PREFEITURA RIO | iplanrio

TERMO DE REFERÊNCIA

REGISTRO DE PREÇO PARA CONTRATAÇÃO DE SOLUÇÃO DE OBSERVABILIDADE E GESTÃO DE PERFORMANCE DE APLICAÇÃO COMPREENDENDO SUBSCRIÇÃO DE SOFTWARE DE SERVIÇOS E SERVIÇOS ESPECIALIZADOS.

SETEMBRO/2025

Rua Beatriz Larragoiti Lucas, s/n - Cidade Nova, Rio de Janeiro - RJ, 20211-175

PARTE I - DAS ESPECIFICAÇÕES TÉCNICAS

1. DO OBJETO

1.1. Registro de Preços para contratação de solução de observabilidade e gestão de performance de aplicações, compreendendo subscrição de software e serviços especializados por 24 (vinte e quatro) meses, conforme descrito, caracterizado e especificado neste Termo de Referência.

1.2. Os serviços serão realizados por demandas, por meio de documento contratual, sem garantia de consumo mínimo e/ou máximo.

1.3. O objeto descrito neste Termo de Referência é caracterizado como comum, sendo cabível a utilização da modalidade de licitação denominada Pregão, tendo em vista que foi objetivamente definido neste documento por meio de especificações usuais do mercado.

1.4. Trata-se de objeto disponível em mercado próprio, fornecido habitualmente, independentemente da demanda da Administração, de forma padronizada, sem a exigência de atendimento de qualquer especificidade ou variantes de adequação.

2. DA JUSTIFICATIVA DA NECESSIDADE DA CONTRATAÇÃO

A presente contratação tem por finalidade prover uma solução de observabilidade de aplicações, com serviços especializados de apoio técnico, voltada ao monitoramento contínuo, análise de desempenho, detecção de anomalias e melhoria da experiência do usuário em sistemas críticos da Prefeitura do Rio de Janeiro, sob gestão da IPLANRIO.

A motivação para essa contratação está fundamentada em três pilares principais:

1. Alinhamento com a missão institucional da IPLANRIO e os objetivos estratégicos da Prefeitura

   A IPLANRIO, como empresa pública de tecnologia da Prefeitura do Rio de Janeiro, tem por missão fornecer soluções digitais inovadoras que promovam a eficiência da gestão pública e a aproximação entre os cidadãos e os serviços municipais. Esse compromisso implica não apenas a digitalização de processos, mas também a garantia da qualidade, disponibilidade e desempenho das aplicações ofertadas à população.

   Diante da crescente demanda por serviços públicos digitais mais ágeis, responsivos e confiáveis, torna-se essencial contar com mecanismos capazes de:
   - Detectar proativamente falhas ou degradações na performance de sistemas críticos;
   - Garantir níveis adequados de experiência do usuário, especialmente em cenários de alta carga ou infraestrutura adversa;
   - Apoiar a tomada de decisões com base em dados concretos sobre o comportamento das aplicações, suas transações e usuários.

   Para isso, propõe-se o monitoramento e análise contínua dos sistemas e aplicações consideradas críticas, conforme especificado no ANEXO II, cujas funcionalidades sustentam serviços essenciais à população e aos processos internos da administração municipal.

2. Disponibilidade de soluções maduras no mercado

   O mercado nacional e internacional dispõe hoje de um conjunto robusto de plataformas especializadas em observabilidade de aplicações, que integram de forma nativa recursos de monitoramento de desempenho, rastreamento distribuído, análise de logs, detecção de anomalias com inteligência artificial, e visualização de métricas técnicas e funcionais.

   Essas soluções possibilitam:

- O mapeamento completo das jornadas dos usuários, incluindo ações, chamadas de API, interações com banco de dados, tempos de resposta e fluxos entre microserviços;
- A captura e correlação de eventos em tempo real, facilitando a identificação da causa raiz de incidentes;
- A geração de relatórios, painéis e alertas inteligentes, otimizando a comunicação entre áreas técnicas e de negócio.

Além disso, a adoção do modelo SaaS em nuvem pública elimina a necessidade de aquisição de infraestrutura própria, evita o risco de obsolescência tecnológica e reduz o esforço interno com atualização, sustentação e suporte da solução.

3. Processos e pessoas para garantiria de eficácia e eficiência

A contratação não se limita ao licenciamento da ferramenta de observabilidade. Para que a solução tenha efetividade real na prevenção e resolução de problemas, é indispensável a composição com serviços especializados, tais como:

- Configuração e parametrização da ferramenta conforme os sistemas monitorados;
- Criação de dashboards, indicadores e alertas aderentes à realidade da IPLANRIO;
- Apoio contínuo à análise de eventos e recomendação de ações corretivas ou evolutivas;
- Transferência de conhecimento e capacitação técnica das equipes internas.

Sem esses serviços, a ferramenta operaria como um repositório passivo de dados, incapaz de gerar o valor esperado em termos de redução do tempo médio de resolução de falhas (MTTR), melhoria contínua da performance das aplicações e aumento da confiabilidade percebida pelos usuários.

Portanto, a contratação de uma solução de observabilidade como serviço, com ferramenta em nuvem e serviços especializados, é uma medida necessária, tempestiva e coerente com a missão institucional da IPLANRIO. Ela permitirá aprimorar a qualidade dos serviços digitais prestados à população, ampliar a capacidade analítica da organização com menor esforço e baixa complexidade operacional, e consolidar uma abordagem preventiva e responsiva à operação de sistemas críticos da Prefeitura do Rio de Janeiro.

3. DA DESCRIÇÃO DA SOLUÇÃO A SER CONTRATADA

3.1. A solução a ser contratada consiste na disponibilização de uma plataforma de observabilidade de aplicações e infraestrutura digital, acompanhada de um conjunto de serviços especializados de apoio técnico-operacional, com vistas à implantação, capacitação, operação assistida e análise contínua dos sistemas críticos sob responsabilidade da IPLANRIO. Essa solução deverá permitir o monitoramento abrangente, em tempo real, da saúde, desempenho, segurança e experiência de uso das aplicações, por meio de diferentes módulos complementares e integrados, que assegurem visibilidade ponta a ponta do ambiente digital.

3.1.1. Para os quantitativos da solução a serem contratadas, foram consideradas as métricas contidas no inventário detalhado no ANEXO II a memória de cálculo e aplicado as definições de unidades de referência para levantamento das quantidades a seguir:

ITEM	Descrição	Unidade de referência	Qtde.
3.2	**Licenciamento dos componentes principais**		
3.2.1	Módulo de análise de aplicações	Unidade 1	118 Hosts
3.2.2	Módulo de análise de usuários	Unidade 2	11,8 milhões
3.2.3	Módulo de análise de segurança	Unidade 3	118 Hosts
3.2.4	Módulo de análise de Log	Unidade 4	104 Tb
3.3	**Detalhamento dos serviços**		
3.3.1	Serviços de implantação inicial da solução	Unitário	01
3.3.2	Serviços de capacitação na solução	Turma	01
3.3.3	Serviços especializado de Operação Assistida e Análise Contínua, sob demanda, de 8 horas para cada 12 sistemas por 24 meses	HST	2,304 Horas

Tabela 1 – Solução a ser contratada – Ver Anexo II memória de cálculo

3.2. A contratação compreenderá os seguintes componentes principais:

3.2.1. **Módulo de Análise de Aplicações**, voltado à observação profunda de fluxos transacionais, tempos de resposta, gargalos e falhas em todas as camadas das aplicações;
3.2.2. **Módulo de Análise de Usuários**, para mapeamento das jornadas individuais e identificação de padrões de comportamento, engajamento e frustração;
3.2.3. **Módulo de Análise de Segurança**, com foco na detecção de vulnerabilidades, comportamentos anômalos e riscos associados à superfície de ataque das aplicações monitoradas;
3.2.4. **Módulo de Análise de Log**, capaz de consolidar, estruturar e correlacionar dados de log provenientes de diferentes fontes, promovendo maior capacidade de auditoria e detecção de falhas;

3.3. Além dos recursos tecnológicos mencionados, a solução deverá incluir:

3.3.1. **Serviços de Implantação,** abrangendo a configuração inicial, parametrizações, integração com os sistemas-alvo e validação da aderência funcional;
3.3.2. **Serviços de Capacitação**, com foco na formação das equipes da IPLANRIO para uso pleno e autônomo da solução;
3.3.3. **Serviços de Operação Assistida e Análise Contínua**, por meio de uma equipe especializada, apoiará o uso cotidiano da plataforma, incluindo ajustes e análise de eventos, voltados à produção de diagnósticos periódicos, relatórios analíticos e recomendações de melhoria baseadas nos dados coletados pela solução.

3.4. Esta composição integrada de módulos e serviços visa assegurar não apenas a implantação técnica da ferramenta, mas também sua adoção eficaz como disciplina de trabalho estruturada, capaz de ampliar a visibilidade operacional da IPLANRIO, reduzir riscos de indisponibilidade, e aprimorar continuamente a qualidade dos serviços digitais ofertados pela Prefeitura do Rio de Janeiro

3.5. Para cada item descrito na tabela (item 3.1.1), deverá ser considerado a unidade de referência definida, para manter a conformidade com os princípios estabelecidos, propõe-se que as métricas de licenciamento sejam expressas nas seguintes unidades técnicas, passíveis de mensuração direta e vinculadas às capacidades entregues:

Unidade 1 – Uma unidade 1 deverá ter a capacidade de monitorar até 1 host ou 16,0 GB de memória ou 8 vCPU, na modalidade full-stack. Para a modalidade de monitoramento apenas de infraestrutura, uma unidade 1 deverá ter a capacidade de monitorar um host independente de memória ou CPU.

Unidade 2 – Uma unidade 2 deve ter a capacidade de monitorar até 1.000.000 (um milhão) de visitas de usuários por ano, totalizando 2.000.000 (dois milhões) durante a vigência do contrato (24 meses), com coleta de dados relativos à jornada, comportamento, performance percebida e experiência do usuário final.

Unidade 3 – Uma unidade 3 deverá ter a capacidade de monitorar até 1 host ou 16,0 GB de memória ou 8 vCPU, na modalidade full-stack. Para a modalidade de monitoramento apenas de infraestrutura, uma unidade 3 deverá ter a capacidade de monitorar um host independente de memória ou CPU, com foco adicional em identificação de vulnerabilidades, análise de risco e correlação com eventos de segurança.

Unidade 4 – Uma unidade 4 deve ter a capacidade de ingestão e analisar até 1 (um) Terabytes de logs por ano, totalizando 2 (dois) Terabytes durante a vigência do contrato (24 meses), oriundos de diferentes fontes (aplicações, servidores, gateways, APIs etc.), com suporte à correlação de eventos e geração de alertas

Unitário – Conjunto único e indivisível de atividades executadas para implantação e configuração da solução executadas uma única vez ao início do contrato, incluindo configuração da instância SaaS, parametrizações, integrações com sistemas-alvo, testes e validações técnicas de funcionamento. Corresponde a uma execução integral e única ao início da vigência contratual.

Turma – Turma de no máximo 10 (dez) integrantes da CONTRATANTE a serem capacitadas no uso da solução oferecida segundo programa oficial de treinamento previsto pelo fabricante da solução, com foco em formação operacional no uso da solução contratada, com conteúdos teóricos e práticos. A carga horária e o cronograma deverão ser definidos em conjunto com a CONTRATANTE.

HST – Horas de serviços técnicos a serem executadas sob demanda, para execução de atividades técnicas especializadas relacionadas à análise contínua de dados coletados pela solução, com vistas à produção de

diagnósticos, identificação de anomalias, elaboração de relatórios analíticos e recomendações de melhoria. A quantidade de HST será estimada de acordo com a complexidade e volume das análises demandadas.

3.6. O grupo técnico responsável por este Termo de Referência, a partir de avaliação do mercado e as práticas de comercialização associado ao seguimento que provê soluções da mesma natureza que este certame, estabelece a definição de métricas de licenciamento da solução de Observabilidade para os seguintes princípios orientadores:

3.6.1. Assegurar a ampla participação dos principais fabricantes e fornecedores de mercado, mediante adoção de critérios compatíveis com os modelos de licenciamento amplamente praticados por soluções consolidadas no segmento de Application Performance Monitoring (APM) e Observabilidade

3.6.2. Garantir aderência aos modelos de subscrição, evitando o uso de métricas proprietárias ou de difícil equivalência entre diferentes produtos, o que poderia comprometer a comparabilidade técnica e a competitividade do processo de contratação;

3.6.3. Prever a flexibilidade na alocação e uso dos recursos licenciados, de modo a absorver variações sazonais ou oscilações de demanda ao longo do período contratual, sem prejudicar a previsibilidade orçamentária nem comprometer a continuidade dos serviços monitorados;

3.6.4. Adotar métricas técnicas objetivas, auditáveis e amplamente reconhecidas no mercado, de forma que a aferição do consumo e do atendimento contratual possa ser realizada com base em relatórios nativos da própria solução ou por meio de dashboards automatizados e disponíveis para fiscalização técnica.

3.7. Detalhamento da solução a ser contratada, conforme tabela I (item 3.1.1)

3.7.1 **Módulo de análise de aplicações (Item 3.2.1)**

3.7.1.1 O monitoramento de aplicação é focado na performance e integridade dos aplicativos, identificando gargalos, falhas, e lentidões que afetam a experiência do usuário. Esse módulo oferece visibilidade profunda no comportamento das aplicações em produção, analisando tempos de resposta, transações, e dependências entre componentes, como APIs e bancos de dados.

3.7.1.2 Funcionalidades básicas:

- Análise de tempo de resposta das transações;

- Rastreamento de erros e exceções de código;
- Identificação de gargalos de desempenho em componentes individuais (banco de dados, API);
- Visualização de fluxos de transações complexas entre múltiplos serviços.

3.7.1.3 Requisitos técnicos:

- O módulo/solução deve permitir ser implantada na modalidade SaaS, a CONTRATADA deverá disponibilizar os recursos de computação em provedor que possua ao menos as certificações: ABNT NBR ISO/IEC 27001:2013;ISO/IEC 27017:2015; e ISO/IEC 27018:2019, com validade vigente durante a execução do contrato, referentes à infraestrutura hospedada em datacenter no Brasil;
- Ser oferecida com interface de operação e administração, exclusivamente WEB, com compatibilidade com os seguintes navegadores: Microsoft Edge, Mozilla Firefox ou Google Chrome;
- O módulo deve permitir a visualização de erros de processo e exceções de negócios em cada etapa;
- O módulo deverá possibilitar a criação e desenvolvimento de novos aplicativos customizados na plataforma, para atender casos de uso específicos, aproveitando os dados de observabilidade;
- O módulo deverá possuir documentação do fabricante para auxílio do desenvolvimento dos novos aplicativos;
- Através de um agente unificado instalado em cada servidor, deverá descobrir automaticamente todas as tecnologias, processos, serviços e aplicações, e suas respectivas dependências e relacionamentos de forma dinâmica e contínua, não necessitando configuração prévia e parametrização manual;
- O módulo deve monitorar as aplicações dinamicamente, utilizando tecnologia de bytecode instrumentation, de forma automática e sem a necessidade de intervenção manual nos arquivos de configuração e arquivos fontes das aplicações, incluindo arquivos JS;
- Deve haver criptografia nativa do módulo para a comunicação ponto a ponto entre todos os componentes/módulos do módulo;
- A interface de administração e operação do módulo deve ser 100% WEB (sem demandar instalação de clientes em estações);
- Monitorar automaticamente aplicações baseadas em arquitetura de micro serviços, como [nome do módulo de containers e administradores de containers se houver], não necessitando configuração prévia de arquivo de configuração e definição de regras, devendo monitorar os processos que estão ocorrendo em cada host;

- Realizar injeção automática do agente em contêineres (glibc ou musl-libc) em CONTAINERD (https://containerd.io/);
- Deverá ser possível de forma automática monitorar clusteres em Kubernetes/Openshift, sem alteração de código e parametrização prévia de scripts de configuração para que a monitoração ocorra;
- Deverá de forma automatizada injetar/configurar agentes nos containers Docker, containerd e CRIO, sem a necessidade de qualquer atividade de configuração de script do coletor, alteração da imagem, bastando apenas a instalação do agente no servidor onde os containers são excetuados;
- Permitir o monitoramento dos componentes do cluster [nome da Tecnologia do container] para orquestração de contêineres, sendo possível obter métricas sobre os servidores, processos de gerenciamento, utilização de recursos computacionais (CPU, memória, rede e armazenamento);
- Realizar o auto-discovery do cluster, garantindo a continuidade e escalabilidade automática, para que mesmo em caso de mudanças ou adições de novos elementos na arquitetura, a monitoração ocorra;
- O módulo deverá fornecer Dashboards pré-construídos e oferecer um editor que permita a criação e customização de dashboards, painéis personalizados permitindo a inclusão de imagens, labels, e permitindo também a configuração da navegação em fluxo, Drill Downs customizados entre dashboards e entidades;
- Os dashboards deverão permitir a extração de dados da integridade operacional, desempenho do aplicativo, infraestrutura e dados relevantes de negócios;
- O módulo deverá prover suporte a autenticação em OpenLDAP, Microsoft Active Directory e SAML;
- Prover mecanismos de atualização de versão e/ou distribuição do produto durante toda a vigência do Contrato. O processo de atualização deve ocorrer de forma nativa e totalmente automático sem a necessidade de qualquer configuração manual, de apoio de ferramentas terceiras e de scripts automatizados;
- O módulo deverá possuir ferramenta para automação de tarefas a partir de condições especificadas para execução de fluxos de trabalho criados;
- O módulo deverá possibilitar a criação e configuração da automação a partir de uma interface gráfica amigável com drag-and-drop;
- Deverá possibilitar a execução de tarefas a partir de gatilhos ou cronogramas para execuções de ações que integrem com outros sistemas;

- Deve possuir templates prontos para enviar notificações ou criar tickets;
- Permitir a trilha de auditoria de cada tarefa executada;
- O módulo deve permitir o envio de requisições HTTP a APIs públicas na internet ou para APIs privadas dentro da infraestrutura do cliente;
- No caso de APIS privadas O módulo deve permitir o envio de requisições sem a necessidade de abrir as APIs privadas para a Internet;
- O módulo deve oferecer suporte à configuração como código por meio de um provedor Terraform ou similar;
- O módulo deve oferecer um mecanismo nativo de configuração como código;
- Indicar e sugerir a instalação dos agentes em novos servidores que ainda não estão com monitoração instalada, nos casos em que alguma tecnologia, processo, serviço ou aplicação se comunicar com o novo servidor a partir de um servidor com monitoração ativa;
- O módulo deve oferecer endpoints de API para gestão de configuração da própria plataforma;
- O módulo poderá contar com comunicação externa do próprio fabricante desde que a comunicação seja totalmente segura e criptografada;
- Fornecer o nível de disponibilidade do servidor, bem como eventos, problemas e erros ocorridos;
- Apresentar visibilidade fim-a-fim, investigando os diversos estágios das aplicações sem a necessidade de instalação de agentes adicionais que não componham O módulo ofertada;
- Para servidores físicos e virtuais, apresentar automaticamente, no mínimo, as seguintes métricas de performance e disponibilidade: CPU, memória, disco, rede;
- Permitir a integração com sistemas de virtualização VMware. Com esta integração, o Módulo deverá realizar a performance digital e apresentar ao menos as seguintes métricas: número de servidores criados por dia, número de servidores baixados por dia, número de Vmotion por dia;
- Permitir a integração nativa com ambiente de virtualização VMWare e monitorar, no mínimo, as seguintes métricas: número de cluster, número de servidores físicos e virtuais, situação dos servidores físicos e virtuais (exemplo: ativo, suspenso);
- Realizar a verificação automática de performance e disponibilidade da comunicação dos processos, coletando e exibindo, no mínimo, as informações de tráfego de entrada e saída, disponibilidade, taxa de transmissão e retransmissão, erros e perdas de pacotes, falhas tcp e round trip time;

- Indicar, para as tecnologias descobertas, no mínimo, as informações de uso de CPU, consumo de memória, taxa de transmissão e disponibilidade ao longo do tempo;
- Descobrir automaticamente e dinamicamente a topologia da aplicação alvo, contendo a comunicação entre seus componentes e apresentando um mapa completo da aplicação e suas dependências;
- A descoberta deverá ser realizada de forma automática e constante, atualizando dinamicamente sem a necessidade de qualquer configuração manual, e de apoio de ferramentas terceiras e de scripts automatizados;
- A descoberta automática deverá suportar, no mínimo, os seguintes elementos: HTTP/HTTPS, Web Services, banco de dados, serviços de mensageria, Hosts da VMware, máquina física ou virtual, chamada a serviço externo de terceiros ou servidor remoto;
- A nuvem pública será responsável pelo provimento da infraestrutura de TI necessária para o funcionamento do módulo, como servidores (hosts), armazenamento de dados, programas de software básico (ex: sistema operacional, banco de dados, servidor de aplicação/web, etc) e pela sua gestão/manutenção (ex: atualização de versão, aplicação de correções de segurança, backup de dados, etc);
- O módulo deverá indicar a quantidade de componentes de tecnologia descobertos por categoria (exemplo: hosts, processos, serviços, aplicações) indicando, inclusive, quantidade de componentes afetados por um problema em tempo real;
- Para os componentes de tecnologia descobertos, deverá ser monitorado o volume de chamadas/requisições, tempo de resposta e taxa de falhas;
- A monitoração das aplicações deverá ser iniciada de forma automática, junto com a inicialização do respectivo servidor de aplicação;
- Acompanhar a performance do ambiente, verificando a utilização de CPU por processo. Para cada processo instrumentado, deverá ser possível identificar o código-fonte, no nível de métodos dos processos que mais consomem CPU;
- Permitir a verificação do consumo de CPU dos processos instrumentados e efeito do Garbage Collector, tais como número de execuções e percentual de suspensão do thread;
- O módulo deverá identificar todas as classes e métodos com maior consumo do tempo de execução visando a otimização do código;

- O módulo deverá, para cada serviço, indicar as aplicações que consomem o serviço específico, bem como os bancos de dados acessados e os respectivos comandos SQL executados pelo serviço analisado;
- O módulo deverá automaticamente e dinamicamente identificar os serviços. E apontar as requisições mais lentas, que estão consumindo mais recursos e possuem taxa de falha mais alta;
- Realizar a verificação da performance e disponibilidade dos principais serviços de terceiros acessados na Internet;
- O módulo deverá, para cada serviço, indicar, de forma gráfica, fluxo das requisições que chamam e que são chamadas pelo serviço em análise;
- Plataforma AIOps (Artificial Intelligence for IT Operations) que permita gerenciar ambiente de modo proativo, identificando rapidamente indisponibilidades, com detalhamento que facilite inclusive as tomadas de decisões não só relacionadas à manutenção corretiva, mas até para melhorias nos serviços;
- O módulo deve determinar de forma automática (aprender automaticamente) e sem configuração prévia os limites e baselines (dados de referência) de métricas-chave, inclusive de negócio, de funcionamento normal das aplicações para geração de alertas de anomalias (desvios de comportamento com algoritmos que permitam detecção de anomalias) e identificar de forma automática possíveis impactos levando em consideração a topologia da aplicação. Por exemplo: uma transação no front-end está lenta porque o serviço de banco está com a taxa de falha elevada;
- O módulo deve ser capaz de analisar e apresentar os relacionamentos existentes entre os componentes, não somente de forma vertical, mas horizontal e baseado em topologia, de forma a apontar a causa raiz dos problemas;
- Deverá identificar os problemas que estão ocorrendo no ambiente, analisando automaticamente os incidentes e relacionamentos entre todos os componentes, de forma a apontar os problemas agrupados, separando causa e efeito, de forma automática com uso de inteligência artificial, em tempo real e mantendo o histórico dos problemas ocorridos;
- O módulo deve identificar, de forma automática e com uso de inteligência artificial, a causa raiz dos problemas nas aplicações monitoradas, de forma contextualizada, em tempo real e classificando a natureza, apontando o número de aplicações, usuários, chamadas, serviços, SLOs impactados e componentes de infraestrutura afetados;

- O módulo deverá fornecer mecanismos para acompanhar os indicadores de uma aplicação a cada release, visando garantir que uma nova release tenha os seus SLOs e objetivos de capacidade atendidos. Deve permitir automatizar essa verificação, podendo inclusive ser integrada a um pipeline, para impedir o seu avanço em caso de violação desses indicadores;
- Deve permitir que os usuários possam comparar a validação de confiabilidade com objetivos de nível de serviço, de uma versão de release do passado ou de uma release progressiva.
- O módulo deve permitir fazer a predição e forecast para qualquer métrica presente na plataforma usando o seu motor de inteligência artificial;
- Deve ser possível gerar análises de predição sob demanda e inclusive gerar alertas baseados nos resultados dessa predição;
- O módulo deve prover observabilidade para desenvolvedores permitindo que os desenvolvedores possam fazer o debug de aplicações Java "ao vivo" em ambiente produtivo sem impactar a aplicação e sem qualquer impacto aos usuários das aplicações. O Debug deve permitir a visualização da execução linha a linha assim como as propriedades da linha de código;
- O debug "ao vivo" não deve enviar qualquer parte do código fonte da aplicação para os servidores do módulo, evitando assim qualquer vazamento de informações sigilosas;
- Compatibilidade com o ambiente atual do IPLAN RIO para o monitoramento de performance de aplicações, serviços, infraestrutura e experiência digital dos usuários;
- O debug "ao vivo" deve permitir que dados sensíveis (CPF, Número de cartão de crédito, etc…) sejam imediatamente mascarados permitindo o debug pelos desenvolvedores sem a exposição de quaisquer dados que comprometam a privacidade dos usuários da aplicação;
- Deduplicação - quando múltiplos eventos repetitivos são recebidos para o mesmo incidente de um mesmo elemento de infraestrutura, devendo registrar o evento apenas uma vez;
- Correlação automática baseada em topologia - suprimir os eventos gerados a partir de elementos relacionados entre si, onde um destes elementos é o causador do incidente, sem necessidade prévia de criação de regras;
- Deverá executar ações resultantes da deflagração de um alerta, suportando, no mínimo: envio de e-mail, integração com Jira ou Webhook;

- O módulo deve suportar a coleta de dados de forma simples e sem a necessidade de escrever scripts para as seguintes tecnologias: WMI, SNMP, JMX, Prometheus e SQL;
- O módulo deve suportar a coleta de dados através de criações de scripts em Python;
- Disponibilizar informações a respeito de problemas que afetam uma aplicação, permitindo o detalhamento do problema;
- Deverá monitorar aplicações heterogêneas, hospedadas em ambiente próprio de Datacenter do IPLAN RIO.
- Para os problemas identificados no ambiente monitorado, O módulo deverá apontar o número de serviços, aplicações e componentes de infraestrutura afetados pelo problema. Além disso, deverá indicar o número de usuários reais Das aplicações que foram afetados;
- Para os problemas identificados de forma automática e inteligente, identificar além do impacto do problema, também a sua causa raiz;
- Disponibilizar na página do problema mecanismo de gravação do comportamento e evolução do problema demonstrando visualmente todos os componentes de tecnologia afetados durante a vigência do problema, bem como os relacionamentos entre eles. O módulo deverá indicar os tempos e momentos em que ocorrem os eventos, bem como os serviços impactos ao longo do tempo;
- Apresentar o nível de disponibilidade do servidor, bem como eventos, problemas e erros ocorridos.
- Disponibilizar visão fim-a-fim das transações, investigando os diversos estágios das aplicações sem a necessidade de instalação de agentes adicionais que não componham o módulo ofertada;
- Descobrir automaticamente transações de negócio (ações resultantes da interação com usuários ou sistemas) tanto no FrontEnd quanto Backend;
- Detectar transações de negócio de forma automática, iniciadas, no mínimo, com base nos seguintes protocolos/tecnologias: HTTP/HTTPS e web services;
- Permitir monitorar as execuções das requisições de backend, contendo minimamente as seguintes métricas: quantidade de execuções da transação, tempos de resposta e volume de erros, com drilldown detalhado do código executado (classes e métodos) nas transações executadas nos servidores de aplicação;
- Classificar e quantificar a execução das requisições de acordo com seu tempo de resposta e eventuais erros, de forma a possibilitar ao usuário/analista a identificação de desvio de comportamento na linha do tempo (exemplo: Tempo de Resposta, Taxa de Falha e Throughput);

- Disponibilizar informações a respeito de eventos ocorridos na aplicação, como restart ou deploy, permitindo o correlacionamento de problemas com um possível problema de deploy;
- Deverá monitorar soluções compostas por aplicações construídas com diversidade de plataformas tecnológicas, versões e distribuições providas por fornecedores de marcas variadas, tanto de hardware quanto de software;
- Identificar requisições com baixa performance, lentas, sem intervenção manual;
- Identificar queries SQL com baixa performance ou lentas, sem intervenção manual;
- Identificar sistemas de backend ou serviços externos lentos ou indisponíveis, sem intervenção manual;
- Apresentar detalhamento de tempos de execução em nível de classe, método e comandos SQL, por meio do baseline dinâmico;
- Realizar a verificação da performance das chamadas à banco de dados feita pelas aplicações, não necessitando realizar a instalação de agentes no servidor de banco de dados;
- Exibir, para as conexões com o banco de dados, a taxa de falhas, tempo de resposta médio e quantidade de requisições por período de tempo;
- Exibir a listagem das consultas mais lentas aos bancos de dados;
- O módulo deve monitorar as instruções SQL e apresentar a quantidade de execuções, taxa de falhas e o tempo médio de resposta para as transações com erro ou problemas de performance;
- Para as consultas a banco de dados, disponibilizar gráfico da distribuição dos tempos de resposta pela quantidade de ocorrências, permitindo assim que seja possível identificar os tempos de resposta que mais ocorrem durante a análise;
- Para os comandos de banco de dados, indicar os comandos mais executados (exemplo: alteração, consulta), indicando a quantidade na unidade de tempo e o tempo médio de resposta, bem como detalhando os comandos;
- Deverá permitir flexibilidade no licenciamento dos agentes independente de tecnologia e/ou linguagem das aplicações, possibilitando a reutilização de uma licença em diferentes tecnologias e/ou aplicações, respeitado o limite contratado;
- A partir de um comando de banco de dados, permitir rastrear a aplicação e serviços que o executou, seja em Java ou .NET;

- Possuir mecanismos de visualização de dados históricos sem a necessidade de leitura de arquivos externos à solução;
- O processamento de dados para consolidação da base, assim como para geração de relatórios e consultas, não deverá ocorrer nos servidores monitorados e sim na plataforma de gerenciamento específico da CONTRATADA;
- Possuir controle de acesso, permitindo criar e modificar grupos de perfis de acesso;
- Permitir ao administrador do módulo habilitar ou desabilitar a verificação da performance do ambiente monitorado;
- Permitir o monitoramento de quantidade de chamadas e tempo de resposta de API REST providas pelas aplicações;
- O módulo deverá possuir mecanismo de particionamento de informações, permitindo a visualização separada da topologia e conjunto de entidades monitoradas ou dados dimensionais (como logs e métricas) em um ambiente. Deve ser possível realizar filtros por grupos específicos de monitoramento e visualização separada dos problemas de cada grupo, assim como controle de acesso às informações;
- Apresentar visão gráfica (mapas ou representação gráfica equivalente) do ambiente ou aplicação monitorada, contendo no mínimo:
  - Visão gráfica pré-definida para as principais métricas e análises disponibilizadas pelo módulo. Deverá permitir a criação e customização de painéis, gráficos ou mapas com a inclusão ou retiradas de informações disponibilizadas pelo módulo;
  - Visão gráfica da análise da performance da aplicação identificando os serviços e infraestrutura utilizada pela aplicação, bem como informações a respeito dos acessos de origem das transações, como navegador e visão geográfica dos acessos;
- Não serão aceitas soluções que demandem uso de espelhamento/mirror/span de dados de rede;
- Visão gráfica apresentando as informações da aplicação em períodos históricos e permitindo filtros na escala e período de tempo (por exemplo: tempo real, ontem, últimos 7 dias, últimos 15 dias e últimos 30 dias);
- Visão gráfica apresentando o volume de execuções e tempos médio de resposta entre todos os componentes da aplicação de acordo com a escala e período de tempo selecionado;

- O módulo deverá permitir configurar e monitorar objetivos de nível de serviços (SLOs) utilizando indicadores de diferentes dimensões da aplicação, como serviços, experiência de usuário e taxa de falhas;
- O módulo deverá permitir a realização de análise de negócio, com a capacidade de conectar informações de desempenho da aplicação alvo e a experiência do usuário à métricas de negócio;
- O módulo deve possibilitar a monitoração de indicadores de desempenho (KPI) de negócio, detectando anomalias nas transações e permitindo análise para fundamentar melhores decisões;
- O módulo deverá permitir a criação de relatórios analíticos derivados de métricas da experiência de usuário e transações com o objetivo de obter insights de negócio;
- O módulo deve permitir análise avançada de condições de negócio, permitindo acompanhar eventos relevantes para o negócio diretamente na plataforma. A coleta de eventos de negócio deve ser possível das seguintes formas: diretamente no agente que monitora as aplicações, através da monitoração da experiência do usuário, envio de eventos através de API dedicada, a partir dos logs ingeridos pelas plataformas;
- O módulo deve permitir reportar KPIs de processos de negócios, incluindo fluxos concluídos (conversões), tempo médio de conclusão de fluxos, exceções de negócios e KPI de negócios específicos;
- O módulo deve permitir, para os eventos de negócio já armazenados na plataforma a criação, visualização e análise de fluxos de processos de negócio do início ao fim;
- O módulo deve permitir a detecção e exploração de fluxos de processos de negócio incompletos ou interrompidos para determinar a causa, como um erro de TI, uma exceção de negócios ou tempo de trânsito anormal entre etapas.

3.7.2 **Módulo de análise de usuários (Item 3.2.2)**

3.7.2.1 Esse módulo fornece visibilidade sobre a interação dos usuários finais com as aplicações e sistemas. Ele captura dados sobre os acessos, incluindo geolocalização, dispositivos usados, tempos de carregamento, e padrões de navegação, permitindo a avaliação da experiência do usuário (UX) em tempo real.

3.7.2.2 Funcionalidades básicas:

- Rastreamento de atividades de usuários (clickstreams).

- Análise de experiência de usuário real (Real User Monitoring - RUM).
- Identificação de problemas de acesso e tempos de resposta.
- Monitoramento de perfis de uso por dispositivo, localização e navegador.

3.7.2.3 Requisitos técnicos:

- Deverá permitir o acompanhamento da experiência do usuário final no acesso às aplicações corporativas hospedadas no ambiente do DataCenter;
- O módulo deve ser capaz de monitorar a experiência de usuários finais da aplicação, através de um código JavaScript injetado no front-end da aplicação de maneira automática e sem esforço de configuração via interface, ou alteração de arquivo ou alteração de código da aplicação (ou arquivos de configuração, mesmo que arquivos JS), a ser executado no ambiente/navegador do usuário final. Não será permitido alterações nos servidores HTTP e inserções manuais de URLs;
- Deverá permitir a configuração de capturas de informações a partir de pelo menos Meta Tag, componentes CSS e JavaScript Variables, na página executada no navegador do usuário. O objetivo identificar o usuário logado ou enriquecer as transações de negócio. Não será permitido a alteração de código para captura de informações;
- O módulo deverá permitir a consulta (querys) de informações capturadas no monitoramento da experiência do usuário, podendo ser visualizadas em dashboards e utilizá-las como métricas de negócio;
-
    - A execução do código nos servidores de aplicação.
    - As consultas aos servidores de banco de dados. Deverá realizar a monitoração fim-a-fim das aplicações hospedadas no DataCenter, registrando e avaliando, no mínimo a requisição feita pelo usuário no navegador (click e carregamento de páginas ou ação do usuário na aplicação, gerando tráfego no servidor), para:
    - O retorno do resultado ao navegador do usuário.
    - Tempo de execução total da sessão/visita.
    - Tempo gasto em rede.
    - Tempo de servidor (execução transacional da aplicação).
    - Tempo de download do HTML e outros recursos da página.

  - Tempo de renderização do browser (DOM Build);
  - Tempo de pós-load;
  - Identificar webservices e chamadas a serviços externos das transações de uma aplicação.
- Disponibilizar informações a respeito das principais ações de usuário nas aplicações, indicando o total de ações executadas por período de tempo, exibindo informações a respeito do tempo de contribuição das ações, considerando ao menos, tempo de rede e tempo de servidor;
- Para os erros de JavaScript identificados nas aplicações, apresentar ao menos as seguintes informações: sistema operacional utilizado, navegador, localidade e ação que gerou o erro. Para cada tipo de informação, O módulo deverá indicar a quantidade de erros ocorrida, por categoria.
- Verificar se uma transação ou requisição WEB (exemplo: HTTP ou HTTPS) foi atendida do ponto de vista do usuário final, identificando a satisfação do usuário segundo a métrica APDEX (www.apdex.org). Não será permitido a utilização de própria métrica para identificar a satisfação do usuário;
- Possuir forte integração com a análise de causa raiz, permitindo conectar imediatamente um problema na experiência do usuário com o componente da aplicação ou da infraestrutura, que está causando a degradação (exemplo: comando SQL, chamada WebServices .Net);
- Realizar a verificação da performance das ações dos usuários exibindo, no mínimo, na linha do tempo, a quantidade de ações, a duração das ações e situação das ações (exemplo: sucesso, erro);
- Monitorar a experiência do usuário em página web, virtual pages, iFrames e chamadas AJAX;
- Para cada ação de usuário nas aplicações, apresentar ao menos as seguintes informações: falhas/sucesso, origem geográfica das ações, navegador de origem e duração média da ação, distribuição da quantidade de ações por duração e chamadas a serviços de terceiros por períodos históricos;
- Disponibilizar informações a respeito das principais ações de usuário nas aplicações, indicando o total de ações executadas por período, exibindo informações a respeito do tempo de contribuição das ações, considerando ao menos tempo de rede e tempo de servidor;
- Permitir a criação e definição customizada de localidade a partir de um range de endereços IP, permitindo assim que o administrador crie suas próprias regiões para melhor visualizar as informações de performance, volumetria e falhas por regiões;

- O módulo de experiência de usuário deve permitir a configuração de capturas de dados na página executada no navegador do usuário de forma anonimizada, com objetivo de reproduzir a sessão do usuário a partir da captura de eventos do navegador que permitam a visualização em formato de vídeo do ponto de vista do usuário a navegação realizada. Estas visualizações devem estar disponíveis para reprodução por, no mínimo, 30 dias após a sua realização;
- O módulo de reprodução de sessão do usuário deve vir com mascaramento de informações sensíveis do usuário por padrão e também permitir a configuração customizada deste mecanismo de privacidade de dados, permitindo, a nível de permissões de perfis de analistas, visualizar ou não as informações sensíveis;
- O módulo de observabilidade deverá prover funcionalidades para monitoramento sintético (synthetic monitoring), isto é, permitir agendamento de requisições periódicas a páginas web como se o acesso fosse realizado a partir de um navegador de internet (browser) a determinados endereços web (URL);
- O monitoramento sintético deverá conseguir simular uma transação (sequência de ações/passos) como fosse realizada por um usuário real utilizando um navegador de internet (browser). Nenhuma codificação deverá ser feita para provimento da funcionalidade;
- Deve ser possível utilizar um “recorder” para gravar todos os passos da navegação, integrados com os principais navegadores utilizados pelos usuários reais;
- O módulo deverá permitir que seja contemplado no script de gravação ações reais dos usuários, simulando, de fato, o acesso que o usuário faz ao acessar o serviço digital;
- A simulação do acesso ao serviço digital, conforme definição e script gravado, sendo executado a partir da Internet (fora das dependências do IPLAN RIO). Dessa forma, será uma visão mais real do usuário dos serviços digitais;
- A possibilidade de executar estas simulações a cada 5 (cinco) minutos (no mínimo) e de ao menos 3 (três) origens distintas;
- O módulo deverá coletar os dados de tempo de cada atividade simulada, exibindo estes dados ao longo do tempo;
- O módulo deverá permitir a realização de testes sintéticos para mensurar a disponibilidade da rede, utilizando testes ICMP, TCP e DNS;

3.7.3 **Módulo de análise de segurança (Item 3.2.3)**

3.7.3.1 O monitoramento de segurança oferece uma visão abrangente sobre a integridade e vulnerabilidades dos sistemas. Ele detecta atividades suspeitas, como tentativas de invasão, acessos não autorizados e comportamentos anômalos, além de rastrear a conformidade com políticas de segurança.

3.7.3.2 Funcionalidades básicas:

- Detecção de intrusões e análise de comportamento de usuários.
- Monitoramento de vulnerabilidades e ameaças em tempo real.
- Correlacionamento de eventos de segurança com outros eventos de sistema.
- Relatórios de conformidade e auditoria.

3.7.3.3 Requisitos técnicos:

- Permitir a detecção automática e em tempo real de vulnerabilidades nas aplicações sem a necessidade de configuração prévia de escaneamentos periódicos;
- O monitoramento de vulnerabilidades não deverá exigir agente adicional para coleta de dados, deverá utilizar o mesmo agente unificado solicitado nos requisitos funcionais para ambas as soluções;
- Descobrir automaticamente os problemas de segurança no ambiente e fornecer avaliações de risco automatizadas e contextualizadas;
- Identificar vulnerabilidades que precisam de investigação imediatamente;
- Usar Inteligência Artificial para gerar automaticamente uma pontuação de risco exclusiva para cada vulnerabilidade potencial reclassificando a nota com base na topologia em tempo real e na análise de vetores de transações;
- Permitir detectar, visualizar, analisar e monitorar vulnerabilidades de terceiros em ambientes de produção e não produção em tempo de execução para as tecnologias: Java, .NET, PHP, Node.js, Go e Kubernetes;

- Fornecer uma visão geral dos problemas de segurança atuais no ambiente monitorado;
- Exibir o número de problemas de segurança abertos atualmente no ambiente monitorado;
- Exibir o número máximo de problemas de segurança no ambiente monitorado que foram abertos no mês corrente, classificados por nível de risco;
- Listar todas as vulnerabilidades detectadas no ambiente monitorado;
- Pontuar as vulnerabilidades de acordo com o nível de riscos (Crítico, Alta, Médio, Baixo e Nenhum);
- Listar a situação de cada vulnerabilidade: Aberta, resolvida, aberta e silenciada pelo operador e resolvida e silenciada);
- O módulo deverá monitorar as vulnerabilidades de código aberto permitindo a detecção automática de ataques a partir do código vulnerável;
- A detecção deverá ocorrer para os ataques via SQL, JNDI e injeção de comando para à linguagem JAVA;
- A detecção deverá permitir a configuração do bloqueio e lista de permissão para os ataques;
- O módulo deverá mapear, para cada ataque: endereço de origem, processo vulnerável, vulnerabilidade de código que permitiu o ataque, detalhamento do ponto de entrada e o alvo;
- O módulo deverá correlacionar automaticamente os logs com os ataques ocorridos para facilitar a investigação;

3.7.4 **Módulo de análise de log (Item 3.2.4)**

3.7.4.1 Esse módulo coleta, armazena e analisa logs gerados por sistemas, aplicações e dispositivos. Ele facilita a correlação de eventos, fornecendo insights sobre o comportamento do sistema e ajudando a identificar falhas, ameaças de segurança e incidentes operacionais com base nos registros detalhados das atividades.

3.7.4.2 Funcionalidades básicas:

- Centralização e gerenciamento de logs de diferentes fontes.
- Análise de logs em tempo real para detecção de anomalias.

- Correlação de eventos para identificar causas raiz de incidentes.
- Geração de alertas automáticos com base em padrões predefinidos.

3.7.4.3 Requisitos técnicos:

- O módulo deve, para os dados de observabilidade e segurança, realizar o armazenamento de forma unificada, permitindo consultas aos dados e com gestão na interface da plataforma;
- O módulo deve possuir uma única interface que permita consultas de vários tipos de dados e múltiplas formas de visualização dos resultados;
- O módulo não deverá exigir reidratação de dados, independentemente do tempo;
- O módulo deve gerenciar eficientemente o armazenamento de dados sem a necessidade de configurações de armazenamento quente/frio;
- O módulo deve ter escalabilidade nativamente para acomodar o volume de dados crescente e a carga de trabalho;
- O módulo deve possuir a capacidade de realizar análises na leitura para dados históricos armazenados com até 10 anos de retenção;
- O módulo deve atender aos requisitos padrão de segurança e conformidade, incluindo criptografia de dados, controles de acesso e auditoria;
- O módulo deve ser capaz de analisar os logs das aplicações, serviços e infraestrutura permitindo criar regras de notificação baseado na ocorrência de palavras ou grupos de palavras existentes nos logs;
- O módulo deverá permitir explorar, consultar, combinar e processar todos os dados de logs armazenados na plataforma;
- O módulo deverá permitir realização de buscas textuais simples e avançadas utilizando linguagem própria do fabricante;
- O módulo deverá possuir funcionalidade de exclusão de dados (Hard Delete) em nível de registro, sem a possibilidade de recuperação, para cumprir com mais eficiência as solicitações de exclusão do usuário final, em linha com a lei de proteção de dados;
- O módulo deverá possibilitar a conversão de registros de log em eventos de negócio;
- O módulo deve permitir criar pipelines de dados possibilitando a criação de métricas, processamento de dados e extração de dados em eventos de negócio;

- O módulo deverá permitir configurar endpoints customizados para a ingestão de dados;
- O módulo deverá permitir criar rotas dinâmicas para os dados ingeridos com base em condições específicas;
- O módulo deverá permitir o isolamento lógico dos dados com o objetivo de controlar o acesso e o tempo de retenção. Essa separação lógica deve ser configurável e permitir que as regras sejam aplicadas no momento da ingestão dos dados para atender essa separação lógica;
- O módulo deverá permitir a ingestão de logs por meio do protocolo syslog;
- O módulo deverá contextualizar e enriquecer os dados de syslog automaticamente, com atributos específicos do servidor.

3.7.5 **Serviços de Implantação da solução (Item 3.3.1):**

3.7.5.1 Os Serviços de Implantação será constituído pelas seguintes atividades principais:

- Provisionamento e configuração da solução na infraestrutura do contratante;
- Integração com sistemas e aplicações existentes para monitoramento de desempenho e logs;
- Criação de dashboards personalizados para visualização em tempo real de métricas de desempenho e segurança, considerando no mínimo 05 dashboards por aplicação monitorada;
- Definição e ajuste de alertas automáticos para anomalias e eventos críticos;
- Desenvolvimento de algoritmos de detecção de problemas.

3.7.5.2 Essas atividades visam garantir a efetiva implementação e operação da ferramenta conforme os requisitos de monitoramento e governança estabelecidos.

3.7.6 **Serviços de Capacitação (Item 3.3.2)**

3.7.6.1 A capacitação da equipe técnica do IPLAN RIO voltada para o uso da ferramenta de OBSERVABILIDADE deverá ser realizada por meio de treinamentos teóricos e práticos, de forma presencial ou remota, conforme a necessidade do IPLAN RIO. A capacitação incluirá:

- Visão geral da solução: administração e operação da plataforma de OBSERVABILIDADE, incluindo todos os seus componentes;
- Treinamento prático: exercícios práticos com base em cenários reais de uso, com o objetivo de assegurar que a equipe técnica seja capaz de administrar a ferramenta, orientar o seu uso e realizar as interações necessárias com a equipe prestadora dos serviços de modo a atuar de maneira proativa na gestão das soluções digitais observadas;
- O programa de treinamento deverá ser apresentado juntamente com as propostas técnica e comercial, destacando conteúdo programático cobrindo todas as funcionalidades oferecidas e atendidas nos requisitos exigidos neste Termo de Referência, com carga horária mínima de 20 (vinte) horas para ministração do conteúdo previsto;
- A CONTRATADA será responsável por fornecer todo o material didático necessário, como manuais, tutoriais e vídeos, e deverá realizar a capacitação com avaliação dos participantes.

3.7.6.2 Quaisquer custos relacionados a deslocamento, hospedagem e alimentação dos instrutores ficam sob responsabilidade da empresa CONTRATADA e já devem estar incluídos no valor final do contrato.

3.7.7 **Serviços Especializados de Operação Assistida e Análise Contínua (Item 3.3.3):**

3.7.7.1 Os Serviços Especializados de Operação Assistida e de Análise Contínua em OBSERVABILIDADE englobam a realização de diagnósticos detalhados para identificar a causa raiz de problemas, análise forense para rastreamento de falhas, apoio técnico durante o uso cotidiano e geração de relatórios sobre o estado de saúde do sistema e desempenho. Incluem auditorias regulares de conformidade com políticas de segurança, análise estatística e preditiva para identificar tendências e propor medidas mitigatórias.

3.7.7.2 Outras atividades envolvem análise de padrões de comportamento, coleta de dados de múltiplas fontes, monitoramento contínuo de ameaças de segurança, previsão de tendências de uso, balanceamento de carga, testes de desempenho e a integração das ferramentas de OBSERVABILIDADE com soluções já existentes, garantindo interoperabilidade e adaptação contínua às mudanças do ambiente.

3.7.7.3 Os Serviços de Análise Contínua compreendem um conjunto significativo de atividades, cujo objetivo é gerar entregáveis que forneçam indicadores claros para a gestão dos serviços prestados pelo IPLAN RIO no âmbito da Prefeitura do Rio de Janeiro, especialmente aqueles que impactam diretamente os níveis de serviço e a continuidade dos negócios, descritos na tabela de catalogo de serviços:

Serviços de Operação Assistida e Análise Contínua	**Periodicidade**	**Produtos. Entregáveis**	**Expectativa de retorno**
Realização de diagnósticos detalhados para identificar a causa raiz de problemas.	Conforme necessário	Relatórios de diagnóstico detalhados, documentação das causas raízes dos problemas	2-4 horas por diagnóstico
Utilização de técnicas de análise forense para rastrear a origem de falhas e anomalias.	Conforme necessário	Relatórios de análise forense, documentação das falhas e anomalias encontradas	4-8 horas por análise
Geração de relatórios detalhados sobre o estado de saúde do sistema e desempenho.	Semanal	Relatórios de saúde do sistema, dashboards de desempenho	4-6 horas por relatório
Realização de auditorias regulares para garantir a conformidade com as políticas de segurança e regulamentos.	Trimestral	Relatórios de auditoria, documentação de conformidade	1-2 dias por auditoria
Análise estatística e preditiva para identificar tendências e possíveis problemas futuros.	Mensal	Relatórios de análise estatística, previsões de tendências, gráficos de tendências	6-8 horas por análise
Proposição de medidas mitigatórias para minimizar o impacto de problemas futuros.	Mensal	Planos de mitigação, recomendações de ações preventivas	4-6 horas por proposta
Análise de padrões de comportamento e desempenho para detectar desvios inesperados.	Quinzenal	Relatórios de análise de padrões, alertas de desvios	4-6 horas por análise
Coleta e agregação de dados de diversas fontes (logs, métricas, traços).	Diária	Relatórios de agregação de dados	2-4 horas diárias

Serviços de Operação Assistida e Análise Contínua	Periodicidade	Produtos. Entregáveis	Expectativa de retorno
Implementação de monitoramento contínuo para identificar ameaças de segurança e vulnerabilidades.	Contínua	Relatórios de monitoramento, alertas de segurança, documentação de vulnerabilidades	8 horas iniciais, 2 horas semanais de manutenção
Identificação e mitigação de riscos de segurança.	Mensal	Planos de mitigação de riscos, relatórios de segurança	4-6 horas por análise
Previsão de tendências de uso e planejamento de capacidade baseado em análise estatística.	Mensal	Relatórios de previsão de uso, planos de capacidade	6-8 horas por análise
Balanceamento da distribuição de carga e recomendação para ampliação de recursos técnicos conforme necessário.	Mensal	Relatórios de balanceamento de carga, recomendações de escalabilidade	6-8 horas por análise
Realização de testes de carga para avaliar a capacidade e desempenho dos sistemas.	Trimestral	Relatórios de testes de carga, gráficos de desempenho	2-3 dias por teste
Identificação de possíveis gargalos e pontos de falha sob condições de alta demanda.	Mensal	Relatórios de gargalos, documentação de pontos de falha	6-8 horas por análise
Integração das ferramentas de OBSERVABILIDADE com outras soluções de TI já existentes.	Semestral	Relatórios de integração, documentação de interoperabilidade	2-3 dias por integração
Customização de integrações para assegurar a interoperabilidade entre sistemas diferentes.	Semestral	Documentação de customizações, relatórios de testes de integração	2-3 dias por customização
Adaptação de estratégias de OBSERVABILIDADE com base no feedback e nas mudanças de ambiente.	Mensal	Relatórios de adaptação, documentação de mudanças nas estratégias	4-6 horas por análise
Fornecimento de suporte técnico especializado para resolução de problemas relacionados à OBSERVABILIDADE.	Conforme necessário	Relatórios de suporte, logs de atendimento técnico, documentação de resolução de problemas	1-2 horas por incidente

Serviços de Operação Assistida e Análise Contínua	Periodicidade	Produtos. Entregáveis	Expectativa de retorno
Operação assistida, para realizar ajustes	Conforme necessário	Apoiar durante o uso cotidiano da plataforma, incluindo ajustes finos e análise de eventos;	1-2 horas por demanda

Tabela 2 - Catalogo de Serviços

3.7.7.4 Os serviços relacionados na tabela anterior terão medidos os seus esforços para execução em HST e obedecerão aos critérios de dimensionamento apresentados nos próximos itens deste Termo de Referência;

3.7.7.4.1 Processo de Cálculo das Horas Necessárias

O cálculo das horas necessárias para a execução de uma atividade prevista no Catálogo de Serviços deverá seguir um processo estruturado que garanta precisão e conformidade. O processo será realizado conforme as seguintes etapas:

3.7.7.4.2 Identificação da Atividade:

- A equipe técnica deverá identificar a atividade específica a ser realizada, conforme descrito no catálogo de serviços;
- A atividade deverá ser claramente documentada, incluindo a justificativa da sua execução.

3.7.7.4.3 Estimativa Preliminar:

- A partir da descrição da atividade, será realizada uma estimativa preliminar do esforço necessário, considerando:
  - Complexidade da Tarefa: Análise qualitativa da dificuldade e do nível técnico requerido;
  - Volume de Dados e Processamento: Avaliação quantitativa do volume de dados envolvidos, quando aplicável;
  - Experiência Anterior: Uso de dados históricos de atividades similares, quando disponíveis.
  - A estimativa será expressa em Horas de Serviço Técnico

3.7.7.4.4 Discussão e Validação da Estimativa:

- A estimativa preliminar será apresentada à gestão do projeto e ao responsável pelo contrato para análise;

- Em conjunto, serão debatidos os seguintes pontos:
  - Clareza da Atividade: A descrição está suficientemente detalhada?
  - Adequação da Estimativa: O tempo calculado está coerente com a complexidade?
  - Ajustes Necessários: Caso necessário, serão feitas correções na previsão de horas.
- A concordância entre as partes será formalizada no documento de Planejamento do Serviço aberta para a atividade.

3.7.7.4.5 Aferição ao Final da Atividade

Após a conclusão da atividade, será realizado um processo de aferição e validação das horas efetivamente dedicadas, conforme os seguintes passos:

- Registro de Horas:
  - O preposto da contratada irá apresentar relatório técnico detalhando o quantitativo de horas efetivamente empreendidas na execução das atividades de forma agrupada dia a dia durante o período de execução. Para cada dia de trabalho efetivo, além do total de horas, a contratada deverá descrever as macros atividades executadas.
- Os registros deverão indicar:
  - Descrição macro da Tarefa Realizada;
  - Tempo Efetivo Gasto (em horas);
  - Resultados Obtidos ou Entregas Realizadas.
- O relatório será submetido à análise da gestão do projeto, que verificará:
  - Conformidade com a OS previamente acordados;
  - Qualidade da Entrega: Se os resultados correspondem ao previsto;
  - Justificativas para Divergências: Caso as horas efetivamente gastas ultrapassem a estimativa inicial, será necessário detalhar as causas e ajustes realizados.
- Avaliação Final:
  - A gestão do projeto realizará uma validação do relatório e, se necessário, solicitará ajustes ou justificativas;
  - Após a validação, o relatório será aprovado e registrado como documento oficial para faturamento e controle de qualidade.

3.7.7.4.6 Critérios de Concordância entre as Partes

Para evitar divergências, as seguintes práticas serão adotadas:

- Planejamento Participativo: A estimativa será construída com a participação das equipes técnicas e da gestão do cliente;
- Validação Prévia: Acordo formal no início da atividade sobre o tempo estimado, registrado no documento de Planejamento do Serviço;
- Monitoramento Contínuo: A gestão acompanhará o progresso por meio de relatórios parciais, possibilitando ajustes ainda durante a execução;
- Registro Transparente: O sistema de gestão de horas deverá garantir a rastreabilidade das atividades, registrando data, hora e descrição da tarefa.

4. DA FUNDAMENTAÇÃO LEGAL DA CONTRATAÇÃO

4.1. A presente contratação tem fundamento na Lei Federal n.º 13.303/2016, no Regulamento de Licitações e Contratos da IPLANRIO – RLC IPLANRIO, disponível no Portal da Prefeitura do Rio de Janeiro: https://iplanrio.prefeitura.rio/contratos-e-licitacoes/, bem como nas regras procedimentais acerca da modalidade de pregão eletrônico, dispostas na Lei Federal n.º14.133/2021.

5. DA QUALIFICAÇÃO TÉCNICA

5.1. Prova de aptidão da empresa licitante para desempenho de atividade pertinente e compatível com o objeto da licitação, por meio de certidão (ões) ou atestado (s), fornecido (s) por pessoa jurídica de direito público ou privado de fornecimento de licenças/subscrição na solução de APM ofertada, incluindo consultoria técnica especializada.

5.2. Considera-se compatível com o objeto da licitação o fornecimento de licenciamento de soluções de observabilidade e prestação de Serviços relacionados à operacionalização e consultoria na disciplina APM e na solução ofertada, que:

5.2.1. A solução referenciada no atestado tenha a capacidade de monitorar no **mínimo 59 hosts e 500 mil acessos de usuários**, pelo período mínimo de 12 (doze) meses, executado de forma satisfatória.

5.2.2. Além da comprovação do fornecimento de licenciamento, a licitante deverá comprovar a execução de ao **menos 1.000 horas de serviços técnicos especializados** especificamente na disciplina APM (análise de performance de aplicações) com o uso da solução de observabilidade

5.3. Será admitida a soma dos atestados ou certidões apresentadas pelas licitantes, desde que os mesmos sejam tecnicamente pertinentes e compatíveis em características, quantidades e prazos com o objeto da licitação.

5.4. A licitante deverá apresentar carta de apresentação, emitida pelo fabricante da solução ofertada, indicando que o licitante é uma empresa que faz parte do programa de parceria formal e está autorizada e capacitada a revender os produtos e serviços ofertados.

5.5. A licitante deverá apresentar documentação comprovando o atendimento a todos os requisitos funcionais da solução ofertada. A equipe técnica Da CONTRATANTE irá realizar a análise da documentação apresentada e caso seja caracterizado que a documentação não seja suficiente para comprovar o atendimento a todos os requisitos, a licitante será convocada a realizar prova de bancada para demonstração dos itens não esclarecidos na documentação.

5.6. É facultativo, a prova de bancada para confirmação de atendimento os requisitos técnicos solicitados de para dos módulos/solução ofertada, em caso de necessidade:

5.6.1. A comissão de pregão fará a convocação para apresentação da prova de bancada, descrito no ANEXO III;

5.6.2. A Licitante deverá demonstrar até o prazo máximo de 03 dias úteis, podendo ser prorrogado a critério da Comissão de Licitação.

5.6.3. A Licitante deverá demonstrar os requisitos solicitados em ambiente próprio para a equipe técnica da CONTRATANTE realizar a avaliação em que preencherá o quadro de requisitos do ANEXO III quanto ao atendimento do requisito pelo Licitante;

5.6.4. Em caso, de não atendimento dos requisitos técnicos solicitados a Licitante poderá ser inabilitada do certame.

5.7. Caso a licitante não comprove o atendimento a todos os requisitos, seja via documentação seja via prova de bancada, a licitante será inabilitada.

5.8. A licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

5.9. O (s) atestado (s) apresentado (s) pela licitante devem (rão) conter no mínimo as seguintes informações:

- Identificação do órgão ou empresa emitente com nome ou razão social, CNPJ, endereço completo, nome da pessoa responsável e função no órgão ou empresa, telefone e fax para contato;
- Indicação do CONTRATANTE de que foram atendidos os requisitos de qualidade e prazos requeridos (descrição, duração e avaliação dos resultados);
- Descrição das principais características dos serviços, comprovando que a CONTRATADA executa ou executou o objeto da contratação, considerando;
- Data de emissão do atestado ou da certidão;
- Assinatura e identificação do signatário (nome, telefone, cargo e função que exerce junto ao órgão ou empresa emitente).

5.10. Ficará a cargo da CONTRATANTE, caso julgue necessário, realizar diligências para averiguação das informações constantes dos atestados de capacidade técnica apresentados.

5.11. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

5.12. Declaração formal da licitante de que disponibilizará, no momento da execução do objeto de profissional com certificação oficial ou declaração emitida pelo fabricante da solução de APM ofertada atestando a capacidade técnica e ter experiência comprovada em soluções de monitoramento de performance de aplicação (APM), que atende a exigência contida no Termo de Referência.

5.13. Para fins de qualificação técnica, a licitante deverá apresentar TODOS os documentos, atestados, declarações e certidões, que comprovem a solução ofertada e que demonstrem experiência e conhecimento avançados da Licitante.

6. DAS OBRIGAÇÕES DA CONTRATANTE

6.1. São obrigações da CONTRATANTE:

6.1.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

6.1.2. Encaminhar formalmente a demanda por meio de documento contratual, de acordo com os critérios estabelecidos no TERMO DE REFERÊNCIA;
6.1.3. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;
6.1.4. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;
6.1.5. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC.

7. DAS OBRIGAÇÕES DA CONTRATADA

São obrigações da CONTRATADA:
7.1. Realizar os serviços de acordo com todas as exigências contidas no Termo de Referência e na proposta;
7.2. Tomar as medidas preventivas necessárias para evitar danos a terceiros, em consequência da execução dos serviços;
7.3. Responsabilizar-se integralmente pelo ressarcimento de quaisquer danos e prejuízos, de qualquer natureza, que causar à CONTRATANTE ou a terceiros, decorrentes da execução do objeto desta contratação, respondendo por si, seus empregados, prepostos e sucessores, independentemente das medidas preventivas adotadas e da comprovação de sua culpa ou dolo na execução do contrato;
7.4. Atender às determinações e exigências formuladas pela CONTRATANTE;
7.5. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios defeitos ou incorreções resultantes da execução ou de materiais empregados, no prazo determinado pela Fiscalização;
7.6. Responsabilizar-se, na forma do Contrato, por todos os ônus, encargos e obrigações comerciais, sociais, tributárias, trabalhistas e previdenciárias, ou quaisquer outras previstas na legislação em vigor, bem como por todos os gastos e encargos com material e mão-de-obra necessária à completa execução dos serviços:
7.7. Em caso de ajuizamento de ações trabalhistas contra a CONTRATADA, decorrentes da execução do presente Contrato, com a inclusão do Município do Rio de Janeiro ou da CONTRATANTE a como responsável subsidiário ou solidário, a CONTRATANTE poderá reter, das parcelas vincendas, o montante dos valores cobrados, que serão complementados a qualquer tempo com nova retenção em caso de insuficiência:

"a". No caso da existência de débitos tributários ou previdenciários, decorrentes da execução do presente Contrato, que possam ensejar responsabilidade subsidiária ou solidária da CONTRATANTE, as parcelas vincendas poderão ser retidas até o montante dos valores cobrados, que serão complementados a qualquer tempo com nova retenção em caso de insuficiência;

"b". As retenções previstas nas alíneas "a" e no item 7.7, caput poderão ser realizadas tão logo tenha ciência o Município do Rio de Janeiro ou a CONTRATANTE da existência de ação trabalhista ou de débitos tributários e previdenciários e serão destinadas ao pagamento das respectivas obrigações caso o Município do Rio de Janeiro ou entidade da Administração Pública indireta sejam compelidos a tanto, administrativa o judicialmente, não cabendo, em nenhuma hipótese, ressarcimento à CONTRATADA.

"c". Eventuais retenções previstas no item 7.7, caput e alínea "a" somente serão liberadas pela CONTRATANTE se houver justa causa devidamente fundamentada.

7.8. Manter as condições de habilitação e qualificação exigidas para a contratação durante todo prazo de execução contratual;

7.9. Responsabilizar-se inteira e exclusivamente pelo uso regular de marcas, patentes, registros, processos e licenças relativas à execução desta contratação, eximindo a CONTRATANTE das consequências de qualquer utilização indevida;

7.10. Observar o disposto no Decreto Municipal nº 27.715/07, no que couber.

7.11. Indicar, nas notas fiscais emitidas, quando o objeto envolver prestação de serviços, o efetivo período do mês que está sendo faturado.

7.12. Indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato;

7.13. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

7.14. Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão.

8. FORMA DE DISPONIBILIZAÇÃO DO SERVIÇO

8.1. FORNECIMENTO DAS LICENÇAS

8.1.1. A disponibilização das licenças deverá ser realizada por meio eletrônico a ser informado pelo responsável técnico da CONTRATANTE.

8.1.2. Deve ser disponibilizado pela CONTRATADA todas as informações de acesso ao site do fabricante para gestão das licenças, abertura de suporte técnico e acesso a base de conhecimento.

8.1.3. A solução objeto desta contratação deverá ser fornecida na modalidade SaaS, a Contratada deverá disponibilizar os recursos de computação em provedor que possua ao menos as certificações: ABNT NBR ISO/IEC 27001:2013;ISO/IEC 27017:2015; e ISO/IEC 27018:2019, com validade vigente durante a execução do contrato, referentes à infraestrutura hospedada em datacenter no Brasil.

8.1.4. Responsabilizar-se, na forma do Contrato, pela qualidade dos serviços executados e dos materiais empregados, em conformidade com as especificações do Termo de Referência, com as normas da Associação Brasileira de Normas Técnicas – ABNT, e demais normas técnicas pertinentes, a ser atestada pelos responsáveis pela fiscalização da execução do contrato, assim como pelo refazimento do serviço e a substituição dos materiais recusados, sem ônus para o(a) CONTRATANTE e sem prejuízo da aplicação das sanções cabíveis.

8.1.5. O fornecimento das licenças deverá contemplar todos os recursos técnicos, capacidades de monitoramento e perfis de acesso previstos neste Termo de Referência, conforme as unidades contratadas.

8.1.6. A disponibilização do ambiente licenciado deverá ocorrer de forma eletrônica e remota, por meio de endereço de acesso web seguro (via HTTPS), em conformidade com as orientações do responsável técnico da CONTRATANTE, e em até 5 (cinco) dias úteis após a assinatura do contrato.

8.1.7. A CONTRATADA deverá garantir, no ato da disponibilização:

8.1.7.1. A criação de conta administrativa com perfil de superusuário (admin/root) para a equipe designada pela CONTRATANTE;

8.1.7.2. O fornecimento das credenciais iniciais de acesso, com a possibilidade de personalização de usuários, permissões e autenticação multifator (MFA);

8.1.7.3. A disponibilização de um painel de gestão de licenças e consumo, com visibilidade em tempo real das unidades utilizadas, limites contratados e histórico de uso;

8.1.7.4. O acesso à central de suporte técnico do fabricante, incluindo abertura de chamados (tickets), acompanhamento de solicitações e acesso ao nível de suporte previsto no contrato;

8.1.7.5. A liberação integral à base de conhecimento (knowledge base), documentação técnica, manuais de uso, guias de configuração e recursos de autoatendimento;

8.1.7.6. A confirmação de que o ambiente se encontra operacional e pronto para início dos serviços de parametrização e implantação, conforme cronograma estabelecido.

8.1.8. As licenças fornecidas deverão ser exclusivas, intransferíveis e com validade vinculada à vigência contratual. A solução deverá permitir ampliação escalonada das capacidades contratadas, mediante solicitação da CONTRATANTE e sem interrupção dos serviços já em operação.

8.1.9. A CONTRATADA deverá assegurar que as atualizações de versão, correções e melhorias sejam aplicadas automaticamente, sem ônus adicional e sem necessidade de intervenção da equipe da CONTRATANTE, garantindo o acesso contínuo às funcionalidades mais recentes.

8.2. DA PRESTAÇÃO DOS SERVIÇOS:

8.2.1. A prestação dos serviços associados à solução de Observabilidade contratada será realizada de forma parcial ou total sob demanda, conforme as necessidades da CONTRATANTE, mediante documento contratual, nos termos do fluxo operacional estabelecido no item 3.7.5 deste Termo de Referência.

8.2.2. A utilização das horas contratadas, deverá ser por meio de documento de Planejamento do Serviço, deverá conter, no mínimo, a descrição do escopo, a quantidade de unidades a serem utilizadas, os prazos de execução, os entregáveis esperados, e os indicadores de aceite técnico, conforme modelos e condições previamente pactuados contratualmente.

8.2.3. A utilização das horas (HST) contratadas, deverá ser por meio de documento de Planejamento do Serviço, deverá conter, no mínimo, a descrição do escopo, a quantidade de unidades a serem utilizadas, os prazos de execução, os entregáveis esperados, e os indicadores de aceite técnico, conforme modelos e condições previamente pactuados contratualmente.

8.2.4. A CONTRATADA deverá prestar os serviços com base nos seguintes componentes previstos no objeto do contrato:

8.2.4.1. Serviços de Implantação: configuração inicial da solução, integração com os sistemas da CONTRATANTE, adequação de regras de monitoramento, dashboards, alertas e painéis, com foco na ativação técnica dos módulos previstos;

8.2.4.2. Serviços de Capacitação: realização de treinamentos teóricos e práticos para os profissionais da CONTRATANTE, voltados à operação da ferramenta, interpretação dos dados e incorporação da disciplina de observabilidade às rotinas de desenvolvimento, suporte e operação;

8.2.4.3. Serviços Especializados de Operação Assistida e Análise Contínua: elaboração periódica de diagnósticos e relatórios técnicos, com identificação de causas-raiz de falhas, sugestões de melhoria da performance e recomendações proativas com base em dados históricos e correlação entre módulos da solução.

8.2.5. A execução de cada serviço deverá respeitar o planejamento acordado entre as partes, e deverá resultar em produtos documentados, como relatórios técnicos, planos de ação, registros de intervenções, certificados de capacitação, entre outros.

8.2.6. A CONTRATADA deverá manter equipe técnica habilitada e com domínio sobre a solução fornecida, podendo realizar os serviços tanto de forma remota quanto presencial, conforme especificado durante toda a vigência do contrato.

8.2.7. A CONTRATANTE se reserva o direito de solicitar serviços pontuais, contínuos ou escaláveis, de acordo com sua demanda interna, sem gerar ônus a CONTRATANTE, referente a atividades previstas neste Termo de referência.

8.2.8. O Termo de aceite parcial ou definitivo do serviço executado será condicionado à validação técnica formal pela CONTRATANTE, com base nos entregáveis, critérios de qualidade e resultados definidos em cada documento de Planejamento do Serviço, podendo ser utilizados, para fins de comprovação, os registros extraídos da própria solução contratada.

9. DOS PRAZOS

9.1. O prazo de vigência da Ata de Registro de Preço é de 12 (doze) meses, podendo ser prorrogado, nos termos da legislação em vigor.

9.2. O prazo de vigência da contratação é de 24 (vinte e quatro) meses, a partir da data da publicação do instrumento correspondente no Diário Oficial do Município do Rio de Janeiro.

9.3. Os prazos de execução dos serviços poderão ser prorrogados ou alterados nos termos do Decreto Municipal nº 44.698/2018 e do Regulamento de Licitações e contratos da IPLANRIO.

9.4. A disponibilização da solução, devidamente licenciada deverá ocorrer no prazo máximo de 5 (cinco) dias úteis, contados a partir da data de celebração do contrato. A solução deverá estar plenamente acessível para implantação, configuração, parametrização e uso técnico a partir deste prazo.

9.5. Os prazos de execução dos serviços contratados de implantação, capacitação, operação assistida e análise contínua, serão definidos no documento de Planejamento do Serviço, com os seguintes prazos máximos para os sistemas envolvidos:

9.5.1. Serviços de Implantação: até 20 (vinte) dias corridos após a disponibilização do ambiente;

9.5.2. Serviços de Capacitação: até 10 (dez) dias úteis, quando contratado, conforme definido no documento de Planejamento do Serviço;

9.5.3. Serviços Especializados de Operação Assistida e Análise Contínua: quando contratado, conforme definido no documento de Planejamento do Serviço, a entrega dos relatórios técnicos em até 10 (dez) dias úteis do período de referência.

9.6. Todos os prazos definidos neste Termo de Referência e no documento de Planejamento do Serviço serão contados em dias corridos ou úteis, conforme expressamente indicado, sendo o prazo contratual global de vigência contado sempre em dias corridos, salvo estipulação diversa no contrato.

9.7. O prazo da garantia técnica deverá vigorar durante todo o período de vigência contratual, sendo assegurada inclusive nas fases de implantação, operação assistida, análise contínua e suporte técnico.

9.8. O prazo de garantia do fornecimento das licenças será prestado durante a vigência do contrato.

10. DA GARANTIA CONTRATUAL

10.1. A CONTRATADA prestará garantia de 2% (dois por cento) do valor total do Contrato, como determina o art. 457 do RGCAF, a ser prestada antes do ato de assinatura, em uma das modalidades previstas no art. 445 do RGCAF e no art. 81 do Decreto Municipal n.º 44.698/2018. Seus reforços poderão ser igualmente prestados nas mesmas modalidades. Caso o fornecedor escolha a modalidade seguro-garantia, esta deverá incluir a cobertura das multas eventualmente aplicadas, e, caso escolha a modalidade carta-fiança, deverá observar as regras específicas eventualmente existentes e informadas pela Contratante.

10.2. A CONTRATANTE se utilizará da garantia para assegurar as obrigações associadas à contratação, podendo recorrer a esta inclusive para cobrar valores de multas eventualmente aplicadas e ressarcir-se dos prejuízos que lhe forem causados em virtude do descumprimento das referidas obrigações. Para reparar esses prejuízos, poderá a CONTRATANTE ainda reter créditos.

10.3. Os valores das multas impostas por descumprimento das obrigações assumidas na contratação serão descontados da garantia caso não venham a ser quitados no prazo de 03 (três) dias úteis, contados da ciência da aplicação da penalidade. Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá a CONTRATADA pela diferença, que será descontada dos pagamentos eventualmente devidos pela Administração ou cobrada judicialmente.

10.4. Em caso de rescisão decorrente de falta imputável à CONTRATADA, a garantia reverterá integralmente à CONTRATANTE, que promoverá a cobrança de eventual diferença que venha a ser apurada entre o importe da garantia prestada e o débito verificado.

10.5. - Na hipótese de descontos da garantia a qualquer título, seu valor original deverá ser integralmente recomposto no prazo de 7 (sete) dias úteis, exceto no caso da cobrança de valores de multas aplicadas, em que esse será de 48 (quarenta e oito) horas, sempre contados da utilização ou da notificação pela CONTRATANTE, o que ocorrer por último, sob pena de rescisão administrativa do Contrato.

10.6. Caso o valor da contratação seja alterado, de acordo com o art.92 do Decreto Municipal 44.698/2018, a CONTRATADA deverá complementar o valor da garantia para que seja mantido o percentual de 2% (dois porcento) do valor do Contrato.

10.7. Sempre que houver reajuste ou alteração do valor da contratação, a garantia será complementada no prazo de 7 (sete) dias úteis do recebimento, pela CONTRATADA, do correspondente aviso, sob pena de aplicação das sanções previstas no RGCAF.

10.8. A garantia contratual só será liberada ou restituída com o integral cumprimento da contratação, mediante ato liberatório da autoridade contratante, de acordo com o art. 465 do RGCAF e, quando em dinheiro, atualizada monetariamente, podendo ser retida, se necessário, para quitar eventuais obrigações da CONTRATADA.

11. DA FISCALIZAÇÃO E ACEITE DO OBJETO

11.1. A execução do contrato será acompanhada e fiscalizada por representantes designados pela CONTRATANTE, doravante denominados Fiscais do Contrato, que atuarão conforme previsto no Regulamento de Licitações e Contratos da CONTRATANTE, bem como nas cláusulas contratuais específicas.

11.2. A CONTRATADA submeter-se-á a todas as medidas e procedimentos de Fiscalização. Os atos de fiscalização, inclusive inspeções e testes, executados pela CONTRATANTE e/ou por seus prepostos, não eximem a CONTRATADA de suas obrigações no que se refere ao cumprimento das normas, especificações e projetos, nem de qualquer de suas responsabilidades legais e contratuais.

11.3. A CONTRATADA deverá fornecer aos fiscais do contrato todas as informações, relatórios e acessos necessários à fiscalização, inclusive acesso aos dashboards, painéis de uso e consumo, históricos de alertas e documentação técnica produzida.

11.4. A fiscalização compreenderá a supervisão técnica, administrativa e funcional do fornecimento das licenças e da execução dos serviços, abrangendo:

11.4.1. Verificação da ativação e operação da solução conforme requisitos deste Termo de Referência;

11.4.2. Acompanhamento da execução de cada documento de Planejamento do Serviço, desde o aceite da solicitação até a entrega dos produtos e resultados previstos;

11.4.3. Avaliação da conformidade dos entregáveis, da documentação técnica e dos prazos pactuados;

11.4.4. Aferição de desempenho com base em indicadores técnicos, relatórios da ferramenta contratada e registros da execução;

11.4.5. Validação da correta utilização das unidades contratadas, conforme limites, formatos e métricas definidas.

11.5. A Fiscalização da prestação de serviços caberá à comissão designada por ato da autoridade competente no âmbito da CONTRATANTE. Incumbe à Fiscalização a prática de todos os atos que lhe são próprios nos termos da legislação em vigor, respeitados o contraditório e a ampla defesa.

11.6. A CONTRATADA declara, antecipadamente, aceitar todas as decisões, métodos e processos de inspeção, verificação e controle adotados pela CONTRATANTE, se obrigando a fornecer os dados, elementos, explicações, esclarecimentos e comunicações de que este necessitar e que forem considerados necessários ao desempenho de suas atividades.

11.7. A CONTRATADA se obriga a permitir que o pessoal da fiscalização da CONTRATANTE acesse quaisquer de suas dependências, possibilitando o exame das instalações e também das anotações relativas aos equipamentos, pessoas e materiais, fornecendo, quando solicitados, todos os dados e elementos referentes à execução do contrato.

11.8. Compete à CONTRATADA fazer minucioso exame das especificações dos bens, de modo a permitir, a tempo e por escrito, apresentar à Fiscalização, para o devido esclarecimento, todas as divergências ou dúvidas porventura encontradas e que venham a impedir o bom desempenho do Contrato. O silêncio implica total aceitação das condições estabelecidas.

11.9. A atuação fiscalizadora em nada restringirá a responsabilidade única, integral e exclusiva da CONTRATADA no que concerne aos bens adquiridos, à sua entrega e às consequências e implicações, próximas ou remotas, perante a CONTRATANTE, ou perante terceiros, do mesmo modo que a ocorrência de eventuais irregularidades na execução contratual não implicará corresponsabilidade da CONTRATANTE ou de seus prepostos.

11.10. A aceitação do objeto deste Termo de Referência se dará mediante a avaliação de Comissão de Fiscalização designada pela autoridade competente no âmbito da CONTRATANTE, e constituída na forma do art. 501, do RGCAF, que constatará se os bens fornecidos atendem a todas as especificações contidas neste Termo de Referência ou no processo que ensejou a presente contratação.

11.11. Os aceites decorrentes da execução contratual serão classificados em duas modalidades distintas:

11.11.1. Aceite de Fornecimento da Solução: refere-se à disponibilização da solução de Observabilidade, conforme as condições técnicas estabelecidas neste Termo de Referência. Será realizado uma única vez, no início da vigência, mediante verificação do pleno funcionamento do ambiente, em conformidade com todos os requisitos elencados neste Termo de Referência e seus anexos, acesso aos recursos contratados e habilitação dos mecanismos de gestão, suporte e controle de consumo;

11.11.2. Aceites de Execução de Serviços: referem-se à comprovação da realização dos serviços previstos no contrato, mediante a entrega dos respectivos entregáveis, que funcionam como evidência objetiva da execução técnica. Os entregáveis devem estar em conformidade com os critérios definidos no documento de Planejamento do Serviço e podem incluir relatórios analíticos, configurações aplicadas, registros operacionais, documentos técnicos, certificados de capacitação ou qualquer outro artefato vinculado ao escopo demandado.

11.12. Cada aceite será formalizado por meio de Termo de Aceite específico, emitido pela equipe técnica da CONTRATANTE, sendo condição indispensável para a liquidação do pagamento correspondente. Nos casos de prestação contínua, o aceite poderá adotar periodicidade definida em OS ou cronograma de referência:

11.12.1. Após o recebimento do produto ou serviço executado, nos termos do objeto contratual ou do documento de Planejamento do Serviço, a CONTRATANTE terá o prazo máximo de 5 (cinco) dias úteis para realizar a verificação técnica, emitir parecer de aceite provisório e comunicar formalmente a CONTRATADA.

11.12.2. A ausência de manifestação por parte da CONTRATANTE dentro do prazo previsto será considerada como concordância tácita, implicando o aceite definitivo por decurso de prazo, possibilitando à CONTRATADA a tramitação do processo de faturamento, conforme o fluxo financeiro estabelecido no contrato.

11.12.3. O aceite provisório deverá conter a descrição do objeto avaliado, a indicação de conformidade ou não conformidade, a relação de eventuais pendências ou falhas identificadas, bem como o posicionamento inicial da CONTRATANTE quanto à aptidão para liquidação e pagamento.

11.12.4. Recebido o aceite provisório, a CONTRATADA terá o prazo de 3 (três) dias úteis para se manifestar de forma expressa quanto à concordância ou discordância com o conteúdo do parecer técnico emitido.

11.12.5. Na hipótese de concordância, o aceite será considerado definitivo, e a CONTRATANTE deverá emitir a respectiva nota fiscal, conforme estabelecido no contrato.

11.12.6. Na hipótese de discordância, a CONTRATADA deverá apresentar justificativa técnica detalhada, acompanhada de evidências que sustentem a sua posição, dentro do mesmo prazo de 3 (três) dias úteis.

11.12.7. Caberá à CONTRATANTE reavaliar os argumentos apresentados e, se necessário, convocar reunião técnica com a CONTRATADA para deliberar sobre os pontos em disputa, fixando prazo adicional para correções ou complementações, limitado a 3 (três) dias úteis, prorrogável uma única vez mediante justificativa aceita.

11.12.8. A ausência de manifestação por parte da CONTRATADA dentro do prazo previsto será considerada como concordância tácita, implicando o aceite definitivo por decurso de prazo.

11.12.9. O aceite definitivo será formalizado por meio de Termo de Aceite, físico ou eletrônico, conforme os meios operacionais da CONTRATANTE, e passará a integrar o processo administrativo da contratação, servindo como documento habilitador para a fase de liquidação financeira.

11.12.10. Nos casos em que a CONTRATANTE, por qualquer motivo, não se manifestar no prazo de 10 (dez) dias úteis após a entrega formal do produto ou conclusão do serviço, a CONTRATADA poderá solicitar formalmente a manifestação. Persistindo o silêncio da CONTRATANTE por mais 5 (cinco) dias úteis contados da solicitação, o aceite será considerado tácito, para todos os efeitos administrativos e contratuais, desde que não haja registro formal de não conformidade

11.13. O objeto do presente Termo de Referência será recebido em tantas parcelas quantas forem as relativas ao pagamento.

11.14. Os serviços cujos padrões de qualidade estejam em desacordo com a especificação deste Termo de Referência e seus anexos deverão ser recusados pela Comissão responsável pela fiscalização do contrato, que anotará em registro próprio as ocorrências e determinará o que for necessário à regularização das faltas ou defeitos observados. No que exceder à sua competência, comunicará o fato à autoridade superior, em 5 (cinco) dias, para ratificação.

11.15. Na hipótese de recusa de aceitação, por não atenderem às exigências da CONTRATANTE, a CONTRATADA deverá substituir quaisquer bens defeituosos ou qualitativamente inferiores, passando a contar os prazos para pagamento e demais compromissos da CONTRATANTE da data da efetiva aceitação. Caso a CONTRATADA não substitua os bens não aceitos no prazo assinado, a CONTRATANTE se reserva o direito de providenciar o seu fornecimento às expensas da CONTRATADA, sem prejuízo das penalidades cabíveis.

11.16. A CONTRATANTE poderá solicitar ajustes ou complementações antes do aceite final, sem ônus adicional, nos casos em que os produtos ou serviços não atenderem integralmente aos critérios estabelecidos na OS ou neste Termo de Referência.

11.17. O Aceite Definitivo ficará a cargo da Comissão de Fiscalização, que emitirá Termo de Aceitação Definitiva em até 05 (cinco) dias úteis, após a entrega do (s) material (is) /equipamento (s).

11.18. As notas fiscais referentes ao recebimento do objeto serão atestadas por até 02 (dois) servidores a serem designados pela CONTRATANTE, observadas as formalidades descritas no Decreto Municipal n.º 34.012/2011 ou em outro que vier a substituí-lo.

11.19. O encerramento contratual observará a verificação do cumprimento de obrigações acessórias, como a finalização de acessos, devolução de documentos, entrega de relatórios consolidados e liberação de ambientes, sem prejuízo dos aceites técnicos já realizados ao longo da vigência.

11.20. A fiscalização exercida pela CONTRATANTE não exime a CONTRATADA de sua responsabilidade integral pela perfeita execução do objeto, tampouco transfere a responsabilidade por eventuais falhas, vícios ou omissões técnicas.

12. ACORDO DE NÍVEL DE SERVIÇO

12.1. Os níveis mínimos de serviço representam um compromisso assumido por um prestador de serviço perante um cliente para que se possa aferir as entregas programadas dos serviços.

12.2. Por se tratar de níveis mínimos, entende-se que a CONTRATADA deverá entregar, no mínimo, os resultados definidos, para que não esteja sujeita a glosas ou descontos nos seus vencimentos.

12.3. A unidade de medida adotada para remuneração do serviço prestado no item 3,3,3 será mensurado de acordo com o esforço do serviço executado, e o pagamento será mensal, ajustado conforme os níveis de serviço apresentados.

12.4. Os indicadores de cada serviço serão aferidos mensalmente, para eventuais ajustes no valor da fatura mensal e deverão constar no relatório mensal de prestação de serviços com o nível de detalhe necessário para conferência pela CONTRATANTE.

12.5. Os serviços de suporte técnico vinculados à subscrição de licenças da solução deverão ser prestados em regime 24x7x365, ou seja, 24 horas por dia, 7 dias por semana, todos os dias do ano, inclusive feriados. O suporte técnico será feito mediante a abertura de chamados em sistema de registro de chamados disponibilizado pela prestadora do serviço.

12.6. Os chamados deverão serão classificados pela CONTRATANTE segundo nível de severidade da ocorrência e prazos de atendimento e resolução, conforme tabela a seguir:

Classificação	Descrição	Prazo para início de atendimento	Tempo máximo de resolução
Crítico	Problema técnico impeça utilização que a da solução em sua totalidade	30 minutos	2 horas
Importante	Problema técnico que impeça o pleno funcionamento de uma funcionalidade	30 minutos	6 horas

Normal	Consulta técnica, dúvidas geral, monitoramento	4 horas	48 horas

Tabela 3- Classificação de Severidade

12.7. O nível de severidade será atribuído pelo CONTRATANTE no momento da abertura do chamado.

12.8. Para fins de apuração do tempo despendido na solução, serão desconsiderados os períodos em que a CONTRATANTE estiver responsável por realizar ações necessárias à análise ou resolução da ocorrência.

12.9. A contagem dos prazos se inicia a partir do registro formal do chamado, o qual deverá conter identificador único para fins de rastreabilidade.

12.10. Entende-se por prazo para iniciar atendimento o tempo máximo permitido até o primeiro contato do técnico da CONTRATADA com a equipe da CONTRATANTE, a partir do momento de abertura do chamado.

12.11. Ao término do atendimento (fechamento do chamado), a CONTRATADA deverá registrar, detalhadamente, por e-mail ou web, as causas do problema e a resolução adotada.

12.12. A quantidade de chamados e requisições de suporte será ilimitada.

12.13. As manutenções programadas que impliquem indisponibilidade da solução devem ser notificadas com pelo menos 15 (quinze) dias de antecedência para a CONTRATANTE.

12.14. A CONTRATADA deverá apresentar mensalmente os seguintes indicadores de desempenho:

12.14.1. Indicador de disponibilidade da solução, com detalhamento dos períodos de indisponibilidade (downtime);

12.14.2. Indicadores de chamados: número de chamados abertos, atendidos e não atendidos, com respectivos prazos de início de atendimento, início e conclusão da resolução.

12.15. Os valores de referência sobre os quais as penalidades aplicáveis incidirão são os seguintes:

12.15.1. Valor Fixo Inicial com pagamento antecipado (up front): aplicável às subscrições de software, cujo acesso será garantido integralmente desde o início da vigência contratual;

12.15.2. Valor referente aos módulos de serviços (item 3.3), quando contratados: aplicável sob o valor definido no documento de Planejamento do Serviço e pagos somente após a efetiva execução e aceite dos entregáveis.

12.16. Penalidades por Descumprimento de Níveis de Serviço:

12.16.1. Subscrição de Software (Pagamento efetuado antecipadamente (Up Front))

Tendo em vista que o valor referente à subscrição da solução é pago antecipadamente (up front), o descumprimento das metas mínimas de desempenho não será passível de glosa, mas sim de aplicação de multa compensatória pecuniária, a ser recolhida pela CONTRATADA em favor da CONTRATANTE, conforme critérios abaixo:

Desempenho Aferido Disponibilidade	**Penalidade Aplicável**
≥ 90% e < 98%	Multa de 0,2% sobre o valor antecipado a cada mês de não cumprimento
< 90%	Multa de 0,4% sobre o valor antecipado a cada mês de não cumprimento
Desempenho Aferido Atendimento	**Penalidade Aplicável**
≥ 90% e < 95%	Multa de 0,2% sobre o valor antecipado a cada mês de não cumprimento
< 90%	Multa de 0,4% sobre o valor antecipado a cada mês de não cumprimento

Tabela 4 - Penalidades por Descumprimento de Níveis de Serviço

Em caso, de multa por descumprimento de níveis de serviços, o valor apurado da multa poderá ser descontado do valor prestado no mês, após notificação formal da CONTRATANTE.

12.16.2. Serviços sob Demanda (módulo de serviços)

No caso dos serviços contratados, deverá ser executado de acordo com o documento de Planejamento do Serviço, ao não atingimento dos objetivos, prazos ou entregáveis nos termos definidos no respectivo planejamento implicará glosa proporcional ao item não executado, conforme avaliação da fiscalização do contrato. A glosa será registrada diretamente no valor da fatura do mês de referência, conforme aplicável.

13. DA GARANTIA TÉCNICA

13.1. Para efeitos desta contratação, entende-se por garantia técnica o compromisso da CONTRATADA de assegurar a plena funcionalidade da solução licenciada, bem como a qualidade técnica e a conformidade dos serviços prestados, de acordo com os termos definidos neste Termo de Referência.

13.2. No caso da subscrição de software, a garantia técnica compreende:

13.2.1. O acesso ininterrupto à solução contratada, nos termos de disponibilidade pactuados;

13.2.2. A atualização contínua e automática das funcionalidades da solução, sem custos adicionais;

13.2.3. A correção tempestiva de falhas de funcionamento;

13.2.4. O suporte técnico 24x7x365 conforme os níveis de serviço definidos no item 15 deste TR;

13.2.5. O atendimento aos requisitos de segurança, proteção de dados e desempenho conforme especificado.

13.3. No caso da prestação de serviços sob demanda, a garantia técnica compreende:

13.3.1. A execução integral e satisfatória dos serviços contratados, conforme os prazos, escopos e entregáveis definidos;

13.3.2. A responsabilização por eventuais erros, omissões ou falhas técnicas na execução dos serviços, com obrigação de correção sem ônus adicional para a CONTRATANTE;

13.3.3. O cumprimento dos indicadores mínimos de qualidade, quando aplicáveis, conforme definido neste TR e nos respectivos documentos de planejamento dos serviços.

13.4. A garantia técnica deverá vigorar durante todo o período de vigência contratual, sendo assegurada inclusive nas fases de implantação, operação assistida, análise contínua e suporte técnico.

13.5. Em caso de descumprimento da garantia técnica, a CONTRATADA deverá:

13.5.1. Reparar ou corrigir as falhas identificadas no prazo máximo estabelecido pela CONTRATANTE, sem prejuízo da aplicação de penalidades contratuais;

13.5.2. Apresentar justificativa técnica formal caso o cumprimento da garantia não seja possível nos termos pactuados, sujeita à aceitação expressa da CONTRATANTE;

13.5.3. Arcar com os custos decorrentes de qualquer medida corretiva ou substitutiva necessária, incluindo, se for o caso, a reexecução integral do serviço sem ônus adicional.

13.6. A garantia técnica será aferida com base nos relatórios de execução contratual, incluindo:

13.6.1. Relatórios de disponibilidade e desempenho da solução;

13.6.2. Relatórios mensais de execução de serviços;

13.6.3. Aceites parciais e finais conforme definido neste TR;

13.6.4. Registro de chamados e atendimento técnico.

13.7. O não cumprimento das obrigações de garantia técnica poderá ensejar:
  13.7.1. Glosa de valores, nos casos de serviços contra entrega;
  13.7.2. Aplicação de multas, nos casos de serviços pagos antecipadamente (subscrição);
  13.7.3. Eventual rescisão contratual, conforme previsto na legislação e no contrato.
13.8. O direito da CONTRATANTE à garantia cessará caso a solução seja alterada pela própria CONTRATANTE ou por fornecedores que não a CONTRATADA responsável pelo serviço em questão.
13.9. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços, dos materiais, técnicas e equipamentos empregados, de forma a assegurar o perfeito cumprimento do ajuste, que serão exercidos por um ou mais representantes da CONTRATANTE.

14. FORMA DE PAGAMENTO

14.1. O pagamento referente as as subscrições dos módulos funcionais de serviço, identificados com itens 3.2.1, 3.2.2, 3.2.3 e 3.2.4 do objeto a ser contratado, serão integrais, após o aceite definitivo da CONTRATANTE pelo fornecimento e ativação das subscrições que deverá acontecer em até 5 (cinco) dias úteis, contados a partir da data de assinatura do contrato.
14.2. Para a emissão do aceite definitivo também será necessário comprovar, por declaração do fabricante ou por meio de acesso ao site do fabricante da solução ou através do próprio software, o período que se encontra ativo o serviço ou licenças em nome da CONTRATANTE, deve constar a quantidade total de licenças ou créditos para atender os requisitos contratados.
14.3. Os pagamentos referentes a prestação de serviços, identificados como itens 3.3.1, 3.3.2 e 3.3.3, serão efetuados 30 (trinta) dias após o aceite provisório ou definitivo do documento de Planejamento do Serviço pela CONTRATANTE, respeitando as quantidades de serviço pré-estabelecidos para execução do serviço.
14.4. O pagamento dos itens à CONTRATADA se dará após a regular liquidação da despesa, nos termos do art. 63 da Lei Federal nº 4.320/64, observadas as condições de recebimento do objeto descritas neste Termo de Referência e no Regulamento de Licitações e Contratos da Contratante, além das condições de pagamento descritas neste Termo de Referência.

15. DAS CONDIÇÕES DE PAGAMENTO

15.1. O pagamento à CONTRATADA, será realizado em razão dos serviços efetivamente prestados e aceitos, sem que a CONTRATANTE esteja obrigado (a) a pagar o valor total do contrato caso todo o quantitativo do objeto previsto neste Termo de Referência não tenha sido regularmente entregue e aceito.

15.2. O documento de cobrança será apresentado à Comissão de Fiscalização, para atestação, e, após, protocolado no setor pertinente da CONTRATANTE.

15.3. O prazo para pagamento será de 30 (trinta) dias a contar da data do protocolo do documento de cobrança no setor pertinente da CONTRATANTE.

15.4. Para fins de medição, se for o caso, e faturamento, o período-base de medição do serviço prestado será de um mês, considerando-se o mês civil, podendo no primeiro mês e no último, para fins de acerto de contas, o período se constituir em fração do mês, considerado para esse fim o mês com 30 (trinta) dias.

15.5. No caso de erro nos documentos de cobrança, estes serão devolvidos à CONTRATADA para retificação ou substituição, passando o prazo de pagamento a fluir, então, da reapresentação válida desses documentos.

15.6. O valor dos pagamentos eventualmente efetuados com atraso, desde que não decorra de fato ou ato imputável à CONTRATADA, sofrerá a incidência de juros calculados de acordo com a variação da Taxa Selic, pro rata die entre o 31º (trigésimo primeiro) dia da data do protocolo do documento de cobrança no setor competente da CONTRATANTE e a data do efetivo pagamento, limitado ao percentual de 12% (doze porcento) ao ano.

15.7. O valor dos pagamentos eventualmente antecipados será descontado da taxa de 1% (um por cento) ao mês, calculada para a rata die entre o dia do pagamento e o 30° (trigésimo) dia da data do protocolo do documento de cobrança na tesouraria da CONTRATANTE.

15.8. O pagamento será efetuado à CONTRATADA através de crédito em conta bancária do fornecedor cadastrado junto à Coordenação do Tesouro Municipal.

15.9. A CONTRATADA deverá apresentar juntamente com o documento de cobrança, os comprovantes de recolhimento do FGTS e INSS de todos os empregados atuantes no contrato, assim como Certidão Negativa de Débitos Trabalhistas – CNDT ou Certidão Positiva de Débitos Trabalhistas com efeito negativo válida, declaração de regularidade trabalhista, na forma do Anexo do Edital.

15.6

16. DAS SANÇÕES ADMINISTRATIVAS

16.1. Sem prejuízo de indenização por perdas e danos, a CONTRATANTE poderá impor ao contratado, pelo descumprimento total ou parcial das obrigações a que esteja sujeito, as seguintes sanções, observado o Regulamento

Geral do Código de Administração Financeira e Contabilidade Pública do Município do Rio de Janeiro – RGCAF, o Decreto Municipal n.º 44.698/2018 e o Regulamento de Licitações e Contratos da CONTRATANTE, garantida a defesa prévia ao contratado:

i. Advertência;
ii. Multa de mora de até 1% (um por cento) por dia útil sobre o valor do Contrato ou do saldo não atendido do Contrato;
iii. Multa de até 20% (vinte por cento) sobre o valor do Contrato ou do saldo não atendido do Contrato, conforme o caso, e, respectivamente, nas hipóteses de descumprimento total ou parcial da obrigação, inclusive nos casos de rescisão por culpa da CONTRATADA;
iv. Suspensão temporária do direito de licitar e impedimento de contratar com a Administração Municipal;

16.2. A multa aplicada será depositada em conta bancária indicada pela CONTRATANTE, descontada dos pagamentos eventualmente devidos, descontada da garantia ou cobrada judicialmente.

16.3. As sanções previstas nos incisos I e IV do subitem 16.1 poderão ser aplicadas juntamente com as dos incisos II e III, devendo a defesa prévia do interessado, no respectivo processo, ser apresentada no prazo de 10 (dez) dias úteis e não excluem a possibilidade de rescisão unilateral do contrato;

16.4. Do ato que aplicar a pena prevista no inciso IV do subitem 16.1, a autoridade competente no âmbito da CONTRATANTE dará conhecimento aos demais órgãos e entidades municipais interessados, na página oficial desta empresa pública na internet.

16.5. A sanção prevista no inciso IV do subitem 16.1 poderá também ser aplicada às empresas ou aos profissionais que, em razão dos contratos regidos pelo Decreto Municipal n.º 44.698/2018:

i. Tenham sofrido condenação definitiva por praticarem, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;
ii. Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;
iii. Demonstrem não possuir idoneidade para contratar com a CONTRATANTE em virtude de atos ilícitos praticados.

16.6. As multas previstas nos incisos II e III do subitem 16.1 não possuem caráter compensatório, e, assim, o pagamento delas não eximirá a CONTRATADA de responsabilidade pelas perdas e danos decorrentes das infrações cometidas.

16.7. As multas aplicadas poderão ser compensadas com valores devidos à CONTRATADA mediante requerimento expresso nesse sentido.

16.8. Ressalvada a hipótese de existir requerimento de compensação devidamente formalizado, nenhum pagamento será efetuado à CONTRATADA antes da comprovação do recolhimento da multa ou da prova de sua relevação por ato da Administração, bem como antes da recomposição do valor original da garantia, que tenha sido descontado em virtude

de multa imposta, salvo decisão fundamentada da autoridade competente que autorize o prosseguimento do processo de pagamento.

17. DA MATRIZ DE RISCOS

17.1. Para a presente contratação foram identificados os principais riscos conhecidos na Matriz constante do **Anexo I** deste Termo de Referência, bem como estabelecidos os respectivos responsáveis e descritas suas respostas sugeridas.
17.2. É vedada a celebração de aditivos decorrentes de eventos supervenientes alocados na Matriz de Riscos como sendo de responsabilidade da CONTRATADA.
17.3. Sempre que atendidas as condições do contrato e mantidas as disposições da Matriz de Risco, considera-se mantido o equilíbrio econômico-financeiro.
17.4. A proposta comercial deverá ser elaborada levando em consideração a natureza e a extensão dos riscos relacionados na Matriz de Risco.

18. DA PROTEÇÃO DE DADOS PESSOAIS

18.1. No desenvolvimento de quaisquer atividades relacionadas com a execução deste Termo de Referência, as partes observarão o regime legal concernente à proteção de dados pessoais, se empenhando em proceder ao tratamento de dados pessoais estritamente necessários à execução e ao desenvolvimento do objeto deste Termo de Referência, no estrito e rigoroso cumprimento da Legislação de Privacidade e de Proteção de Dados Pessoais e das demais normas que vierem a disciplinar a matéria.

18.2. A CONTRATADA se obriga a:

a) Tratar os dados pessoais, em especial no que tange às operações de coleta, de produção, de recepção, de classificação, de utilização, de acesso, de reprodução, de transmissão, de distribuição, de processamento, de arquivamento, de armazenamento, de eliminação, de avaliação ou de controle da informação, de modificação, de

comunicação, de transferência, de difusão ou de extração, com a devida observância à Lei nº 13.709, de 14 de agosto de 2018 (LGPD);

b) Tratar os dados pessoais de modo compatível com a finalidade, a adequação e a necessidade, como determina o artigo 6º, I, II e III da Lei nº 13.709/2018, bem como em observância às bases legais descritas no artigo 7º da Lei nº 13.709/2018, no que se refere às operações descritas na alínea "a" do item 9.2;

c) Conservar os dados pessoais apenas durante o período necessário à prossecução das finalidades previstas, como determina os artigos 15 e 16 da Lei nº 13.709/2018, guardada a conformidade aos períodos mínimos de retenção previstos em lei;

d) Assegurar que os respectivos colaboradores ou prestadores de serviços que venham a ter acesso a dados pessoais no contexto deste Termo de Referência cumpram as disposições legais aplicáveis em matéria de proteção de dados pessoais.

18.3. As partes se comprometem a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – compartilhados em decorrência da execução contratual, em consonância com a Lei de Dados Pessoais - LGPD, sendo vedado o compartilhamento das informações a outras empresas ou pessoas, salvo o decorrente de obrigações legais ou para viabilizar o cumprimento do presente avença.

18.4. A solução contratada deverá permitir a implementação regras de detecção, ocultação, controle de acesso e monitoramento do tratamento de dados, para os diversos níveis de risco, definidos pelo controlador ou operador de dados dos sistemas implementados para garantir a conformidade com a Lei de Dados Pessoais.

19. DA PROPOSTA DE PREÇOS

19.1. A licitante deverá apresentar proposta de preços de acordo com as especificações deste Termo de Referência, devendo informar o fabricante, modelo e especificação técnica da solução oferta dentro dos moldes praticados pelo Município do Rio de Janeiro.

19.2. Os preços propostos deverão estar de acordo com os praticados no mercado e neles deverão estar inclusos todos os impostos, taxas, fretes, material, mão de obra, instalações e quaisquer outras despesas necessárias e não especificadas neste Termo de Referência, mas julgadas essenciais ao cumprimento do objeto desta contratação.

20. DO TIPO DE LICITAÇÃO

20.1. O critério de julgamento das propostas será o **Menor preço global**, a não divisão por item se justifica pela especialização técnica exigida na solução de observabilidade em modalidade de serviço (SaaS) em que contemplam a prestação de serviços de operação assistida para auxiliar a equipe de TI da IPLANRIO na agilidade de obter maiores ganhos quanto a melhoria de performance, segurança e arquitetura implementada nos sistemas críticos utilizados e disponibilizados aos munícipes por esta Prefeitura da Cidade do Rio de Janeiro.

20.2. Os itens do escopo de fornecimento possuem correlação ente si e são elementos inseparáveis de uma mesma e única solução de TI para prover o gerenciamento, monitoramento, verificação e análise de aplicações. A separação por item dá-se apenas para clareza na composição dos preços, portanto não se deve ter duas empresas distintas prestando os serviços de integração dos sistemas, que fazem parte da contratação.

21. DO REGIME DE EXECUÇÃO DOS SERVIÇOS:

21.1. No tocante à prestação dos serviços descritos nos itens 3.3.1, 3.3.2 e 3.3.3 do objeto desse TR, tendo a natureza da contratação, em que estes itens do objeto se relacionam com a solução a ser ofertado, e que o escopo da execução dos serviços é sob demanda e o pagamento pela quantidade efetivamente executada, será adotado o regime de execução de empreitada por preço unitário.

Rio de Janeiro, 22 de setembro de 2025.

_____
Luciana Nascimento Santos
Matricula 45/622.373-4
Gerente de Infraestrutura Tecnológica
IPLANRIO/DOP

Aprovo,

_____
Jorge Francisco Antunes da Silva
Matricula 45/622.163-4
Diretor de Operações
IPLANRIO

PREFEITURA RIO | iplanrio

ANEXO I – MATRIZ DE RISCO

Id.	Tipo	Origem	Risco	Categoria	Subcategoria	Aplicação	P	I	P x I	Estratégia	Resposta Sugerida	Responsável
R004	Ameaça	Externa	Devido a alteração da política econômico-financeira, pode haver aumento nos tributos após a contratação	Organizacional	Aquisições	Geral	4	5	**20**	Aceitar ativamente	A contratada deverá buscar alternativas para cumprimento do contrato	Contratada
R005	Ameaça	Estratégica	Devido ao atraso do pagamento do contrato, a equipe da contratada poderá ter seus salários atrasados levando a desmotivação ou a ausência de participação no contrato	Organizacional	Aquisições	Pessoal	8	9	**72**	Mitigar	A contratada deverá manter fluxo de caixa para cobrir a despesa de pessoal e não prejudicar a execução do contrato	Contratada
R008	Ameaça	Estratégica	Devido a fusão ou descredenciamento da contratada junto ao fabricante, pode haver o não fornecimento do produto ou serviço contratado	Organizacional	Aquisições	Geral	3	5	**15**	Aceitar ativamente	A contratada buscar alternativas para cumprimento do contrato	Contratada
R010	Ameaça	Operacional	Sobre preço do produto ou serviço, impactando a ata de registro de preços ou contrato celebrado.	Organizacional	Aquisições	Geral	3	8	**24**	Aceitar ativamente	Negociação, entre a contratante e contratada, para redução do valor ou cancelamento do contrato.	Contratada

R011	Ameaça	Operacional	Devido à complexidade do produto ou outras prioridades da equipe responsável pela homologação, esta poderá ter seu prazo extrapolado	Organizacional	Aquisições	Entrega	5	5	**25**	Mitigar	1) A Comissão de Fiscalização do Contrato deverá sensibilizar o servidor que fará a homologação sobre a importância do cumprimento dos prazos para a conclusão e entrega do produto.2) caso a homologação venha a extrapolar os prazos definidos, a Comissão de Fiscalização do Contrato deverá informar à Contratada e replanejar em conjunto as ações necessárias para entrega do produto, sem prejuízo para a Contratante.	Contratan
R016	Ameaça	Externa	Devido a um baixo nível de maturidade (ou conscientização) em Segurança da Informação dos integrantes das equipes disponilizadas pela contratada para prestação dos serviços, pode ocorrer o vazamento de informações sigilosas da (ou sob custódia da) contratante	Organizacional	Aquisições	Pessoal	5	8	**40**	Mitigar	1) garantir que a atuação das equipes da contratada permaneça em conformidade com as diretrizes expressas na Política de Segurança da Informação, em especial com o princípio dos privilégios mínimos.2) garantir a celebração de Termo de confidencialidade entre a contratante e a contratada.	Contratada

PREFEITURA RIO | iplanrio

ANEXO II- SISTEMAS E APLICAÇÕES A SEREM MONITORADAS

O ambiente tecnológico da CONTRATADA é categorizado como um ambiente de infraestrutura híbrida, formado por aplicações On-Premises e em Nuvem. Parte das aplicações estão em seus ambientes On-Premises e parte estão em Nuvem Google Cloud, Microsoft Azure, e Amazon AWS.

As tecnologias utilizadas nas aplicações são:

a) Arquitetura das aplicações monitoradas: monolítica e serveless;
b) Linguagens: Java superior 8;
c) Linguagens ASP.NET framework superior 4.5
d) Banco de dados: Oracle superior 11c
e) Banco de dados Microsoft SQL Server superior 2008;
f) Banco de dados MariaDB superior 10.3, Mysql superior 5.10
g) Servidor de Aplicação: Weblogic superior a 10.6;
h) Sistema Operacional: Red Hat Enterprise Linux superior 6;
i) Orquestração de Containers: Openshift 4.11 (Kubernetes);
j) Balanceador de carga: F5 – Big IP;
k) Storage: de bloco e de objetos DellEMC;
l) Virtualização: VMWare superior 6.7

As tecnologias podem sofrer alterações ao longo do período, por acréscimo ou por atualização de versão de software.

O dimensionamento das máquinas virtuais (VMs) em uso pelos sistemas alvo de monitoramento, para servir de métrica para a elaboração da proposta de preço dos serviços a serem contratados:
Os nomes dos sistemas não foram disponibilizados para evitar a exposição e riscos inerentes as questões de segurança do ambiente.

Dimensionamento para Observabilidade

PREFEITURA RIO | iplanrio

Item	Sistemas	Server	Memory (GB)	vCpu	Vm´s	Usuários únicos	Log/Mês (GB)	Integrações
1	Sistema 1	Tomcat 8	32	8	12	500	1.000	2
		Middleware	16	2	2			
		Oracle 19c	128	32	1			
2	Sistema 2	.Net 4.8	16	4	6	1.500	500	
		SQLServer 2008	128	32	1			
		repositório	8	2	3			
3	Sistema 3	Oracle 19c- RAC	128	32	2	600	500	4
		Tomcat 8	32	4	6			
		Nodejs	8	2	2			
		Repositório	8	2	1			
4	Sistema 4	Wordpress	16	2	3	1.500	300	8
		Mariadb	16	2	1			
		Container	64	16	4			
		Mongodb	64	16	1			
		Tomcat6/Liferay	16	4	3			
		SQLServer 2008	128	32	1			
5	Sistema 5	Wordpress	8	2	4	1.500	300	
		Mariadb	64	16	1			
6	Sistema 6	Asp.net 4.8	16	6	1	500	300	2
		SQL server 2008	128	32	1			
7	Sistema 7	PHP	32	8	2	200	300	1
		Memcache	16	8	1			
		Mariadb	32	8	1			
8	Sistema 8	PHP	16	8	10	500	1.000	
		Memcache	16	4	1			
		MySQL	32	16	1			
		Repositório	8	2	1			
		Middleware	16	8	2			

9	Sistema 9	Tomcat	64	20	1	100	500	2
		SQL server 2016	98	12	1			
		repositório	8	2	1			
10	Sistema 10	Asp.Net 4.8	16	12	6	1.500	1.000	8
		Oracle 19c RAC	162	32	2			
11	Sistema 11	Oracle 19	98	12	1	1.000	1.000	20
		Tomcat9	32	8	2			
		Weblogic	24	4	2			
		Middleware	8	2	1			
		Repositório	8	2	3			
12	Sistema 12	Asp.net 4.8	16	4	1	500	500	1
		SQL Server 2022	131	64	2			
Total			**Memory (GB)**	**vCpu**	**Vm´s**	**Usuários únicos**	**Log/Mês (GB)**	**Integrações**
			1849	**482**	**98**	**9900**	**7200**	**48**
Margem de crescimento 20%			**2.219**	**578**	**118**	**11880**	**8640**	**58**
Previsão - 24 meses							103680	-
Quantidade a ser contratada			2.219	578	118	11.880	103680	-

Para medição da Experiência do usuário, deverá ser utilizado como base o número de usuários/dia multiplicando por 1000, para se estimar o número sessões por mês para cada sistema, não podendo ultrapassar o total de 13.800.000 de sessões monitoradas.

.

Para mediação do volume de Log, deverá ser utilizado como base o valor de log/mês multiplicado por 24 meses para estimar o volume de armazenamento para cada sistema, não podendo ultrapassar o volume total de 207.360 gigabytes de log.

Para que haja possibilidade de crescimento do ambiente, estima-se um aumento de 20% do parque de VM´s, considerando o total de 118 VM´s a serem monitoradas.

As VMs utilizadas pelas aplicações foram divididas em categorias com as respectivas quantidades de CPU, memória e Logs.

As VMs estarão ligadas e em monitoramento o ano todo (24x7x365).

Para cada documento de Planejamento do Serviço, deverá ser informado os dados de dimensionamento do sistema a ser implementado na solução a ser contratada:

Sistema	Unidade de Referência	Valores de referências
Uso da aplicação		
Hospedagem: On-Premises, Cloud		
Estimativa de volume de dados (GB)		
Estimativa de conexões por mês		
Número de integrações com o sistema		
Número de integrações externas com o sistema		
Experiência do Usuários		
- Estimativa de pageViews		
- Estimativa de usuários da aplicação		
- Estimativa de sessões		

Dimensionamento de maquinas virtuais (VM)

VM	Tecnologia	Camada	Qtde.VM	CPUxCore	Memória (GB)	Log/dia (GB)

Unidade de Referência:

Unidade 1 – Uma unidade 1 deverá ter a capacidade de monitorar até 1 host ou 16,0 GB de memória ou 8 vCPU, na modalidade full-stack. Para a modalidade de monitoramento apenas de infraestrutura, uma unidade 1 deverá ter a capacidade de monitorar um host independente de memória ou CPU.

Unidade 2 – Uma unidade 2 deve ter a capacidade de monitorar até 1.000.000 de visitas de usuários por ano, totalizando 2.000.000 de visitas durante a vigência do contrato (24 meses).

Unidade 3 – Uma unidade 3 deverá ter a capacidade de monitorar até 1 host ou 16,0 GB de memória ou 8 vCPU, na modalidade full-stack. Para a modalidade de monitoramento apenas de infraestrutura, uma unidade 3 deverá ter a capacidade de monitorar um host independente de memória ou CPU.
Unidade 4 – Uma unidade 4 deve ter a capacidade de analisar até 1 TB de logs por ano, totalizando 2 TB durante a vigência do contrato (24 meses).

Unitário – Conjunto de atividades executadas para implantação e configuração da solução executadas uma única vez ao início do contrato.

Turma – Turma de no máximo 10 integrantes a serem capacitadas no uso da solução oferecida segundo programa de treinamento previsto pelo fabricante da solução.

HST – Horas de serviços técnicos a serem executadas sob demanda.

Memória de Cálculo:

Item	Unidade de Medida	Descrição do Item	Métrica	Tipo de Software /Serviço/ Produto	Hosts	8vcpu	4GB mem
1	Unidade	Módulo de análise de aplicações	Unidade 1	Software	118 Hosts ou	578 vpcu / 8 = 73 pack 8 vcpu	2219 Gb mem / 16 Gb mem = 139 pack 16 GB mem
2	Unidade	Módulo de análise de usuários	Unidade 2	Software	11.880 * 1000 = 11.880.000 => 12 Milhões por ano	-	-
3	Unidade	Módulo de análise de segurança	Unidade 3	Software	118	578 vpcu / 8 = 73 pack 8 vcpu	2219 Gb mem / 16 Gb mem = 139 pack 16 GB mem
4	Unidade	Módulo de análise de log	Unidade 4	Software	103.680 Gb * 1000 = 103,.680.000	-	-

Item	Unidade de Medida	Descrição do Item	Métrica	Tipo de Software /Serviço/ Produto	Hosts	8vcpu	4GB mem
					GB => 104 TB por ano		
5	Unidade	Serviços de Implantação	UNITÁRIO	Serviços de Suporte a Implantação	01		
6	Unidade	Serviços de Capacitação	Por turma	Serviço de Capacitação	01		
7	Unidade	Serviços Especializados de Operação Assistida e Análise Contínua, sob demanda	Hora de Serviço Técnico (HST)	Serviço de Operação Assistida e Análise de Dados e Anomalias	8 horas * 12 sistemas * 24 meses = 2304 horas		

ANEXO III – PROVA DE BANCADA (FACULTATIVO)

LICITANTE:_____

SOLUÇÃO OFERTADA: _____

FABRICANTE: _____

DATA DE INICIO: ____ /____ /_____ DATA DE TERMINO: ____ /____ /_____

RESULTADO DA AVALIAÇÃO: ( ) HABILITADO ( ) INABILITADO

PARTICIPANTES:

NOME COMPLETO	DOCUMENTO	RÚBRICA

PROVA DE BACADA PARA OS ITENS DE REQUISITOS TÉCNICOS:

REQUISITOS TÉCNICOS	ATENDIMENTO			CONTRATANTE	
ITENS SOLICITADOS	INTEGRAL (I)	PARCIAL (p)	NÃO (N)	CONFIRMAÇÃO (S)	CONFIRMAÇÃO (N)

TOTAL DE ATENDIDOS					

REQUISITOS TÉCNICOS:

1	**Módulo de análise de aplicações (Item 3.2.1)**	ATENDIDO ? (I / P / N)	CONFIRMAÇÃO CONTRATANTE ? (S / N)
1.1	• O módulo/solução deve permitir ser implantada na modalidade SaaS, a CONTRATADA deverá disponibilizar os recursos de computação em provedor que possua ao menos as certificações: ABNT NBR ISO/IEC 27001:2013;ISO/IEC 27017:2015; e ISO/IEC 27018:2019, com validade vigente durante a execução do contrato, referentes à infraestrutura hospedada em datacenter no Brasil;		
1.2	• Ser oferecida com interface de operação e administração, exclusivamente WEB, com compatibilidade com os seguintes navegadores: Microsoft Edge, Mozilla Firefox ou Google Chrome;		
1.3	• O módulo deve permitir a visualização de erros de processo e exceções de negócios em cada etapa;		
1.4	• O módulo deverá possibilitar a criação e desenvolvimento de novos aplicativos customizados na plataforma, para atender casos de uso específicos, aproveitando os dados de observabilidade;		
1.5	• O módulo deverá possuir documentação do fabricante para auxílio do desenvolvimento dos novos aplicativos;		
1.6	• Através de um agente unificado instalado em cada servidor, deverá descobrir automaticamente todas as tecnologias, processos, serviços e aplicações, e suas respectivas dependências e relacionamentos de forma dinâmica e contínua, não necessitando configuração prévia e parametrização manual;		
1.7	• O módulo deve monitorar as aplicações dinamicamente, utilizando tecnologia de bytecode instrumentation, de forma automática e sem a necessidade de intervenção manual nos arquivos de configuração e arquivos fontes das aplicações, incluindo arquivos JS;		
1.8	• Deve haver criptografia nativa do módulo para a comunicação ponto a ponto entre todos os componentes/módulos do módulo;		
1.9	• A interface de administração e operação do módulo deve ser 100% WEB (sem demandar instalação de clientes em estações);		

1.10	• Monitorar automaticamente aplicações baseadas em arquitetura de micro serviços, como [nome do módulo de containers e administradores de containers se houver], não necessitando configuração prévia de arquivo de configuração e definição de regras, devendo monitorar os processos que estão ocorrendo em cada host;		
1.11	• Realizar injeção automática do agente em contêineres (glibc ou musl-libc) em CONTAINERD (https://containerd.io/);		
1.12	• Deverá ser possível de forma automática monitorar clusteres em Kubernetes/Openshift, sem alteração de código e parametrização prévia de scripts de configuração para que a monitoração ocorra;		
1.13	• Deverá de forma automatizada injetar/configurar agentes nos containers Docker, containerd e CRIO, sem a necessidade de qualquer atividade de configuração de script do coletor, alteração da imagem, bastando apenas a instalação do agente no servidor onde os containers são excetuados;		
1.14	• Permitir o monitoramento dos componentes do cluster [nome da Tecnologia do container] para orquestração de contêineres, sendo possível obter métricas sobre os servidores, processos de gerenciamento, utilização de recursos computacionais (CPU, memória, rede e armazenamento);		
1.15	• Realizar o auto-discovery do cluster, garantindo a continuidade e escalabilidade automática, para que mesmo em caso de mudanças ou adições de novos elementos na arquitetura, a monitoração ocorra;		
1.16	• O módulo deverá fornecer Dashboards pré-construídos e oferecer um editor que permita a criação e customização de dashboards, painéis personalizados permitindo a inclusão de imagens, labels, e permitindo também a configuração da navegação em fluxo, Drill Downs customizados entre dashboards e entidades;		
1.17	• Os dashboards deverão permitir a extração de dados da integridade operacional, desempenho do aplicativo, infraestrutura e dados relevantes de negócios;		
1.18	• O módulo deverá prover suporte a autenticação em OpenLDAP, Microsoft Active Directory e SAML;		
1.19	• Prover mecanismos de atualização de versão e/ou distribuição do produto durante toda a vigência do Contrato. O processo de atualização deve ocorrer de forma nativa e totalmente automático sem a necessidade de qualquer configuração manual, de apoio de ferramentas terceiras e de scripts automatizados;		

1.20	• O módulo deverá possuir ferramenta para automação de tarefas a partir de condições especificadas para execução de fluxos de trabalho criados;		
1.21	• O módulo deverá possibilitar a criação e configuração da automação a partir de uma interface gráfica amigável com drag-and-drop;		
1.22	• Deverá possibilitar a execução de tarefas a partir de gatilhos ou cronogramas para execuções de ações que integrem com outros sistemas;		
1.23	• Deve possuir templates prontos para enviar notificações ou criar tickets;		
1.24	• Permitir a trilha de auditoria de cada tarefa executada;		
1.25	• O módulo deve permitir o envio de requisições HTTP a APIs públicas na internet ou para APIs privadas dentro da infraestrutura do cliente;		
1.26	• No caso de APIS privadas O módulo deve permitir o envio de requisições sem a necessidade de abrir as APIs privadas para a Internet;		
1.27	• O módulo deve oferecer suporte à configuração como código por meio de um provedor Terraform ou similar;		
1.28	• O módulo deve oferecer um mecanismo nativo de configuração como código;		
1.29	• Indicar e sugerir a instalação dos agentes em novos servidores que ainda não estão com monitoração instalada, nos casos em que alguma tecnologia, processo, serviço ou aplicação se comunicar com o novo servidor a partir de um servidor com monitoração ativa;		
1.30	• O módulo deve oferecer endpoints de API para gestão de configuração da própria plataforma;		
1.31	• O módulo poderá contar com comunicação externa do próprio fabricante desde que a comunicação seja totalmente segura e criptografada;		
1.32	• Fornecer o nível de disponibilidade do servidor, bem como eventos, problemas e erros ocorridos;		
1.33	• Apresentar visibilidade fim-a-fim, investigando os diversos estágios das aplicações sem a necessidade de instalação de agentes adicionais que não componham O módulo ofertada;		
1.34	• Para servidores físicos e virtuais, apresentar automaticamente, no mínimo, as seguintes métricas de performance e disponibilidade: CPU, memória, disco, rede;		

1.35	• Permitir a integração com sistemas de virtualização VMware. Com esta integração, o Módulo deverá realizar a performance digital e apresentar ao menos as seguintes métricas: número de servidores criados por dia, número de servidores baixados por dia, número de Vmotion por dia;		
1.36	• Permitir a integração nativa com ambiente de virtualização VMWare e monitorar, no mínimo, as seguintes métricas: número de cluster, número de servidores físicos e virtuais, situação dos servidores físicos e virtuais (exemplo: ativo, suspenso);		
1.37	• Realizar a verificação automática de performance e disponibilidade da comunicação dos processos, coletando e exibindo, no mínimo, as informações de tráfego de entrada e saída, disponibilidade, taxa de transmissão e retransmissão, erros e perdas de pacotes, falhas tcp e round trip time;		
1.38	• Indicar, para as tecnologias descobertas, no mínimo, as informações de uso de CPU, consumo de memória, taxa de transmissão e disponibilidade ao longo do tempo;		
1.39	• Descobrir automaticamente e dinamicamente a topologia da aplicação alvo, contendo a comunicação entre seus componentes e apresentando um mapa completo da aplicação e suas dependências;		
1.40	• A descoberta deverá ser realizada de forma automática e constante, atualizando dinamicamente sem a necessidade de qualquer configuração manual, e de apoio de ferramentas terceiras e de scripts automatizados;		
1.41	• A descoberta automática deverá suportar, no mínimo, os seguintes elementos: HTTP/HTTPS, Web Services, banco de dados, serviços de mensageria, Hosts da VMware, máquina física ou virtual, chamada a serviço externo de terceiros ou servidor remoto;		
1.42	• A nuvem pública será responsável pelo provimento da infraestrutura de TI necessária para o funcionamento do módulo, como servidores (hosts), armazenamento de dados, programas de software básico (ex: sistema operacional, banco de dados, servidor de aplicação/web, etc) e pela sua gestão/manutenção (ex: atualização de versão, aplicação de correções de segurança, backup de dados, etc);		
1.43	• O módulo deverá indicar a quantidade de componentes de tecnologia descobertos por categoria (exemplo: hosts, processos, serviços, aplicações) indicando, inclusive, quantidade de componentes afetados por um problema em tempo real;		

1.44	• Para os componentes de tecnologia descobertos, deverá ser monitorado o volume de chamadas/requisições, tempo de resposta e taxa de falhas;		
1.45	• A monitoração das aplicações deverá ser iniciada de forma automática, junto com a inicialização do respectivo servidor de aplicação;		
1.46	• Acompanhar a performance do ambiente, verificando a utilização de CPU por processo. Para cada processo instrumentado, deverá ser possível identificar o código-fonte, no nível de métodos dos processos que mais consomem CPU;		
1.47	• Permitir a verificação do consumo de CPU dos processos instrumentados e efeito do Garbage Collector, tais como número de execuções e percentual de suspensão do thread;		
1.48	• O módulo deverá identificar todas as classes e métodos com maior consumo do tempo de execução visando a otimização do código;		
1.49	• O módulo deverá, para cada serviço, indicar as aplicações que consomem o serviço específico, bem como os bancos de dados acessados e os respectivos comandos SQL executados pelo serviço analisado;		
1.50	• O módulo deverá automaticamente e dinamicamente identificar os serviços. E apontar as requisições mais lentas, que estão consumindo mais recursos e possuem taxa de falha mais alta;		
1.51	• Realizar a verificação da performance e disponibilidade dos principais serviços de terceiros acessados na Internet;		
1.52	• O módulo deverá, para cada serviço, indicar, de forma gráfica, fluxo das requisições que chamam e que são chamadas pelo serviço em análise;		
1.53	• Plataforma AIOps (Artificial Intelligence for IT Operations) que permita gerenciar ambiente de modo proativo, identificando rapidamente indisponibilidades, com detalhamento que facilite inclusive as tomadas de decisões não só relacionadas à manutenção corretiva, mas até para melhorias nos serviços;		

1.54	• O módulo deve determinar de forma automática (aprender automaticamente) e sem configuração prévia os limites e baselines (dados de referência) de métricas-chave, inclusive de negócio, de funcionamento normal das aplicações para geração de alertas de anomalias (desvios de comportamento com algoritmos que permitam detecção de anomalias) e identificar de forma automática possíveis impactos levando em consideração a topologia da aplicação. Por exemplo: uma transação no front-end está lenta porque o serviço de banco está com a taxa de falha elevada;		
1.55	• O módulo deve ser capaz de analisar e apresentar os relacionamentos existentes entre os componentes, não somente de forma vertical, mas horizontal e baseado em topologia, de forma a apontar a causa raiz dos problemas;		
1.56	• Deverá identificar os problemas que estão ocorrendo no ambiente, analisando automaticamente os incidentes e relacionamentos entre todos os componentes, de forma a apontar os problemas agrupados, separando causa e efeito, de forma automática com uso de inteligência artificial, em tempo real e mantendo o histórico dos problemas ocorridos;		
1.57	• O módulo deve identificar, de forma automática e com uso de inteligência artificial, a causa raiz dos problemas nas aplicações monitoradas, de forma contextualizada, em tempo real e classificando a natureza, apontando o número de aplicações, usuários, chamadas, serviços, SLOs impactados e componentes de infraestrutura afetados;		
1.58	• O módulo deverá fornecer mecanismos para acompanhar os indicadores de uma aplicação a cada release, visando garantir que uma nova release tenha os seus SLOs e objetivos de capacidade atendidos. Deve permitir automatizar essa verificação, podendo inclusive ser integrada a um pipeline, para impedir o seu avanço em caso de violação desses indicadores;		
1.59	• Deve permitir que os usuários possam comparar a validação de confiabilidade com objetivos de nível de serviço, de uma versão de release do passado ou de uma release progressiva.		
1.60	• O módulo deve permitir fazer a predição e forecast para qualquer métrica presente na plataforma usando o seu motor de inteligência artificial;		
1.61	• Deve ser possível gerar análises de predição sob demanda e inclusive gerar alertas baseados nos resultados dessa predição;		

1.62	• O módulo deve prover observabilidade para desenvolvedores permitindo que os desenvolvedores possam fazer o debug de aplicações Java "ao vivo" em ambiente produtivo sem impactar a aplicação e sem qualquer impacto aos usuários das aplicações. O Debug deve permitir a visualização da execução linha a linha assim como as propriedades da linha de código;		
1.63	• O debug "ao vivo" não deve enviar qualquer parte do código fonte da aplicação para os servidores do módulo, evitando assim qualquer vazamento de informações sigilosas;		
1.64	• Compatibilidade com o ambiente atual do IPLAN RIO para o monitoramento de performance de aplicações, serviços, infraestrutura e experiência digital dos usuários;		
1.65	• O debug "ao vivo" deve permitir que dados sensíveis (CPF, Número de cartão de crédito, etc…) sejam imediatamente mascarados permitindo o debug pelos desenvolvedores sem a exposição de quaisquer dados que comprometam a privacidade dos usuários da aplicação;		
1.66	• Deduplicação - quando múltiplos eventos repetitivos são recebidos para o mesmo incidente de um mesmo elemento de infraestrutura, devendo registrar o evento apenas uma vez;		
1.67	• Correlação automática baseada em topologia - suprimir os eventos gerados a partir de elementos relacionados entre si, onde um destes elementos é o causador do incidente, sem necessidade prévia de criação de regras;		
1.68	• Deverá executar ações resultantes da deflagração de um alerta, suportando, no mínimo: envio de e-mail, integração com Jira ou Webhook;		
1.69	• O módulo deve suportar a coleta de dados de forma simples e sem a necessidade de escrever scripts para as seguintes tecnologias: WMI, SNMP, JMX, Prometheus, SQL		
1.70	• O módulo deve suportar a coleta de dados através de criações de scripts em Python;		
1.71	• Disponibilizar informações a respeito de problemas que afetam uma aplicação, permitindo o detalhamento do problema;		
1.72	• Deverá monitorar aplicações heterogêneas, hospedadas em ambiente próprio de Datacenter do IPLAN RIO.		

1.73	• Para os problemas identificados no ambiente monitorado, O módulo deverá apontar o número de serviços, aplicações e componentes de infraestrutura afetados pelo problema. Além disso, deverá indicar o número de usuários reais Das aplicações que foram afetados;		
1.74	• Para os problemas identificados de forma automática e inteligente, identificar além do impacto do problema, também a sua causa raiz;		
1.75	• Disponibilizar na página do problema mecanismo de gravação do comportamento e evolução do problema demonstrando visualmente todos os componentes de tecnologia afetados durante a vigência do problema, bem como os relacionamentos entre eles. O módulo deverá indicar os tempos e momentos em que ocorrem os eventos, bem como os serviços impactos ao longo do tempo;		
1.76	• Apresentar o nível de disponibilidade do servidor, bem como eventos, problemas e erros ocorridos.		
1.77	• Disponibilizar visão fim-a-fim das transações, investigando os diversos estágios das aplicações sem a necessidade de instalação de agentes adicionais que não componham o módulo ofertada;		
1.78	• Descobrir automaticamente transações de negócio (ações resultantes da interação com usuários ou sistemas) tanto no FrontEnd quanto Backend;		
1.79	• Detectar transações de negócio de forma automática, iniciadas, no mínimo, com base nos seguintes protocolos/tecnologias: HTTP/HTTPS e web services;		
1.80	• Permitir monitorar as execuções das requisições de backend, contendo minimamente as seguintes métricas: quantidade de execuções da transação, tempos de resposta e volume de erros, com drilldown detalhado do código executado (classes e métodos) nas transações executadas nos servidores de aplicação;		
1.81	• Classificar e quantificar a execução das requisições de acordo com seu tempo de resposta e eventuais erros, de forma a possibilitar ao usuário/analista a identificação de desvio de comportamento na linha do tempo (exemplo: Tempo de Resposta, Taxa de Falha e Throughput);		
1.82	• Disponibilizar informações a respeito de eventos ocorridos na aplicação, como restart ou deploy, permitindo o correlacionamento de problemas com um possível problema de deploy;		

1.83	• Deverá monitorar soluções compostas por aplicações construídas com diversidade de plataformas tecnológicas, versões e distribuições providas por fornecedores de marcas variadas, tanto de hardware quanto de software;		
1.84	• Identificar requisições com baixa performance, lentas, sem intervenção manual;		
1.85	• Identificar queries SQL com baixa performance ou lentas, sem intervenção manual;		
1.86	• Identificar sistemas de backend ou serviços externos lentos ou indisponíveis, sem intervenção manual;		
1.87	• Apresentar detalhamento de tempos de execução em nível de classe, método e comandos SQL, por meio do baseline dinâmico;		
1.88	• Realizar a verificação da performance das chamadas à banco de dados feita pelas aplicações, não necessitando realizar a instalação de agentes no servidor de banco de dados;		
1.89	• Exibir, para as conexões com o banco de dados, a taxa de falhas, tempo de resposta médio e quantidade de requisições por período de tempo;		
1.90	• Exibir a listagem das consultas mais lentas aos bancos de dados;		
1.91	• O módulo deve monitorar as instruções SQL e apresentar a quantidade de execuções, taxa de falhas e o tempo médio de resposta para as transações com erro ou problemas de performance;		
1.92	• Para as consultas a banco de dados, disponibilizar gráfico da distribuição dos tempos de resposta pela quantidade de ocorrências, permitindo assim que seja possível identificar os tempos de resposta que mais ocorrem durante a análise;		
1.93	• Para os comandos de banco de dados, indicar os comandos mais executados (exemplo: alteração, consulta), indicando a quantidade na unidade de tempo e o tempo médio de resposta, bem como detalhando os comandos;		
1.94	• Deverá permitir flexibilidade no licenciamento dos agentes independente de tecnologia e/ou linguagem das aplicações, possibilitando a reutilização de uma licença em diferentes tecnologias e/ou aplicações, respeitado o limite contratado;		
1.95	• A partir de um comando de banco de dados, permitir rastrear a aplicação e serviços que o executou, seja em Java ou .NET;		
1.96	• Possuir mecanismos de visualização de dados históricos sem a necessidade de leitura de arquivos externos à solução;		

1.97	• O processamento de dados para consolidação da base, assim como para geração de relatórios e consultas, não deverá ocorrer nos servidores monitorados e sim na plataforma de gerenciamento específico da CONTRATADA;		
1.98	• Possuir controle de acesso, permitindo criar e modificar grupos de perfis de acesso;		
1.99	• Permitir ao administrador do módulo habilitar ou desabilitar a verificação da performance do ambiente monitorado;		
1.100	• Permitir o monitoramento de quantidade de chamadas e tempo de resposta de API REST providas pelas aplicações;		
1.101	• O módulo deverá possuir mecanismo de particionamento de informações, permitindo a visualização separada da topologia e conjunto de entidades monitoradas ou dados dimensionais (como logs e métricas) em um ambiente. Deve ser possível realizar filtros por grupos específicos de monitoramento e visualização separada dos problemas de cada grupo, assim como controle de acesso às informações;		
1.102	• Apresentar visão gráfica (mapas ou representação gráfica equivalente) do ambiente ou aplicação monitorada, contendo no mínimo:		
1.103	• Visão gráfica pré-definida para as principais métricas e análises disponibilizadas pelo módulo. Deverá permitir a criação e customização de painéis, gráficos ou mapas com a inclusão ou retiradas de informações disponibilizadas pelo módulo;		
1.104	• Visão gráfica da análise da performance da aplicação identificando os serviços e infraestrutura utilizada pela aplicação, bem como informações a respeito dos acessos de origem das transações, como navegador e visão geográfica dos acessos;		
1.105	• Não serão aceitas soluções que demandem uso de espelhamento/mirror/span de dados de rede;		
1.106	• Visão gráfica apresentando as informações da aplicação em períodos históricos e permitindo filtros na escala e período de tempo (por exemplo: tempo real, ontem, últimos 7 dias, últimos 15 dias e últimos 30 dias);		
1.107	• Visão gráfica apresentando o volume de execuções e tempos médio de resposta entre todos os componentes da aplicação de acordo com a escala e período de tempo selecionado;		

1.108	• O módulo deverá permitir configurar e monitorar objetivos de nível de serviços (SLOs) utilizando indicadores de diferentes dimensões da aplicação, como serviços, experiência de usuário e taxa de falhas;		
1.109	• O módulo deverá permitir a realização de análise de negócio, com a capacidade de conectar informações de desempenho da aplicação alvo e a experiência do usuário à métricas de negócio;		
1.110	• O módulo deve possibilitar a monitoração de indicadores de desempenho (KPI) de negócio, detectando anomalias nas transações e permitindo análise para fundamentar melhores decisões;		
1.111	• O módulo deverá permitir a criação de relatórios analíticos derivados de métricas da experiência de usuário e transações com o objetivo de obter insights de negócio;		
1.112	• O módulo deve permitir análise avançada de condições de negócio, permitindo acompanhar eventos relevantes para o negócio diretamente na plataforma. A coleta de eventos de negócio deve ser possível das seguintes formas: diretamente no agente que monitora as aplicações, através da monitoração da experiência do usuário, envio de eventos através de API dedicada, a partir dos logs ingeridos pelas plataformas;		
1.113	• O módulo deve permitir reportar KPIs de processos de negócios, incluindo fluxos concluídos (conversões), tempo médio de conclusão de fluxos, exceções de negócios e KPI de negócios específicos;		
1.114	• O módulo deve permitir, para os eventos de negócio já armazenados na plataforma a criação, visualização e análise de fluxos de processos de negócio do início ao fim;		
1.115	• O módulo deve permitir a detecção e exploração de fluxos de processos de negócio incompletos ou interrompidos para determinar a causa, como um erro de TI, uma exceção de negócios ou tempo de trânsito anormal entre etapas.		
2	**Módulo de análise de usuários (Item 3.2.2)**	**ATENDIDO ? (I / P / N)**	**CONFIRMAÇÃO CONTRATANTE ? (S / N)**
2.1	• Deverá permitir o acompanhamento da experiência do usuário final no acesso às aplicações corporativas hospedadas no ambiente do DataCenter;		

2.2	• O módulo deve ser capaz de monitorar a experiência de usuários finais da aplicação, através de um código JavaScript injetado no front-end da aplicação de maneira automática e sem esforço de configuração via interface, ou alteração de arquivo ou alteração de código da aplicação (ou arquivos de configuração, mesmo que arquivos JS), a ser executado no ambiente/navegador do usuário final. Não será permitido alterações nos servidores HTTP e inserções manuais de URLs;		
2.3	• Deverá permitir a configuração de capturas de informações a partir de pelo menos Meta Tag, componentes CSS e JavaScript Variables, na página executada no navegador do usuário. O objetivo identificar o usuário logado ou enriquecer as transações de negócio. Não será permitido a alteração de código para captura de informações;		
2.4	• O módulo deverá permitir a consulta (querys) de informações capturadas no monitoramento da experiência do usuário, podendo ser visualizadas em dashboards e utilizá-las como métricas de negócio;		
2.5	• Deverá realizar a monitoração fim-a-fim das aplicações hospedadas no DataCenter, registrando e avaliando, no mínimo a requisição feita pelo usuário no navegador (click e carregamento de páginas ou ação do usuário na aplicação, gerando tráfego no servidor), para: - A execução do código nos servidores de aplicação.; - As consultas aos servidores de banco de dados.; - O retorno do resultado ao navegador do usuário.; - Tempo de execução total da sessão/visita.; - Tempo gasto em rede.; - Tempo de servidor (execução transacional da aplicação).; - Tempo de download do HTML e outros recursos da página.; - Tempo de renderização do browser (DOM Build);; - Tempo de pós-load;.		
2.6	○ Identificar webservices e chamadas a serviços externos das transações de uma aplicação.		
2.7	• Disponibilizar informações a respeito das principais ações de usuário nas aplicações, indicando o total de ações executadas por período de tempo, exibindo informações a respeito do tempo de contribuição das ações, considerando ao menos, tempo de rede e tempo de servidor;		
2.8	• Para os erros de JavaScript identificados nas aplicações, apresentar ao menos as seguintes informações: sistema operacional utilizado, navegador, localidade e ação que gerou o erro. Para cada tipo de informação, O módulo deverá indicar a quantidade de erros ocorrida, por categoria.		

2.9	• Verificar se uma transação ou requisição WEB (exemplo: HTTP ou HTTPS) foi atendida do ponto de vista do usuário final, identificando a satisfação do usuário segundo a métrica APDEX (www.apdex.org). Não será permitido a utilização de própria métrica para identificar a satisfação do usuário;		
2.10	• Possuir forte integração com a análise de causa raiz, permitindo conectar imediatamente um problema na experiência do usuário com o componente da aplicação ou da infraestrutura, que está causando a degradação (exemplo: comando SQL, chamada WebServices .Net);		
2.11	• Realizar a verificação da performance das ações dos usuários exibindo, no mínimo, na linha do tempo, a quantidade de ações, a duração das ações e situação das ações (exemplo: sucesso, erro);		
2.12	• Monitorar a experiência do usuário em página web, virtual pages, iFrames e chamadas AJAX;		
2.13	• Para cada ação de usuário nas aplicações, apresentar ao menos as seguintes informações: falhas/sucesso, origem geográfica das ações, navegador de origem e duração média da ação, distribuição da quantidade de ações por duração e chamadas a serviços de terceiros por períodos históricos;		
2.14	• Disponibilizar informações a respeito das principais ações de usuário nas aplicações, indicando o total de ações executadas por período, exibindo informações a respeito do tempo de contribuição das ações, considerando ao menos tempo de rede e tempo de servidor;		
2.15	• Permitir a criação e definição customizada de localidade a partir de um range de endereços IP, permitindo assim que o administrador crie suas próprias regiões para melhor visualizar as informações de performance, volumetria e falhas por regiões;		
2.16	• O módulo de experiência de usuário deve permitir a configuração de capturas de dados na página executada no navegador do usuário de forma anonimizada, com objetivo de reproduzir a sessão do usuário a partir da captura de eventos do navegador que permitam a visualização em formato de vídeo do ponto de vista do usuário a navegação realizada. Estas visualizações devem estar disponíveis para reprodução por, no mínimo, 30 dias após a sua realização;		
2.17	• O módulo de reprodução de sessão do usuário deve vir com mascaramento de informações sensíveis do usuário por padrão e também permitir a configuração customizada deste mecanismo de privacidade de dados, permitindo, a nível de permissões de perfis de analistas, visualizar ou não as informações sensíveis;		

2.18	• O módulo de observabilidade deverá prover funcionalidades para monitoramento sintético (synthetic monitoring), isto é, permitir agendamento de requisições periódicas a páginas web como se o acesso fosse realizado a partir de um navegador de internet (browser) a determinados endereços web (URL);		
2.19	• O monitoramento sintético deverá conseguir simular uma transação (sequência de ações/passos) como fosse realizada por um usuário real utilizando um navegador de internet (browser). Nenhuma codificação deverá ser feita para provimento da funcionalidade;		
2.20	• Deve ser possível utilizar um "recorder" para gravar todos os passos da navegação, integrados com os principais navegadores utilizados pelos usuários reais;		
2.21	• O módulo deverá permitir que seja contemplado no script de gravação ações reais dos usuários, simulando, de fato, o acesso que o usuário faz ao acessar o serviço digital;		
2.22	• A simulação do acesso ao serviço digital, conforme definição e script gravado, sendo executado a partir da Internet (fora das dependências do IPLAN RIO). Dessa forma, será uma visão mais real do usuário dos serviços digitais;		
2.23	• A possibilidade de executar estas simulações a cada 5 (cinco) minutos (no mínimo) e de ao menos 3 (três) origens distintas;		
2.24	• O módulo deverá coletar os dados de tempo de cada atividade simulada, exibindo estes dados ao longo do tempo;		
2.25	• O módulo deverá permitir a realização de testes sintéticos para mensurar a disponibilidade da rede, utilizando testes ICMP, TCP e DNS;		
3	**Módulo de análise de segurança (Item 3.2.3)**	**ATENDIDO ? (I / P / N)**	**CONFIRMAÇÃO CONTRATANTE ? (S / N)**
3.1	• Permitir a detecção automática e em tempo real de vulnerabilidades nas aplicações sem a necessidade de configuração prévia de escaneamentos periódicos;		
3.2	• O monitoramento de vulnerabilidades não deverá exigir agente adicional para coleta de dados, deverá utilizar o mesmo agente unificado solicitado nos requisitos funcionais para ambas as soluções;		
3.3	• Descobrir automaticamente os problemas de segurança no ambiente e fornecer avaliações de risco automatizadas e contextualizadas;		

3.4	• Identificar vulnerabilidades que precisam de investigação imediatamente;		
3.5	• Usar Inteligência Artificial para gerar automaticamente uma pontuação de risco exclusiva para cada vulnerabilidade potencial reclassificando a nota com base na topologia em tempo real e na análise de vetores de transações;		
3.6	• Permitir detectar, visualizar, analisar e monitorar vulnerabilidades de terceiros em ambientes de produção e não produção em tempo de execução para as tecnologias a seguir: Java, .NET, PHP, Node.js e GO, Kubernetes		
3.7	• Fornecer uma visão geral dos problemas de segurança atuais no ambiente monitorado;		
3.8	• Exibir o número de problemas de segurança abertos atualmente no ambiente monitorado;		
3.9	• Exibir o número máximo de problemas de segurança no ambiente monitorado que foram abertos todos os dias nos últimos 30 dias, classificados por nível de risco;		
3.10	• Listar todas as vulnerabilidades detectadas no ambiente monitorado;		
3.11	• Pontuar as vulnerabilidades de acordo com o nível de riscos (Crítico, Alta, Médio, Baixo e Nenhum);		
3.12	• Listar a situação de cada vulnerabilidade: Aberta, resolvida, aberta e silenciada pelo operador e resolvida e silenciada);		
3.13	• O módulo deverá monitorar as vulnerabilidades de código aberto permitindo a detecção automática de ataques a partir do código vulnerável;		
3.14	• A detecção deverá ocorrer para os ataques via SQL, JNDI e injeção de comando para à linguagem JAVA;		
3.15	• A detecção deverá permitir a configuração do bloqueio e lista de permissão para os ataques;		
3.16	• O módulo deverá mapear, para cada ataque: endereço de origem, processo vulnerável, vulnerabilidade de código que permitiu o ataque, detalhamento do ponto de entrada e o alvo;		
3.17	• O módulo deverá correlacionar automaticamente os logs com os ataques ocorridos para facilitar a investigação;		
4	**Módulo de análise de log (Item 3.2.4)**	**ATENDIDO ? (I / P / N)**	**CONFIRMAÇÃO CONTRATANTE ? (S / N)**

4.1	• O módulo deve, para os dados de observabilidade e segurança, realizar o armazenamento de forma unificada, permitindo consultas aos dados e com gestão na interface da plataforma;		
4.2	• O módulo deve possuir uma única interface que permita consultas de vários tipos de dados e múltiplas formas de visualização dos resultados;		
4.3	• O módulo não deverá exigir reidratação de dados, independentemente do tempo;		
4.4	• O módulo deve gerenciar eficientemente o armazenamento de dados sem a necessidade de configurações de armazenamento quente/frio;		
4.5	• O módulo deve ter escalabilidade nativamente para acomodar o volume de dados crescente e a carga de trabalho;		
4.6	• O módulo deve possuir a capacidade de realizar análises na leitura para dados históricos armazenados com até 10 anos de retenção;		
4.7	• O módulo deve atender aos requisitos padrão de segurança e conformidade, incluindo criptografia de dados, controles de acesso e auditoria;		
4.8	• O módulo deve ser capaz de analisar os logs das aplicações, serviços e infraestrutura permitindo criar regras de notificação baseado na ocorrência de palavras ou grupos de palavras existentes nos logs;		
4.9	• O módulo O módulo deverá permitir explorar, consultar, combinar e processar todos os dados de logs armazenados na plataforma;		
4.10	• O módulo deverá permitir realização de buscas textuais simples e avançadas utilizando linguagem própria do fabricante;		
4.11	• O módulo deverá possuir funcionalidade de exclusão de dados (Hard Delete) em nível de registro, sem a possibilidade de recuperação, para cumprir com mais eficiência as solicitações de exclusão do usuário final, em linha com a lei de proteção de dados;		
4.12	• O módulo deverá possibilitar a conversão de registros de log em eventos de negócio;		
4.13	• O módulo deve permitir criar pipelines de dados possibilitando a criação de métricas, processamento de dados e extração de dados em eventos de negócio;		
4.14	• O módulo deverá permitir configurar endpoints customizados para a ingestão de dados;		
4.15	• O módulo deverá permitir criar rotas dinâmicas para os dados ingeridos com base em condições específicas;		

4.16	• O módulo deverá permitir o isolamento lógico dos dados com o objetivo de controlar o acesso e o tempo de retenção. Essa separação lógica deve ser configurável e permitir que as regras sejam aplicadas no momento da ingestão dos dados para atender essa separação lógica;		
4.17	• O módulo deverá permitir a ingestão de logs por meio do protocolo syslog;		
4.18	• O módulo deverá contextualizar e enriquecer os dados de syslog automaticamente, com atributos específicos do servidor.		