS por correio eletrônico e por ferramenta corporativa de mensageria, com escalonamento automático do chamado.

## **4. PLATAFORMA DE ORQUESTRAÇÃO DE CONHECIMENTO COM LLMS EM LOW-CODE E LLMOPS**

### **4.1. Disposições Gerais**

- a) A plataforma deverá ser disponibilizada em modalidade de software como serviço (SaaS) ou implantada em infraestrutura on-premises ou nuvem privada da CONTRATANTE, conforme definição no ato convocatório.
- b) A plataforma deverá suportar múltiplos usuários com papéis diferenciados, contemplando: desenvolvedores de soluções de IA, usuários finais de agentes e administradores da plataforma.
- c) A interface da plataforma deverá estar disponível no idioma português brasileiro e ser acessível por navegador web sem instalação de cliente dedicado.
- d) Todos os módulos e integrações necessários para atendimento desta especificação deverão estar incluídos na proposta, não sendo admitida cobrança adicional por componentes não declarados.

### **4.2. Orquestração de Prompts e Operações de LLMs (LLMOps)**

- a) A plataforma deverá oferecer interface visual intuitiva para orquestração de prompts e gerenciamento de fluxos de trabalho com modelos de linguagem, sem necessidade de programação extensiva.
- b) A plataforma deverá ser agnóstica em relação ao provedor de modelos de linguagem, suportando integração com, no mínimo, os seguintes provedores: OpenAI (família GPT), Anthropic (família Claude) e Google (família Gemini), permitindo inclusão de novos provedores sem alteração estrutural da plataforma.
- c) A plataforma deverá oferecer ferramentas integradas de LLMOps para gerenciamento e otimização de modelos de linguagem, abrangendo desde a experimentação inicial até a implantação em ambiente de produção.
- d) A plataforma deverá disponibilizar interface de gerenciamento para rastreamento de dados, custos e consumo dos modelos de linguagem, com recursos para melhoria contínua de desempenho.
- e) A plataforma deverá suportar ferramentas para engenharia de prompts, permitindo criação, teste, versionamento e reutilização de prompts de forma estruturada.
- f) A plataforma deverá suportar múltiplos estilos de saída dos agentes, configuráveis por contexto de uso.

### **4.3. Fluxos de Trabalho em Low-Code**

- a) A plataforma deverá disponibilizar ambiente de desenvolvimento de soluções de IA com abordagem low-code, permitindo que equipes com pouca ou nenhuma experiência em programação criem e gerenciem aplicações de IA.
- b) A plataforma deverá suportar criação e modificação de pipelines de automação por meio de interface visual intuitiva, permitindo prototipagem rápida e iteração de soluções.
- c) A plataforma deverá permitir a criação de componentes reutilizáveis entre diferentes fluxos de trabalho.
- d) A plataforma deverá disponibilizar painel de controle específico para

consulta, edição, execução e monitoramento dos fluxos criados.

- e) A plataforma deverá suportar a programação de execução dos fluxos ao menos das seguintes formas: agendada (schedule), manual pelo usuário e automática por eventos ou ações de outros sistemas.
- f) A plataforma deverá disponibilizar dashboard com métricas e gráficos do histórico de execuções dos fluxos de trabalho.
- g) A plataforma deverá prover ambientes segregados para desenvolvimento, teste e produção.

#### 4.4. Motores de Recuperação com Auxílio de Contexto (RAG) e Ingestão de Conhecimento

- a) A plataforma deverá disponibilizar motores de Recuperação com Auxílio (RAG — Retrieval-Augmented Generation) de alta qualidade, permitindo combinar dados contextuais com modelos de linguagem para respostas mais precisas e contextualmente relevantes.
- b) A plataforma deverá suportar implementação de fluxo RAG completo, incluindo: ingestão de dados, pré-processamento, fragmentação (chunking), geração de embeddings, armazenamento em banco de dados vetorial e geração de resposta pelo LLM a partir de prompts do usuário.
- c) A plataforma deverá suportar conectores de ingestão de dados que facilitem a acessibilidade, atualização e usabilidade dos dados nas bases de conhecimento.
- d) A plataforma deverá permitir particionamento, limpeza e preparação de dados antes da análise principal.
- e) A plataforma deverá suportar decomposição de textos longos em segmentos menores e consistentes, com configuração de estratégias de fragmentação.
- f) A plataforma deverá converter dados textuais em vetores de tamanho fixo (embeddings) e armazená-los de forma otimizada para buscas de alta velocidade por similaridade semântica.
- g) A plataforma deverá suportar decomposição de textos em tokens e integração nativa com modelos de linguagem próprios e externos.

#### 4.5. Processamento e Particionamento de Documentos

- a) A plataforma deverá suportar processamento e reconhecimento de ao menos os seguintes formatos de arquivo: texto simples (TXT), planilhas (XLS, XLSX, CSV), JSON, PDF, HTML, Markdown, PowerPoint, e-mails e EPUB.
- b) A plataforma deverá realizar detecção automática do tipo de arquivo para roteamento ao processador apropriado.
- c) A plataforma deverá permitir a configuração de opções específicas de particionamento por tipo de documento.
- d) A plataforma deverá permitir a extração de metadados relevantes e a estruturação do conteúdo de documentos.
- e) A plataforma deverá suportar reconhecimento óptico de caracteres (OCR) para processamento de documentos digitalizados, com suporte a múltiplos idiomas.
- f) A plataforma deverá disponibilizar APIs para particionamento de documentos, permitindo integração com sistemas existentes e automação de fluxos de trabalho.

- g) A plataforma deverá permitir atualização das bases de dados de conhecimento em períodos pré-definidos e customização dos modelos de IA com novas informações a qualquer momento.

#### 4.6. Agentes de Inteligência Artificial Personalizáveis

- a) A plataforma deverá oferecer estrutura flexível para criação de agentes de IA personalizáveis, com configuração de comportamento, personalidade e capacidades conforme as necessidades específicas do caso de uso.
- b) A plataforma deverá permitir a utilização dos agentes criados em diversas aplicações, incluindo atendimento ao cidadão, assistentes virtuais especializados e automação de processos, com integração aos sistemas corporativos.
- c) A plataforma deverá suportar flexibilidade para customizar as ações executadas pelos agentes de IA.
- d) A plataforma deverá disponibilizar ferramentas de publicação dos agentes e aplicações diretamente na plataforma.

#### 4.7. APIs e Integrações

- a) A plataforma deverá disponibilizar APIs RESTful para integração com sistemas existentes, permitindo que a lógica de negócios seja desacoplada dos prompts e do motor de IA, e consumir a solução de ITSM por webhook autenticado por chave de API.
- b) A plataforma deverá suportar integração com a solução de gestão de serviços adotada na organização, por interface de programação de aplicações e por eventos nos dois sentidos, permitindo gestão centralizada e eficiente.
- c) A plataforma deverá suportar integração com bancos de dados, webservices, arquivos CSV e correio eletrônico, com envio por SMTP e recebimento por IMAP.
- d) A plataforma deverá suportar tecnologias padrão de integração, incluindo SOAP, REST, JSON e WSDL.
- e) A plataforma deverá permitir integração de dados de múltiplas fontes para alimentar o motor de IA.
- f) A plataforma deverá suportar autenticação do tipo SSO (Single Sign-On), com integração a diretórios corporativos como Active Directory e LDAP.

#### 4.8. Gestão de Modelos e Base de Conhecimento

- a) A plataforma deverá fornecer base de conhecimento centralizada para armazenamento, gerenciamento e acesso a informações relacionadas aos modelos de IA, prompts e fluxos de trabalho, facilitando reutilização e melhoria contínua.
- b) A plataforma deverá oferecer sistema de gestão de modelos com suporte a documentação, rastreamento de alterações e auditoria completa dos projetos de IA.
- c) A plataforma deverá disponibilizar ferramentas de anotação (annotation) para refinamento de modelos com base em feedbacks contínuos dos usuários.
- d) A plataforma deverá permitir personalização e adaptação dos modelos de

linguagem para atendimento às necessidades específicas da organização, incluindo a capacidade de ajuste fino (fine-tuning) de modelos.

#### 4.9. Monitoramento, Avaliação e Extensibilidade

- a) A plataforma deverá incluir ferramentas de monitoramento de desempenho dos modelos e aplicações em produção, permitindo ajustes em tempo real.
- b) A plataforma deverá disponibilizar extensões personalizáveis para adaptação a cenários e setores específicos.
- c) A plataforma deverá suportar a análise automática de dados e fornecimento de insights relevantes a partir dos fluxos executados.
- d) A plataforma deverá possibilitar armazenamento de logs por período mínimo de 30 (trinta) dias, com possibilidade de ampliação desse prazo.
- e) A plataforma deverá permitir a realização de backups periódicos das configurações, modelos e bases de conhecimento.

#### 4.10. Análise de Dados e Aprendizado de Máquina

- a) A plataforma deverá possuir funcionalidades de análise de dados (Data Analytics) com suporte a criação de dashboards dinâmicos por arrastar e soltar (drag & drop).
- b) A plataforma deverá permitir definição de indicadores-chave de desempenho (KPIs), projeção de tendências em métricas e detecção de anomalias.
- c) A plataforma deverá suportar análise e modelagem de séries temporais e modelagem de classificação e regressão.
- d) A plataforma deverá possibilitar análises históricas e aplicação de filtros e agrupamentos nos dashboards.
- e) A plataforma deverá suportar otimização automática de hiperparâmetros dos modelos de aprendizado de máquina.
- f) A plataforma deverá suportar processamento e análise de dados de diferentes modalidades, incluindo texto e áudio.
- g) A plataforma deverá permitir integração com ferramentas de análise exploratória de dados (EDA).
- h) A plataforma deverá permitir a formulação de consultas analíticas em linguagem natural sobre as bases de dados conectadas, traduzindo-as para linguagem de consulta estruturada e apresentando ao usuário a consulta gerada antes da execução.
- i) A plataforma deverá validar sintaticamente toda consulta gerada antes da execução, com bloqueio de comandos de definição e de manipulação de dados, de leitura de arquivo do sistema, de agendamento e de execução dinâmica, e com aplicação automática de limite de linhas e de tempo máximo de execução.
- j) A plataforma deverá conectar-se às fontes de dados exclusivamente por credencial sem privilégio de escrita, verificando essa condição no cadastro da fonte e recusando credencial com privilégio administrativo.
- k) A plataforma deverá permitir o cruzamento de dados de fontes distintas sem replicação nem persistência intermediária dos dados consultados, com limite de recursos por sessão.
- l) A plataforma deverá manter registro auditável das consultas realizadas, com

identificação do usuário, fonte consultada, consulta executada e custo apurado, exportável para instrução de processo.

- m) A plataforma deverá disponibilizar representação geográfica do território brasileiro por unidade federativa e por região, aplicável às visualizações de dados.

#### 4.11. Segurança e Governança

- a) A plataforma deverá implementar criptografia avançada para dados em repouso e em trânsito, garantindo a proteção das informações sensíveis da organização.
- b) A plataforma deverá disponibilizar governança centralizada para gerenciamento de acesso, rastreabilidade e controle sobre os dados e as operações dos modelos de IA em ambiente único.
- c) A plataforma deverá garantir conformidade com a Lei Geral de Proteção de Dados (LGPD), incluindo políticas de privacidade e controle de consentimento.
- d) A plataforma deverá implementar protocolos de segurança de acesso suportando padrões como HTTPS, TLS 1.3, autenticação multifator (MFA) e criptografia AES-256.
- e) A plataforma deverá suportar gerenciamento de identidade e acesso com autenticação forte, múltiplos níveis de permissão e integração com sistemas de diretório existentes (ex.: Active Directory, LDAP).
- f) A plataforma deverá garantir que o acesso às informações dos sistemas da CONTRATANTE seja realizado somente por usuários com os devidos privilégios de visualização e/ou extração dos dados.
- g) A plataforma deverá tratar como dado, e não como instrução, todo conteúdo proveniente de fonte externa incorporado ao contexto do modelo, com mecanismo de detecção e bloqueio de tentativas de subversão de instruções e registro do evento de bloqueio.

#### 4.12. Escalabilidade e Infraestrutura

- a) A plataforma deverá suportar autoescalabilidade baseada em desempenho e demanda, sem intervenção manual, com provisionamento e desprovisionamento dinâmico de recursos.
- b) A plataforma deverá suportar balanceamento de carga para distribuição eficiente do tráfego e otimização de recursos.
- c) A plataforma deverá garantir disponibilidade por meio de replicação de dados e configuração de failover automático.
- d) A plataforma deverá ser compatível com múltiplos provedores de processamento e modelos em nuvem.
- e) A plataforma deverá suportar escalabilidade eficiente para lidar com cargas de trabalho variáveis, garantindo alto desempenho dos modelos de linguagem.

#### 4.13. Requisitos Não Funcionais

- a) Propriedade dos Dados: todas as informações armazenadas são de propriedade exclusiva da CONTRATANTE e deverão ser disponibilizadas em sua integralidade por, no mínimo, 120 (cento e vinte) dias após o

encerramento contratual.

- b) Compatibilidade: a plataforma deverá ser compatível com as duas últimas versões principais dos principais navegadores web modernos (Google Chrome, Mozilla Firefox, Microsoft Edge, Safari).
- c) Atualizações: a versão ofertada deverá ser a mais recente e estável disponível, com fornecimento de atualizações corretivas e evolutivas durante toda a vigência contratual.
- d) Sincronização de horário: todos os componentes da solução deverão sincronizar o horário automaticamente com a Hora Legal Brasileira (Observatório Nacional).
- e) Custos: todos os custos necessários para a viabilização do projeto, incluindo deslocamentos, hospedagens e alimentação, deverão estar previstos na proposta, não sendo admitidas cobranças extras não declaradas.

## **5. PLATAFORMA DE SEGURANÇA E GOVERNANÇA DA INFORMAÇÃO**

### **5.1. Diretrizes Gerais**

5.1.1. O monitoramento dos ativos de segurança do ambiente da CONTRATANTE deverá ser realizado através de ferramenta (hardware e/ou software) que coletará as informações necessárias via agente ou sem agente para o monitoramento de segurança (SOC), em plataforma que unifique as informações, para permitir avaliação da postura de segurança da organização.

5.1.2. Os serviços descritos neste termo de referência, serão realizados totalmente baseado nas ferramentas de segurança que serão entregues nesta contratação, com processos e pessoas para operacionalizar;

5.1.3. As ferramentas que deverão ser entregues durante os serviços, estão descritas com seus requisitos técnicos de atendimento para o ambiente da CONTRATANTE.

5.1.4. Todo o processo de serviços descritos neste edital, será realizado conforme requisitos descritos das ferramentas de segurança da informação.

5.1.5. O acesso a solução de monitoramento deverá ser realizado apenas pela equipe de segurança da CONTRATANTE e a equipe de serviço de SOC da CONTRATADA;

5.1.6. Deverão ser realizadas reuniões trimestrais gerenciais para avaliação e acompanhamento dos serviços contratados;

5.1.7. A CONTRATA deve fornecer acesso a ferramenta de resultados e status de segurança para monitoramento de incidentes, controles de SLA e avaliações da prestação do serviço, com visão do ambiente de segurança da informação em um único ponto de análise.

5.1.8. A CONTRATADA deverá monitorar alertas gerados pelas soluções de Segurança, envolvendo atividades como por exemplo:

I - Monitoramento de Potenciais Ataques Cibernéticos e Hacktivismo

II - Capacidade de coleta e análise de dados de fontes distintas, incluindo redes sociais, fóruns, aplicativos de mensageria e a Deep/Dark Web.

III - Identificação de ameaças cibernéticas e atividades de hacktivismo.

IV - Notificações sobre Vulnerabilidades

V - Monitoramento constante de feeds de vulnerabilidades e malware.

VI - Emissão de alertas sobre novas vulnerabilidades que possam afetar a segurança do ambiente.

## 5.2. **Governança e Consultoria de Segurança**

5.2.1. Criação de Políticas de Segurança da Informação: Desenvolvimento de políticas e procedimentos alinhados às melhores práticas do mercado e frameworks de segurança da informação.

5.2.2. Recomendações Estratégicas: Suporte consultivo contínuo para a equipe de infraestrutura e gestão, com recomendações para aumentar a segurança do ambiente e otimizar a arquitetura existente.

## 5.3. **Análise de Eventos de Segurança**

5.3.1. Deve possuir console web para acesso ao dashboard de gerenciamento através de navegadores web padrão.

5.3.2. A interface web deve ser responsiva e compatível com dispositivos móveis (tablets e smartphones).

5.3.3. A interface deve permitir personalização de temas e layouts conforme preferências do usuário.

5.3.4. A ferramenta deve permitir criação de dashboards personalizados com widgets configuráveis.

5.3.5. A solução deve oferecer visualizações em tempo real de dados de log e eventos de segurança.

5.3.6. A ferramenta deve suportar diferentes tipos de gráficos: barras, linhas, pizza, histogramas, mapas de calor e métricas.

5.3.7. A solução deve permitir drill-down em visualizações para análise detalhada de dados.

5.3.8. A ferramenta deve oferecer dashboards pré-configurados para casos de uso comuns de segurança.

5.3.9. A ferramenta deve implementar controle de acesso baseado em funções (RBAC) com granularidade de permissões.

5.3.10. A solução deve suportar autenticação via Active Directory/LDAP.

5.3.11. A ferramenta deve suportar autenticação multifator (MFA) para acesso administrativo.

5.3.12. A solução deve permitir coleta de dados via API REST e webhooks.

5.3.13. A solução deve suportar enriquecimento de dados com informações de contexto (geolocalização, threat intelligence).

5.3.14. A ferramenta deve implementar motor de busca full-text com indexação automática de campos.

5.3.15. A solução deve suportar busca em tempo real e histórica com performance otimizada.

5.3.16. A ferramenta deve implementar correlação de eventos baseada em regras configuráveis.

- 5.3.17. A solução deve suportar análise estatística e agregações de dados.
- 5.3.18. A ferramenta deve permitir análise de tendências e padrões temporais.
- 5.3.19. A solução deve implementar detecção de anomalias baseada em machine learning.
- 5.3.20. A solução deve suportar alertas em tempo real e baseados em agregações históricas.
- 5.3.21. A solução deve permitir integração com sistemas de ticketing.
- 5.3.22. A ferramenta deve suportar notificações via webhook para integração com sistemas externos.
- 5.3.23. A ferramenta deve implementar políticas de retenção configuráveis por tipo de dado.
- 5.3.24. A ferramenta deve permitir exportação de dados em formatos padrão (JSON, CSV).
- 5.3.25. A solução deve implementar autenticação de API via tokens de acesso.
- 5.3.26. A ferramenta deve implementar rate limiting para proteção da API.
- 5.3.27. A solução deve suportar integração com plataformas de threat intelligence.
- 5.3.28. A ferramenta deve permitir integração com ferramentas de SOAR (Security Orchestration).
- 5.3.29. A solução deve suportar integração com sistemas de monitoramento (Nagios, Zabbix).
- 5.3.30. A ferramenta deve permitir integração com plataformas de nuvem (AWS, Azure, GCP).
- 5.3.31. A ferramenta deve implementar criptografia em trânsito (TLS 1.2+) para todas as comunicações.
- 5.3.32. A solução deve suportar criptografia em repouso para dados sensíveis.
- 5.3.33. A ferramenta deve implementar logs de auditoria para todas as ações administrativas.
- 5.3.34. A solução deve suportar segregação de dados por tenant em ambientes multi-tenant. A solução deve suportar retenção de dados conforme regulamentações específicas.
- 5.3.35. A ferramenta deve implementar controles de acesso para atendimento a LGPD/GDPR.
- 5.3.36. A ferramenta deve fornecer métricas de performance e saúde do sistema.
- 5.3.37. A solução deve implementar alertas para problemas de infraestrutura.
- 5.3.38. A ferramenta deve suportar monitoramento de uso de recursos (CPU, memória, disco).
- 5.3.39. A ferramenta deve permitir gerenciamento centralizado de configurações.
- 5.3.40. A solução deve suportar deployment automatizado de configurações.
- 5.3.41. A ferramenta deve implementar versionamento de configurações.
- 5.3.42. A solução deve ser compatível com sistemas operacionais Linux (Ubuntu, CentOS, RHEL).

- 5.3.43. A ferramenta deve suportar deployment em containers (Docker, Kubernetes).
- 5.3.44. A solução deve ser compatível com ambientes on-premises.
- 5.3.45. A ferramenta deve especificar requisitos mínimos de hardware para diferentes volumes de dados.
- 5.3.46. A solução deve fornecer calculadora de dimensionamento baseada em volume de logs.
- 5.3.47. A ferramenta deve especificar todas as dependências de software necessárias.
- 5.3.48. A solução deve fornecer documentação técnica completa em português.
- 5.3.49. A solução deve suportar atualizações automáticas com rollback em caso de problemas.

#### 5.4. **ANÁLISE E DETECÇÃO DE AMEAÇAS**

- 5.4.1. Deve possuir console web para acesso a dashboard de gerenciamento com interface intuitiva e responsiva.
- 5.4.2. A interface web deve ser flexível e permitir mineração, análise e visualização de dados de eventos e alertas de segurança.
- 5.4.3. O dashboard deve permitir navegação através de diferentes tipos de dados coletados pelos agentes de monitoramento.
- 5.4.4. Deve fornecer visualização de alertas de segurança gerados pelo servidor em tempo real.
- 5.4.5. Deve fornecer dashboards pré-configurados para conformidade regulatória.
- 5.4.6. Deve incluir interface para navegação no framework MITRE ATT&CK e alertas relacionados.
- 5.4.7. Deve implementar controle de acesso baseado em funções (RBAC) com granularidade de permissões.
- 5.4.8. Deve incluir monitoramento do Registry do Windows com detecção de alterações maliciosas.
- 5.4.9. Deve implementar detecção de malware através de monitoramento de integridade de arquivos e regras de detecção de ameaças.
- 5.4.10. Deve suportar listas CDB (Custom Database) e integração com feeds de threat intelligence.
- 5.4.11. Deve implementar integração nativa para análise de arquivos suspeitos.
- 5.4.12. Deve fornecer scripts de resposta ativa pré-configurados para cenários comuns.
- 5.4.13. Deve permitir criação e implementação de scripts de resposta ativa customizados.
- 5.4.14. Deve permitir configuração flexível do módulo SCA com políticas personalizáveis.
- 5.4.15. Deve fornecer políticas SCA pré-configuradas para diferentes sistemas operacionais e aplicações.
- 5.4.16. Deve implementar detecção automática de vulnerabilidades em sistemas e aplicações monitorados.

5.4.17. Deve implementar coleta automática de inventário de hardware e software dos sistemas monitorados.

5.4.18. A solução deve implementar arquitetura baseada em agentes executando em endpoints monitorados.

5.4.19. Deve implementar indexação e armazenamento de alertas gerados pelo servidor.

## 5.5. **PLATAFORMA DE GERENCIAMENTO DE SERVIÇOS DE SEGURANÇA**

5.5.1. A CONTRATADA deverá disponibilizar ao CONTRATANTE acesso a uma plataforma centralizada de gerenciamento, que atuará como camada de orquestração e visibilidade unificada para todos os serviços e disciplinas de segurança da informação previstos neste termo de referência.

5.5.2. A plataforma deverá consolidar os dados provenientes do monitoramento de ativos, gestão de vulnerabilidades, inteligência de ameaças e proteção de endpoints, permitindo uma visão convergente entre a saúde da infraestrutura de tecnologia e a postura de cibersegurança da instituição.

5.5.3. A interface de gerenciamento deve ser baseada em navegador web, possuir capacidades de visualização interativa e permitir a realização de drill-down para análises detalhadas e investigação de eventos específicos em tempo real.

5.5.4. **As capacidades esperadas para a plataforma incluem, no mínimo:**

I - Visualização Unificada e Convergente

II - Centralização de indicadores de diferentes fontes de dados em uma única interface, eliminando silos de informação e proporcionando visibilidade completa da superfície de ataque.

### 5.5.5. **Dashboards Executivos e Técnicos**

I - Apresentação de cronogramas de atividades recentes, logs de auditoria e status de conformidade com frameworks de segurança da informação.

### 5.5.6. **Gestão de Desempenho e Acordos de Nível de Serviço (SLA)**

I - Monitoramento analítico da eficiência operacional dos serviços prestados, com exibição de indicadores fundamentais como o Tempo Médio de Detecção (MTTD) e o Tempo Médio de Resposta (MTTR).

II - Painéis específicos para acompanhamento da conformidade de SLA e tendências históricas de incidentes, permitindo a avaliação da evolução da maturidade de segurança ao longo do contrato.

### 5.5.7. **Orquestração de Resposta e Remediação**

I - Integração dos resultados da gestão de vulnerabilidades, permitindo a identificação, classificação por criticidade e acompanhamento do ciclo de vida de remediação de falhas em ativos de TI.

II - Capacidade de correlacionar eventos de segurança com ações proativas de resposta, visando a redução da exposição cibernética através de um fluxo contínuo de identificação, governança, remediação e monitoramento.

### 5.5.8. **Detecção de Anomalias e Inteligência Analítica**

### 5.5.9. **Relatórios Automatizados e Governança**

I - Suporte à avaliação de conformidade regulatória e atendimento a requisitos legais através da documentação histórica de eventos e ações de resposta

tomadas.

## 5.6. **Sistema de Análise de Postura de Segurança da Informação**

5.6.1. O Sistema de Análise de Postura de Segurança da Informação, deve permitir:

- I - Cadastro e gestão de soluções de tecnologia implementadas
- II - Cadastro e gestão de soluções de segurança implementadas
- III - Avaliação de conformidade com PPSI Programa de Privacidade e Segurança a Informação
- IV - Avaliação de conformidade com CIS Controls (v8)
- V - Avaliação de conformidade com MITRE ATT&CK
- VI - Avaliação de conformidade com ISO 27001
- VII - Correlação entre frameworks CIS Controls e MITRE ATT&CK
- VIII - Análise e gestão de riscos de segurança
- IX - Planejamento faseado para implementação de controles
- X - Acompanhamento de evolução de postura de segurança
- XI - Geração de relatórios e recomendações baseadas em inteligência de ameaças

5.6.2. A análise contínua de postura de segurança é essencial para a proteção de dados e infraestrutura de TI, deveser permitir:

- I - Avaliação estruturada e contínua de segurança da informação
- II - Identificação de lacunas de segurança baseada em frameworks internacionais
- III - Correlação entre técnicas de ataque (MITRE ATT&CK) e controles de segurança (CIS)
- IV - Priorização de investimentos em segurança baseada em risco
- V - Planejamento faseado de implementação de controles
- VI - Demonstração de conformidade com regulamentações
- VII - Redução de exposição a ataques cibernéticos
- VIII - Melhoria contínua da postura de segurança
- IX - Otimização de recursos de segurança

## 5.6.3. **CADASTRO DE SOLUÇÕES DE TECNOLOGIA**

- Registro de servidores (quantidade, SO, versão, localização)
- Registro de estações de trabalho (quantidade, SO, versão)
- Registro de dispositivos de rede (firewalls, switches, roteadores, versão)
- Registro de dispositivos móveis (quantidade, tipo, SO)
- Registro de aplicações críticas (nome, versão, responsável)
- Registro de banco de dados (tipo, versão, dados sensíveis)
- Registro de infraestrutura de backup e disaster recovery
- Registro de conectividade e acesso remoto (VPN, RDP, etc.)
- Registro de segmentação de rede

- Importação em massa de dados (Excel, CSV)
- Edição e exclusão de registros
- Histórico de alterações de cada ativo
- Relatório de inventário de tecnologia

#### 5.6.4. CADAstro DE SOLUÇÕES DE SEGURANÇA

- Registro de antivírus/antimalware (versão, data de atualização, cobertura)
- Registro de firewalls (tipo, versão, regras, localização)
- Registro de IDS/IPS (tipo, versão, assinaturas)
- Registro de SIEM (tipo, versão, retenção de logs)
- Registro de WAF (Web Application Firewall)
- Registro de Acesso Remoto (tipo, versão, protocolo) ex.: VPN/ZTNA
- Registro de autenticação multifator (tipo, cobertura)
- Registro de criptografia de dados (tipo, escopo)
- Registro de backup automatizado (frequência, retenção)
- Registro de DLP (Data Loss Prevention)
- Registro de EDR (Endpoint Detection and Response)
- Registro de SOAR (Security Orchestration, Automation and Response)
- Registro de gerenciamento de identidade e acesso (IAM)
- Registro de outras soluções de segurança
- Status de ativação (ativo/inativo)
- Data de implementação
- Responsável pela solução
- Mapeamento com controles CIS
- Mapeamento com técnicas MITRE
- Edição em massa e histórico de alterações

#### 5.6.5. CADAstro DE ATIVOS DE TECNOLOGIA

- Classificação de ativos (crítico, importante, padrão)
- Registro de vulnerabilidades conhecidas
- Registro de patches e atualizações
- Histórico de incidentes relacionados
- Relatório de ativos críticos

#### 5.6.6. AVALIAÇÃO DE CONFORMIDADE DO PPSI

- Suporte aos requisitos e diretrizes do Programa de Privacidade e Segurança da Informação
- Avaliação por nível de maturidade e implementação (ex: 0-3 ou 0-5)
- Descrição detalhada de cada diretriz de privacidade e segurança
- Mapeamento automático com processos, políticas e soluções implementadas

- Anexação de evidências de conformidade (documentos, registros e logs)
- Comentários e notas sobre cada requisito avaliado
- Cálculo automático de score de adequação ao PPSI (0-100%)
- Identificação de riscos críticos, gaps e controles prioritários
- Agrupamento por domínios (ex: Governança, Privacidade, Proteção de Dados e Defesa Cibernética)
- Histórico de avaliações e auditorias anteriores
- Comparação temporal da evolução da conformidade
- Relatório de conformidade do PPSI (incluindo status de adequação à LGPD)
- Exportação em PDF e Excel

#### 5.6.7. AVALIAÇÃO DE CONFORMIDADE CIS CONTROLS

- Suporte a 150+ controles CIS v8
- Avaliação por nível de implementação (0-3)
- Descrição detalhada de cada controle
- Mapeamento automático com soluções implementadas
- Anexação de evidências de implementação
- Comentários e notas sobre cada controle
- Cálculo automático de score de conformidade (0-100%)
- Identificação de controles críticos e prioritários
- Agrupamento por categoria de controle
- Histórico de avaliações anteriores
- Comparação temporal de conformidade
- Relatório de conformidade CIS
- Exportação em PDF e Excel

#### 5.6.8. AVALIAÇÃO MITRE ATT&CK

- Suporte a 200+ técnicas MITRE ATT&CK
- Mapeamento com 14 táticas MITRE
- Correlação com soluções de segurança implementadas
- Correlação com controles CIS
- Identificação de técnicas expostas
- Cálculo de cobertura por tática
- Cálculo de cobertura geral
- Visualização em matriz interativa
- Filtros por tática, técnica, plataforma
- Recomendações de mitigação
- Histórico de evolução de cobertura
- Comparação com benchmark do setor
- Relatório de postura MITRE

- Exportação em PDF e Excel

#### 5.6.9. CORRELAÇÃO ENTRE CIS CONTROLS E MITRE ATT&CK

- Mapeamento completo de 150+ controles CIS com 200+ técnicas MITRE
- Visualização em página única correlacionando ambos frameworks
- Identificação de técnicas expostas por controle não implementado
- Análise de lacunas de segurança
- Recomendações de controles prioritários
- Visualização de impacto de cada controle
- Priorização automática de implementação
- Relatório de correlação CIS-MITRE
- Exportação de matriz de correlação

#### 5.6.10. AVALIAÇÃO E GESTÃO DE RISCOS

- Cadastro de riscos identificados
- Classificação de riscos (Técnico, Operacional, Estratégico)
- Avaliação de probabilidade (1-5)
- Avaliação de impacto (1-5)
- Cálculo automático de score de risco (Probabilidade × Impacto)
- Status de risco (Aberto, Mitigado, Aceito, Eliminado)
- Proprietário do risco
- Plano de mitigação
- Matriz de risco interativa (5×5)
- Visualização de riscos por categoria
- Filtros por status e severidade
- Histórico de alterações de risco
- Associação de controles a riscos
- Cálculo de redução de risco por controle
- Relatório de análise de riscos
- Exportação em PDF e Excel

#### 5.6.11. ACOMPANHAMENTO DE EVOLUÇÃO DE POSTURA DE SEGURANÇA

- Dashboard de conformidade geral (0-100%)
- Score por framework (CIS, MITRE, ISO 27001)
- Comparação de scores entre avaliações
- Alertas de tendência negativa
- Relatório de evolução de postura
- KPIs de segurança
- Exportação de gráficos e relatórios

### 5.7. REQUISITOS TÉCNICOS COMPROVADOS DA PLATAFORMA DE DEFESA CIBERNÉTICA

5.7.1. Os requisitos relacionados nesta seção correspondem a funcionalidades efetivamente comprovadas na Matriz de Comprovação Técnica da plataforma de defesa cibernética, com indicação de documento, página e seção que evidenciam cada item, e integram o escopo mínimo exigível da SOLUÇÃO.

#### 5.7.2. **Arquitetura, implantação e escalabilidade**

5.7.2.1. A SOLUÇÃO deverá ser plataforma unificada de defesa cibernética, operada a partir de console único, que concentre em uma mesma experiência integrada o monitoramento de segurança, a análise de postura, a governança, a gestão de risco, o compliance, a correlação de eventos de segurança (SIEM), a gestão de vulnerabilidades e a inteligência de ameaças, vedada a entrega por meio de ferramentas independentes sem integração entre si.

5.7.2.2. A SOLUÇÃO deverá ser organizada em módulos integrados sob núcleo comum, contemplando no mínimo: operação de segurança em tempo real, priorização de vulnerabilidades por risco, governança de risco e compliance, e inteligência de ameaças, todos acessíveis pelo mesmo console e apoiados na mesma base de dados.

5.7.2.3. A SOLUÇÃO não deverá ser fornecida em modalidade de serviço gerenciado em nuvem.

5.7.2.4. A SOLUÇÃO deverá admitir, alternativamente, implantação em infraestrutura própria do CONTRATANTE, seja local ou em nuvem privada sob sua guarda, por meio de containers, com administração integral da solução pela equipe do CONTRATANTE, de modo a atender requisitos de soberania de dados.

5.7.2.5. Na implantação em infraestrutura própria, a SOLUÇÃO deverá operar sobre componentes de banco de dados relacional e de cache em memória, com containers endurecidos.

5.7.2.6. A SOLUÇÃO deverá possuir mecanismo de alta disponibilidade que a mantenha operante e responsiva ainda que as fontes externas de dados fiquem indisponíveis, mediante sincronização dos dados para base local e entrega por camada de cache.

5.7.2.7. As consultas realizadas pelas telas da SOLUÇÃO deverão ser atendidas a partir da base local ou da camada de cache, de modo que o tempo de resposta ao usuário não dependa da latência ou da disponibilidade das fontes externas no instante da consulta.

5.7.2.8. A SOLUÇÃO deverá ser construída sobre arquitetura preparada para crescimento de volume, com processamento em segundo plano e camada de cache que preservem desempenho e disponibilidade sob alta carga.

5.7.2.9. A documentação técnica da SOLUÇÃO deverá ser fornecida integralmente em português do Brasil.

#### 5.7.3. **Multilocação (multi-tenant) e isolamento de dados**

5.7.3.1. A SOLUÇÃO deverá adotar arquitetura multilocatária (multi-tenant) com isolamento total dos dados entre as organizações atendidas, vedado o compartilhamento de dados entre locatários.

5.7.3.2. Cada organização atendida deverá operar com banco de dados dedicado, de modo que o isolamento seja assegurado na camada de persistência e não apenas por filtro de aplicação.

5.7.3.3. Cada organização atendida deverá operar com instância de cache dedicada, assegurando que os dados em memória também permaneçam segregados por locatário.

5.7.3.4. A SOLUÇÃO deverá oferecer nível de visão consolidada, na forma de locatário virtual ou visão global, que agregue os indicadores de todas as organizações atendidas para a equipe responsável pela operação, sem misturar os dados de cada locatário nas visões individuais.

5.7.3.5. A SOLUÇÃO deverá dispor de função de administração multilocatária, com provisionamento e manutenção das organizações atendidas pela própria interface administrativa.

5.7.3.6. O isolamento de dados por organização deverá integrar os controles de segurança e governança da SOLUÇÃO, e não apenas a sua arquitetura de dados.

#### 5.7.4. **Coleta de telemetria e cobertura de ativos**

5.7.4.1. A SOLUÇÃO deverá realizar coleta de telemetria por agentes nativos para os sistemas operacionais Windows, Linux e macOS.

5.7.4.2. A SOLUÇÃO deverá disponibilizar instaladores dedicados para cada sistema operacional suportado pelos agentes de coleta.

5.7.4.3. A coleta por agentes deverá abranger estações de trabalho e servidores, permitindo detecção em ambos os tipos de ativo.

5.7.4.4. A SOLUÇÃO deverá apresentar painel do parque de agentes em tempo real, discriminando no mínimo os estados ativo, desconectado, nunca conectado e pendente.

5.7.4.5. Para cada agente, a SOLUÇÃO deverá manter e exibir a versão instalada, o sistema operacional e a data e hora do último sinal de atividade.

5.7.4.6. A SOLUÇÃO deverá sinalizar automaticamente os agentes com versão desatualizada.

5.7.4.7. A SOLUÇÃO deverá permitir a exportação do inventário de agentes em formato CSV.

5.7.4.8. A SOLUÇÃO deverá integrar-se, por interface de programação de aplicações, a fontes externas de telemetria e de inteligência, incorporando os dados coletados às suas próprias análises.

5.7.4.9. A SOLUÇÃO deverá incorporar, por integração, métricas de disponibilidade e de capacidade da infraestrutura, convergindo-as com os demais dados para priorização de ações.

#### 5.7.5. **Monitoramento, detecção e correlação de eventos**

5.7.5.1. A SOLUÇÃO deverá centralizar alertas, regras de detecção e técnicas de ataque associadas, com políticas de retenção e rotinas de sincronização automatizadas.

5.7.5.2. A SOLUÇÃO deverá apresentar resumo dos alertas por severidade referente às últimas 24 horas.

5.7.5.3. A SOLUÇÃO deverá identificar automaticamente picos de alertas no período monitorado.

5.7.5.4. A SOLUÇÃO deverá apresentar a evolução temporal dos alertas com análise de tendência em janelas de 7 e de 30 dias.

5.7.5.5. A SOLUÇÃO deverá apresentar ranking das regras de detecção que mais dispararam e dos ativos que mais geram alertas.

5.7.5.6. A SOLUÇÃO deverá correlacionar os alertas por nível ou severidade da regra e identificar automaticamente candidatos a falso positivo, subsidiando o ajuste contínuo das detecções.

5.7.5.7. A SOLUÇÃO deverá consultar os dados em tempo real das fontes integradas e sinalizar automaticamente, por indicador de atualidade, quando uma fonte estiver indisponível ou com dados defasados.

5.7.5.8. A SOLUÇÃO deverá oferecer visão consolidada por ativo, reunindo os últimos alertas, as vulnerabilidades identificadas e as técnicas de ataque associadas ao mesmo ativo.

5.7.5.9. A SOLUÇÃO deverá disponibilizar dados forenses de rede por ativo, contemplando endereços IP, portas, protocolos e geolocalização, apresentados em linha do tempo de atividades.

5.7.5.10. A SOLUÇÃO deverá apresentar fluxo de eventos em tempo real com fila de priorização por classe, controle de prazo por evento e ranking das regras acionadas, permitindo aprofundamento investigativo a partir do próprio fluxo.

5.7.5.11. A SOLUÇÃO deverá dispor de mecanismo de busca e indexação de alto desempenho sobre grandes volumes de eventos.

5.7.5.12. A priorização do fluxo de eventos deverá considerar impacto, urgência e confiança da detecção.

#### 5.7.6. **Cobertura MITRE ATT&CK e maturidade de detecção**

5.7.6.1. A SOLUÇÃO deverá classificar as detecções segundo táticas e técnicas do framework MITRE ATT&CK, apresentando a distribuição resultante.

5.7.6.2. A SOLUÇÃO deverá calcular e apresentar o percentual de cobertura de detecção em relação ao conjunto de técnicas do MITRE ATT&CK Enterprise.

5.7.6.3. A SOLUÇÃO deverá identificar e priorizar as lacunas de detecção nas táticas mais críticas.

5.7.6.4. A SOLUÇÃO deverá apresentar a trajetória do alerta desde a fonte até a conclusão do tratamento, mapeada sobre as táticas do MITRE ATT&CK.

5.7.6.5. As hipóteses de caça a ameaças deverão ser associadas a táticas e técnicas do MITRE ATT&CK.

5.7.6.6. A SOLUÇÃO deverá apresentar avaliação de conformidade técnica da configuração dos ativos frente a linhas de base de segurança reconhecidas, com pontuação por ativo.

#### 5.7.7. **Gestão de vulnerabilidades**

5.7.7.1. A SOLUÇÃO deverá apresentar a distribuição da base de vulnerabilidades por faixa de criticidade CVSS, contemplando crítica, alta, média e baixa, com histograma por pontuação e aprofundamento por severidade.

5.7.7.2. A SOLUÇÃO deverá relacionar as vulnerabilidades mais críticas identificadas com a respectiva pontuação CVSS e a quantidade de ativos afetados.

5.7.7.3. A SOLUÇÃO deverá cruzar a base de vulnerabilidades com catálogo público de vulnerabilidades exploradas ativamente, destacando os itens nele listados.

5.7.7.4. A SOLUÇÃO deverá apresentar ranking dos ativos mais vulneráveis, informando a contagem de vulnerabilidades críticas e altas, o sistema operacional e a pontuação de risco de cada ativo.

5.7.7.5. A SOLUÇÃO deverá medir a cobertura de correções frente à meta estabelecida, segmentando por sistema operacional e por ativo, e rastreando os ativos críticos ainda sem correção.

5.7.7.6. A SOLUÇÃO deverá apresentar gráfico de redução acumulada das

vulnerabilidades críticas abertas e fechadas ao longo do tempo, com linha de previsão, meta de resolução e apuração das novas e das fechadas nos últimos 7 dias.

5.7.7.7. A SOLUÇÃO deverá controlar prazos de remediação por severidade, apurando o percentual de conformidade e o status individual de cada vulnerabilidade.

5.7.7.8. A SOLUÇÃO deverá priorizar automaticamente as violações de prazo de remediação, apresentando-as em fila de ação.

5.7.7.9. A SOLUÇÃO deverá apresentar a tendência de 30 dias do cumprimento dos prazos de remediação.

5.7.7.10. A SOLUÇÃO deverá apresentar filas de ação ordenadas por impacto, orientando a sequência de tratamento.

5.7.7.11. As vulnerabilidades identificadas deverão estar acessíveis também pela visão individual do ativo, associadas aos respectivos alertas e técnicas de ataque.

#### 5.7.8. **Governança de risco e resposta a incidentes**

5.7.8.1. A SOLUÇÃO deverá apresentar matriz de risco cruzando probabilidade e impacto, com codificação por cores e plotagem dos incidentes conforme a severidade.

5.7.8.2. A SOLUÇÃO deverá destacar, em fila prioritária, os incidentes de maior risco apurado.

5.7.8.3. A SOLUÇÃO deverá realizar análise de causa raiz dos incidentes, com agrupamento por causa, ranking de frequência, identificação da severidade dominante por causa e tendência ao longo do tempo.

5.7.8.4. A SOLUÇÃO deverá apresentar recomendações de ações preventivas decorrentes da análise de causa raiz.

5.7.8.5. A SOLUÇÃO deverá controlar prazos de resposta a incidentes por severidade, apresentando o status individual de cada incidente, a conformidade consolidada e a tendência do indicador.

5.7.8.6. A SOLUÇÃO deverá apurar o tempo médio de resposta agrupado por categoria de incidente, com média, percentual, distribuição de severidade, linha de referência da meta e destaque dos melhores e piores desempenhos.

5.7.8.7. A SOLUÇÃO deverá calcular e apresentar pontuação de risco consolidada da postura de segurança da organização.

5.7.8.8. A SOLUÇÃO deverá apresentar análise de conformidade do ambiente e apoiar a adequação a frameworks e normas de segurança da informação.

5.7.8.9. A priorização apresentada pela SOLUÇÃO deverá considerar o impacto no negócio.

5.7.8.10. A SOLUÇÃO deverá registrar e acompanhar a resposta a incidentes de segurança até a conclusão do tratamento.

#### 5.7.9. **Indicadores, análise e relatórios**

5.7.9.1. A SOLUÇÃO deverá apresentar indicadores executivos no topo de cada tela de análise.

5.7.9.2. A SOLUÇÃO deverá gerar insights executivos com priorização automática, indicando os pontos que exigem atenção imediata.

5.7.9.3. A SOLUÇÃO deverá permitir aprofundamento investigativo do panorama consolidado até o detalhe do registro individual em poucos cliques.

5.7.9.4. A SOLUÇÃO deverá disponibilizar gráficos interativos de evolução e de tendência.

5.7.9.5. A SOLUÇÃO deverá apresentar filas de ação priorizadas nas telas de análise, com indicação do que deve ser tratado primeiro.

5.7.9.6. A SOLUÇÃO deverá disponibilizar relatórios em tempo real e relatórios históricos.

5.7.9.7. A SOLUÇÃO deverá permitir a exportação dos dados apresentados em formato CSV.

5.7.9.8. A SOLUÇÃO deverá apurar os indicadores de tempo médio de reconhecimento, de detecção e de resposta frente às metas de nível de serviço estabelecidas.

5.7.9.9. A SOLUÇÃO deverá apurar taxa de acurácia, volume de alertas tratados, quantidade de analistas ativos e conformidade frente às metas, com tendência de 30 dias.

5.7.9.10. A SOLUÇÃO deverá apresentar indicadores de desempenho por analista, permitindo a gestão da equipe de operação por dados.

5.7.9.11. A SOLUÇÃO deverá dispor de painel executivo consolidando superfície de ataque, pontuação de risco e incidentes críticos priorizados.

5.7.9.12. A SOLUÇÃO deverá fornecer métricas executivas que permitam comprovar a postura de segurança à alta administração.

#### 5.7.10. **Controle de acesso, segurança e auditoria**

5.7.10.1. A autenticação dos usuários da SOLUÇÃO deverá ser realizada por token assinado.

5.7.10.2. A SOLUÇÃO deverá exigir segundo fator de autenticação baseado em senha de uso único por tempo, de forma obrigatória para todos os usuários.

5.7.10.3. A SOLUÇÃO deverá implementar controle de acesso baseado em papéis, com perfis distintos de administração e de uso e possibilidade de perfil com acesso à visão global.

5.7.10.4. A SOLUÇÃO deverá manter gestão das sessões de usuário, permitindo o seu controle e encerramento.

5.7.10.5. A SOLUÇÃO deverá manter trilha de auditoria completa de todas as ações praticadas pelos usuários.

5.7.10.6. A SOLUÇÃO deverá aplicar cabeçalhos de segurança nas respostas da aplicação web.

5.7.10.7. A SOLUÇÃO deverá permitir a gestão de usuários, papéis e permissões pela própria interface de administração.

5.7.10.8. Os controles de autenticação, autorização e auditoria deverão integrar a arquitetura da SOLUÇÃO como configuração padrão, e não como componente opcional.

#### 5.7.11. **Sincronização, retenção e administração**

5.7.11.1. A SOLUÇÃO deverá dispor de agendador de rotinas em segundo plano que sincronize agentes, alertas, vulnerabilidades e métricas em intervalos otimizados, sem intervenção manual.

5.7.11.2. A SOLUÇÃO deverá monitorar e exibir o status das rotinas de sincronização.

5.7.11.3. A SOLUÇÃO deverá permitir a configuração de políticas de retenção de dados, com rotina automatizada de limpeza dos dados que excederem o período definido.

5.7.11.4. A SOLUÇÃO deverá permitir a gestão dos agentes de coleta e das fontes de dados pela própria interface de administração.

5.7.11.5. A SOLUÇÃO deverá utilizar cache em duas camadas para assegurar desempenho e disponibilidade das consultas.

5.7.11.6. A SOLUÇÃO deverá sinalizar automaticamente, por indicador próprio, a indisponibilidade ou a defasagem dos dados de cada fonte integrada.

## **6. INDICADORES DE NÍVEIS DE SERVIÇO E NÍVEIS MÍNIMOS DE SERVIÇO (INS/NMS)**

### **6.1. Diretrizes Gerais**

6.1.1. A CONTRATADA deverá garantir a prestação dos serviços com base em indicadores objetivos de desempenho, mensurados continuamente e vinculados a níveis mínimos de serviço (NMS, conforme diretrizes do modelo de contratação de TIC do SISP.

6.1.2. Os indicadores definidos nesta seção terão caráter obrigatório e serão utilizados para:

- a) aferição da qualidade dos serviços prestados;
- b) verificação do cumprimento contratual;
- c) aplicação de penalidades e ajustes financeiros;
- d) suporte à governança e à tomada de decisão da CONTRATANTE.

6.1.3. Todos os indicadores deverão ser mensurados de forma automatizada, com base em dados coletados pela própria plataforma ou por mecanismos independentes de monitoramento, garantindo rastreabilidade, auditabilidade e reprodutibilidade dos resultados.

6.1.4. A CONTRATADA deverá disponibilizar dashboards e relatórios contendo a apuração dos indicadores, com atualização em tempo real ou periodicidade mínima diária.

6.2. Os indicadores relacionados a seguir tem relação direta a estas especificações e estão detalhados no Apêndice V, do ETP 6/2026:

- I. INS11 - Tempo Médio de Resposta Autônoma (MTTA-AI)
- II. INS 12 - Taxa de Resolução Autônoma de Incidentes
- III. INS 13 — Disponibilidade da Plataforma da CONTRATADA

### **6.3. Consolidação e Apuração dos Indicadores**

6.3.1. A apuração dos indicadores será realizada mensalmente.

6.3.2. A CONTRATADA deverá apresentar relatório consolidado contendo:

- a) valor apurado de cada indicador;
- b) memória de cálculo detalhada;
- c) eventos considerados e excluídos;
- d) evidências técnicas associadas;

6.3.3. A CONTRATANTE poderá auditar, a qualquer tempo, os dados utilizados

na apuração dos indicadores.

6.4. Disposições Complementares

6.4.1. O não atingimento das metas estabelecidas implicará aplicação de penalidades contratuais, conforme tabela de faixas de desempenho a ser definida em instrumento específico.

6.4.2. Disposições Complementares

6.4.3. Todos os dados utilizados na mensuração dos indicadores são de propriedade da CONTRATANTE.

6.4.4. A CONTRATADA deverá garantir a integridade, disponibilidade e rastreabilidade dos dados de medição por todo o período contratual.

6.4.5. A CONTRATADA deverá disponibilizar acesso à CONTRATANTE para consulta em tempo real dos indicadores.

7. PROVA DE CONCEITO - POC

7.1. Os requisitos da prova de conceito estão separados por ferramenta, na mesma ordem das seções deste Apêndice. A LICITANTE deverá demonstrar cada requisito e assinalar Sim ou Não, registrando na coluna Observação a evidência apresentada.

7.2. Solução de Gerenciamento de Serviços de TIC (ITSM)

7.2.1. A Tabela a seguir apresenta a lista de requisitos da Solução de Gerenciamento de Serviços de TIC que deverão ser demonstrados pela LICITANTE, obrigatoriamente de forma presencial na sede do ITI durante a realização da prova de conceito:

| Requisitos da Prova de Conceito |                             |                                                                                                                                                                                              | Conformidade de Atendimento |     |
|---------------------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|-----|
| Nº                              | Tipo                        | Requisito                                                                                                                                                                                    | Sim                         | Não |
| 1                               | Gestão de Serviços e Ativos | Os serviços cadastrados devem permitir o vínculo com ativos suportados.                                                                                                                      |                             |     |
| 2                               | Gestão de Serviços e Ativos | Os serviços cadastrados devem permitir o vínculo do Cliente demandante do serviço.                                                                                                           |                             |     |
| 4                               | Gestão de Serviços e Ativos | Os acordos de nível de serviço devem ser vinculados ao serviço e exibidos no próprio dossiê do serviço, de modo que o analista tenha acesso imediato a prazos e metas durante o atendimento. |                             |     |
| 5                               | Gestão de Serviços e Ativos | O cadastro do serviço deve permitir o vínculo com contrato.                                                                                                                                  |                             |     |
| 6                               | Gestão de Serviços e Ativos | Deve possuir relatório de ativos vinculados a serviços.                                                                                                                                      |                             |     |
| 7                               | Gestão de Serviços e Ativos | O cadastro do ativo e o cadastro do serviço devem permitir o vínculo com contrato, inclusive para serviços gerenciados.                                                                      |                             |     |

|    |                                    |                                                                                                                                                                                                                                                                                                           |  |  |
|----|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|    |                                    |                                                                                                                                                                                                                                                                                                           |  |  |
|    |                                    |                                                                                                                                                                                                                                                                                                           |  |  |
| 8  | Gestão de Serviços e Ativos        | O cadastro do ativo deve conter nome, tipo, fabricante, modelo, número de série, contrato, localização e etiqueta de patrimônio, e deve permitir a geração de etiqueta com QR Code que dê acesso direto à abertura de chamado para aquele ativo.                                                          |  |  |
| 9  | Gestão de Incidentes e Requisições | Deve apresentar os indicadores do próprio serviço: total de chamados, incidentes, requisições, chamados abertos, prazos estourados e tempo médio de solução.                                                                                                                                              |  |  |
| 10 | Gestão de Incidentes e Requisições | A solução deve notificar requerentes, analistas e observadores quando o chamado ultrapassar o percentual do prazo de solução definido pela Gestão da Instituição, com verificação a cada 15 minutos e percentual parametrizável, adotado 95% como padrão.                                                 |  |  |
| 11 | Gestão de Incidentes e Requisições | A solução deve enviar notificação diária aos administradores com a relação dos chamados pendentes há mais tempo que o período definido pela Gestão da Instituição, informando os dias de pendência e o responsável por cada chamado.                                                                      |  |  |
| 12 | Gestão de Incidentes e Requisições | A solução deve encerrar automaticamente os chamados pendentes há mais tempo que o período definido pela Gestão da Instituição, com a rotina desligada por padrão até que a Gestão defina o prazo.                                                                                                         |  |  |
| 14 | Gestão de Incidentes e Requisições | A solução deve possuir painel nativo do processo de gestão de incidentes contendo, no mínimo, volume de incidentes registrados, volume de incidentes encerrados, tempo médio de solução, tempo médio de atribuição, satisfação média e incidentes solucionados sem uso de artigo da base de conhecimento. |  |  |
| 16 | Gestão de Incidentes e Requisições | A solução deve possuir painel de desempenho da equipe na gestão de requisições.                                                                                                                                                                                                                           |  |  |
| 17 | Gestão de Problemas                | A solução deve permitir a criação do Relatório de Causa Raiz dentro do registro do problema, com estado próprio, separado do status do problema.                                                                                                                                                          |  |  |
| 18 | Gestão de Problemas                | O Relatório de Causa Raiz deve possuir campo para o registro técnico da ocorrência, de preenchimento obrigatório para o encerramento.                                                                                                                                                                     |  |  |

|    |                                         |                                                                                                                                                                                                                                                                                                     |  |  |
|----|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|    |                                         |                                                                                                                                                                                                                                                                                                     |  |  |
|    |                                         |                                                                                                                                                                                                                                                                                                     |  |  |
| 19 | Gestão de Problemas                     | O Relatório de Causa Raiz deve possuir campo para o registro da solução de contorno, de preenchimento obrigatório para o encerramento.                                                                                                                                                              |  |  |
| 20 | Gestão de Problemas                     | O Relatório de Causa Raiz deve possuir campo para o registro da evidência que identificou a causa raiz, de preenchimento obrigatório para o encerramento.                                                                                                                                           |  |  |
| 21 | Gestão de Problemas                     | O Relatório de Causa Raiz deve possuir campo para o plano de ação contra a recorrência do problema em produção, de preenchimento obrigatório para o encerramento.                                                                                                                                   |  |  |
| 22 | Gestão de Problemas                     | O problema somente poderá ser encerrado com o Relatório de Causa Raiz já encerrado, com a trava aplicada no servidor e não apenas na interface.                                                                                                                                                     |  |  |
| 23 | Gestão de Problemas                     | O Relatório de Causa Raiz somente poderá ser encerrado com todos os seus campos preenchidos, e a mensagem de recusa deve nomear os campos que faltam.                                                                                                                                               |  |  |
| 24 | Gestão de Mudanças                      | A solução deve possuir formulário de registro de mudanças contendo plano de implantação, plano de reversão, comitê de aprovação e janela planejada.                                                                                                                                                 |  |  |
| 25 | Gestão de Mudanças                      | A solução deve permitir a tipificação da mudança entre Normal, Pré-aprovada, Emergencial e Planejada.                                                                                                                                                                                               |  |  |
| 26 | Gestão de Mudanças                      | Para cada item de configuração impactado pela mudança, a solução deve permitir o registro descritivo do impacto numa visão otimista e do impacto numa visão pessimista, mantidos no vínculo entre a mudança e o IC, de modo que a mesma mudança possa ser avaliada de forma distinta em cada ativo. |  |  |
| 27 | Aprovações e Notificações Automatizadas | A solução deve enviar periodicamente, por e-mail, relatório de desempenho da equipe ao gestor marcado no cadastro da própria equipe, recaindo nos administradores quando não houver gestor marcado.                                                                                                 |  |  |
| 28 | Aprovações e Notificações Automatizadas | A solução deve enviar por e-mail aos responsáveis pelas unidades de negócio o desempenho da entrega de serviços em sua unidade, contendo volume, resolvidos, prazos estourados e satisfação.                                                                                                        |  |  |

|    |                                         |                                                                                                                                                                                                                                                                                                                               |  |  |
|----|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|    |                                         |                                                                                                                                                                                                                                                                                                                               |  |  |
|    |                                         |                                                                                                                                                                                                                                                                                                                               |  |  |
| 29 | Aprovações e Notificações Automatizadas | A solução deve enviar e-mail diário aos usuários com aprovações pendentes, limitado a um lembrete por aprovador por dia.                                                                                                                                                                                                      |  |  |
| 30 | Aprovações e Notificações Automatizadas | A solução deve permitir ao administrador estipular o prazo máximo, em dias, que o chamado pode permanecer aguardando aprovação e, esgotado o prazo, encerrar o chamado por não aprovação.                                                                                                                                     |  |  |
| 31 | Aprovações e Notificações Automatizadas | A solução deve notificar diariamente os usuários que ainda possuam pendências de aprovação em chamados abertos.                                                                                                                                                                                                               |  |  |
| 32 | Aprovações e Notificações Automatizadas | A solução deve permitir a aprovação ou a reprovação do chamado diretamente pelo e-mail, por link de uso único por aprovador, sem exigir acesso à ferramenta e sem que o link sirva uma segunda vez.                                                                                                                           |  |  |
| 33 | Relatórios e Dashboards                 | A solução deve possuir módulo de relatórios e painéis para a tomada de decisão da Gestão, com exportação em PDF e painéis executivo, tático e operacional.                                                                                                                                                                    |  |  |
| 34 | Relatórios e Dashboards                 | A solução deve produzir indicadores a partir de coleta em formatos abertos, permitindo ao administrador cadastrar a fonte em endpoint XML ou JSON, com autenticação opcional, informar os caminhos do documento, conferir o valor lido em pré-visualização antes de salvar e agendar a coleta, tudo sem desenvolvimento.      |  |  |
| 35 | Relatórios e Dashboards                 | A solução deve permitir a vinculação entre indicadores e relatórios, com o relatório montado pelo administrador bloco a bloco, atualização automática da leitura no intervalo definido e alternância entre os níveis de detalhamento global, parcial e individual sem recarregar a página.                                    |  |  |
| 36 | Relatórios e Dashboards                 | A solução deve permitir ao administrador configurar gráficos comparativos com visualização web, contemplando ao menos oito tipos de gráfico, eixo por rótulo, por agrupamento ou por tempo, até oito séries com cor própria, empilhamento, legenda, rótulo de valor e linha de meta, com prévia redesenhada a cada alteração. |  |  |

|    |                                           |                                                                                                                                                                                                                                                                                                                                        |  |  |
|----|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|    |                                           |                                                                                                                                                                                                                                                                                                                                        |  |  |
|    |                                           |                                                                                                                                                                                                                                                                                                                                        |  |  |
| 37 | Relatórios e Dashboards                   | A solução deve manter o histórico de cada indicador por rodada de coleta, com meta e sentido definidos, apresentar a evolução no tempo com a linha de meta e sinalizar, em cada leitura, o desvio em relação à meta.                                                                                                                   |  |  |
| 38 | Relatórios e Dashboards                   | A solução deve possuir painel de análise de performance por Grupo contendo requisições abertas, encerradas e solucionadas por dia, incidentes abertos, encerrados e solucionados por dia, as dez maiores categorias, os chamados fora do prazo, o total de chamados, os integrantes do grupo e a divisão entre dentro e fora do prazo. |  |  |
| 39 | Relatórios e Dashboards                   | A solução deve possuir relatório de desempenho por analista, com a quantidade de chamados atendidos, resolvidos, o tempo médio de atendimento e a aderência ao acordo de nível de serviço.                                                                                                                                             |  |  |
| 40 | Autenticação e Integrações de Comunicação | A solução deve permitir, inclusive em ambiente de nuvem, a autenticação de usuários via SSO de forma segura.                                                                                                                                                                                                                           |  |  |
| 43 | Autenticação e Integrações de Comunicação | A solução deve permitir a autenticação por OAuth2 com Google, Microsoft, cabendo ao CONTRATANTE registrar o aplicativo e informar o identificador e o segredo do cliente.                                                                                                                                                              |  |  |
| 45 | Autenticação e Integrações de Comunicação | A solução deve permitir ao administrador definir os domínios válidos para a autenticação por OAuth, com aceite de subdomínio, e deve recusar a ativação da criação automática de usuários sem lista de domínios definida.                                                                                                              |  |  |
| 46 | Autenticação e Integrações de Comunicação | A solução deve bloquear todo acesso não configurado pelo administrador, mantendo o provedor desligado por padrão, não iniciando o fluxo sem credencial cadastrada e recusando e-mail desconhecido quando a criação automática estiver desligada.                                                                                       |  |  |
| 48 | Autenticação e Integrações de Comunicação | A solução deve enviar notificações de atualização de chamado por WhatsApp, pela Cloud API da Meta, com ou sem uso de template, cabendo ao CONTRATANTE o número comercial verificado, o template aprovado e o token de acesso.                                                                                                          |  |  |

|    |                                           |                                                                                                                                                                                               |  |  |
|----|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|    |                                           |                                                                                                                                                                                               |  |  |
|    |                                           |                                                                                                                                                                                               |  |  |
| 49 | Autenticação e Integrações de Comunicação | A solução deve enviar notificações de atualização de chamado via Telegram, configurável na tela com token de bot e chat de destino e com teste de conexão.                                    |  |  |
| 50 | Autenticação e Integrações de Comunicação | A solução deve enviar notificações de atualização de chamado via Microsoft Teams, por webhook de entrada, com roteamento por equipe.                                                          |  |  |
| 51 | Monitoria                                 | A SOLUÇÃO deve disponibilizar painéis de monitoramento de status de chamado para monitoria e acompanhamento, com indicadores e alertas, permitindo interação direto pela pagina de monitoria. |  |  |
| 52 | Relatórios                                | Personalização com logo, período e SLA, INS, relatório completos gerados em PDF.                                                                                                              |  |  |

### 7.3. **Plataforma de Monitoramento Avançado com IA para Operações de TI (AIOps)**

| Requisitos da Prova de Conceito |                                 |                                                | Conformidade de Atendimento |     |
|---------------------------------|---------------------------------|------------------------------------------------|-----------------------------|-----|
| Nº                              | Tipo                            | Requisito                                      | Sim                         | Não |
| 53                              | Descoberta automática           | Descobrir ativo (VM/Container) automaticamente |                             |     |
| 54                              | Discovery em tempo real         | Identificar ativo ao ser criado                |                             |     |
| 55                              | Mapa de dependência             | Construir relação entre app, serviço e infra   |                             |     |
| 56                              | Identificação de criticidade    | Classificar ativo crítico                      |                             |     |
| 57                              | Monitoramento de aplicação      | Coletar métricas (tempo resposta, erro)        |                             |     |
| 58                              | Distributed tracing             | Rastrear transação ponta a ponta               |                             |     |
| 59                              | Deteção de anomalia             | Detectar degradação sem threshold manual       |                             |     |
| 60                              | Correlação de eventos           | Agrupar eventos relacionados                   |                             |     |
| 61                              | Identificação causa raiz        | Identificar origem da falha                    |                             |     |
| 62                              | Criação automática de incidente | Evento gera incidente automaticamente          |                             |     |
| 63                              | Associação com CMDB             | Relacionar incidente ao ativo                  |                             |     |

|      |                             |                                                                                                                                                |  |  |
|------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|      |                             |                                                                                                                                                |  |  |
| 64   | Análise com base histórica  | Correlacionar com eventos anteriores                                                                                                           |  |  |
| 65   | Base de conhecimento        | Correlacionar com eventos anteriores                                                                                                           |  |  |
| 66   | Execução automática         | Executar playbook de correção                                                                                                                  |  |  |
| 67   | Remediação autônoma         | Resolver incidente sem intervenção humana                                                                                                      |  |  |
| 68   | Ajuste preditivo            | Antecipar degradação futura                                                                                                                    |  |  |
| 69   | Atualização do estado       | Atualizar status após correção                                                                                                                 |  |  |
| 70   | Visão unificada             | Navegar entre aplicação, evento e infra                                                                                                        |  |  |
| 71   | Integração cloud/on-prem    | Navegar entre aplicação, evento e infra                                                                                                        |  |  |
| 72   | Aprendizado contínuo        | IA melhora após execução                                                                                                                       |  |  |
| 72.1 | Topologia física e lógica   | Apresentar, no mesmo grafo de dependências, ativo de armazenamento, empilhamento de comutadores e componente de nuvem pública                  |  |  |
| 72.2 | Agente sem porta em escuta  | Demonstrar que o componente instalado nos ativos monitorados não mantém porta de serviço em escuta                                             |  |  |
| 72.3 | Reconciliação de inventário | Descobrir o mesmo ativo por dois métodos distintos e consolidá-lo em um único item de configuração, com registro da fonte que prevaleceu       |  |  |
| 72.4 | Triagem de eventos          | Demonstrar o registro distinto entre a caracterização do evento e a decisão de acionamento, com apuração da taxa de supressão por fonte        |  |  |
| 72.5 | Autonomia graduada          | Configurar a mesma ação como automática em um ambiente e sujeita a aprovação em outro, sem desenvolvimento                                     |  |  |
| 72.6 | Auditabilidade da decisão   | Reconstituir integralmente uma decisão automatizada a partir dos dados persistidos (entrada, raciocínio, ação, parâmetros, resultado e modelo) |  |  |

#### 7.4. Plataforma de Orquestração de Conhecimento com LLMs em Low-Code e LLMOps

| Requisitos da Prova de Conceito |                                           |                                                                                                                                                        | Conformidade de Atendimento |     |
|---------------------------------|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|-----|
| Nº                              | Tipo                                      | Requisito                                                                                                                                              | Sim                         | Não |
| 73                              | Geração de resposta com RAG               | O sistema deverá responder a consulta utilizando base de conhecimento previamente ingerida, por meio de mecanismo RAG (Retrieval-Augmented Generation) |                             |     |
| 71                              | Segurança contra prompt injection         | O sistema deverá identificar e bloquear tentativas de manipulação do modelo por meio de prompts maliciosos                                             |                             |     |
| 75                              | Orquestração multi-LLM                    | A plataforma deverá executar requisição utilizando modelo e no mesmo fluxo utilizar outro modelo para sequência da tarefa                              |                             |     |
| 76                              | Execução de fluxo automatizado com IA     | O sistema deverá executar fluxo de trabalho definido em linguagem natural, envolvendo múltiplas etapas automatizadas com uso de IA                     |                             |     |
| 77                              | Geração automatizada de documento técnico | O sistema deverá gerar documento técnico estruturado a partir de dados reais (ex.: incidente, logs ou métricas)                                        |                             |     |
| 77.1                            | Consulta em linguagem natural             | Formular consulta analítica em linguagem natural sobre base conectada, exibindo a consulta estruturada gerada antes da execução                        |                             |     |
| 77.2                            | Proteção da base de dados                 | Demonstrar o bloqueio de comando de manipulação de dados em consulta gerada e a recusa de credencial com privilégio de escrita                         |                             |     |
| 77.3                            | Cruzamento federado                       | Cruzar dados de duas fontes distintas sem persistência intermediária dos dados consultados                                                             |                             |     |
| 77.4                            | Auditoria de consultas                    | Exibir o registro auditável da consulta realizada, com usuário, fonte, consulta executada e custo apurado                                              |                             |     |

## 7.5. Plataforma de Segurança e Governança da Informação

| Requisitos da Prova de Conceito |                                               |                                                                            | Conformidade de Atendimento |     |
|---------------------------------|-----------------------------------------------|----------------------------------------------------------------------------|-----------------------------|-----|
| Nº                              | Tipo                                          | Requisito                                                                  | Sim                         | Não |
| 78                              | Análise de Postura de Segurança da Informação | O Sistema de Análise de Postura de Segurança da Informação, deve permitir: |                             |     |

|    |                                               |                                                                                       |  |  |
|----|-----------------------------------------------|---------------------------------------------------------------------------------------|--|--|
|    |                                               |                                                                                       |  |  |
| 79 | Análise de Postura de Segurança da Informação | Avaliação de conformidade com Programa de Privacidade e Segurança a Informação (PPSI) |  |  |
| 80 | Análise de Postura de Segurança da Informação | Avaliação de conformidade com CIS Controls (v8).                                      |  |  |
| 81 | Análise de Postura de Segurança da Informação | Avaliação de conformidade com MITRE ATT&CK.                                           |  |  |
| 82 | Análise de Postura de Segurança da Informação | Avaliação de conformidade com ISO 27001.                                              |  |  |
| 83 | Análise de Postura de Segurança da Informação | Correlação entre frameworks CIS Controls e MITRE ATT&CK.                              |  |  |
| 84 | Análise de Postura de Segurança da Informação | Análise e gestão de riscos de segurança.                                              |  |  |
| 85 | Análise de Postura de Segurança da Informação | Planejamento faseado para implementação de controles.                                 |  |  |
| 86 | Análise de Postura de Segurança da Informação | Acompanhamento de evolução de postura de segurança.                                   |  |  |
| 87 | Análise de Postura de Segurança da Informação | Geração de relatórios e recomendações baseadas em inteligência de ameaças.            |  |  |



Documento assinado eletronicamente por **Ramon Leonn Victor Medeiros, Assessor(a)**, em 08/10/2026, às 15:28, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site [https://sei.iti.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://sei.iti.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0818009** e o código CRC **D06DE0F1**.