



SUPERIOR TRIBUNAL DE JUSTIÇA
SAFS - Quadra 6 - Lote 1 - CEP 70095-900 - Brasília - DF

ESTUDOS TÉCNICOS PRELIMINARES - ETP

1. Informações Gerais
1.1 N. do Processo SEI: 022004/2024
1.2 Unidade Requisitante: Coordenadoria de Infraestrutura - CIEP
1.3 Unidade Técnica: Seção de Plataforma - SEPLA
1.4 Houve uma centralização da solicitação de diversas unidades? (X) Não se aplica () A unidade centralizou as solicitações das seguintes unidades:
1.5 Equipe de planejamento da contratação ou servidora/servidor responsável: Integrantes Administrativos a) Tiemi Umebara, matrícula S072847- Coordenadoria de Planejamento e Gestão de Contratos TIC (titular); b) Francisco Carlos Alves Diniz, matrícula: S030575 - Seção de Gestão de Contratações de TIC (suplente). Integrantes Requisitantes a) Eronildes Ribeiro da Silva, matrícula: S025490 - Unidade: Coordenadoria de Infraestrutura (titular); b) Alexandre Rodrigues da Silva, matrícula: S061799 - Unidade: Coordenadoria de Infraestrutura (suplente). Integrantes Técnicos a) Rafael Eduardo Alves de Souza, matrícula: S077938 - Seção de Plataforma (titular); b) Daniel de Souza Vasconcelos, matrícula: S078411 - Seção de Plataforma (titular); c) Valfran Santana de Almeida, matrícula: S060318 - Seção de Sustentação de Sistemas Judiciais (titular); d) Carlos Leonardo Pires, matrícula: S043260 - Seção de Plataforma (suplente).
1.6 Responsável pela aprovação do Estudo Preliminar: Nome: Humberto Fontoura Pradera Secretaria/Assessoria: Secretaria de Tecnologia da Informação e Comunicação - STI
1.7 Responsáveis pela fiscalização e gestão: I. A Seção de Gestão de Contratações de TIC indicará, após a assinatura do contrato, os servidores que serão designados como gestor titular e substituto, e acompanhará a execução do contrato, devendo proceder à orientação, fiscalização e interdição da execução do contrato, se necessário, a fim de garantir o exato cumprimento das condições estabelecidas em contrato. II. Integrantes da Seção de Plataforma e Seção de Sustentação de Sistemas Judiciais serão designados como fiscal técnico titular e substituto, e acompanharão a execução técnica dos serviços, devendo proceder à orientação, acompanhamento e fiscalização da execução do contrato, se necessário, a fim de garantir o exato cumprimento das condições estabelecidas em contrato. III. A Seção de Monitoramento e Planejamento de Contratos de TIC indicará, após a assinatura do contrato, os servidores que serão designados fiscal administrativo titular e suplente. Se houver necessidade de designação de comissão de recebimento definitivo, indicar os servidores que serão designados: (X) A equipe de gestão da contratação contará com servidoras e/ou servidores que atuarão no seu planejamento, uma vez que estes terão melhor conhecimento das regras que serão fiscalizadas. Ademais, a unidade não possui quantidade de servidoras e servidores suficientes para indicar equipes distintas.
2. Necessidade da contratação

2.1 Descrição da Necessidade:

O Superior Tribunal de Justiça (STJ), como instituição fundamental no sistema judiciário brasileiro, é responsável pela gestão de um grande volume de processos, o que requer sistemas ágeis e confiáveis, a exemplo do Justiça WEB. No entanto, o tribunal enfrenta desafios relacionados com a modernização da sua infraestrutura tecnológica, em particular devido à recente migração para uma arquitetura baseada em microsserviços no ambiente Kubernetes.

A expansão da infraestrutura, o aumento da quantidade de microserviços, o uso crescente de ambientes em nuvem e a multiplicidade de camadas tecnológicas são características presentes do nosso ambiente que fazem com que a adoção de um sistema que seja capaz de fornecer funcionalidades além do simples monitoramento e desempenho de aplicações se faz necessário. A partir daí temos uma abordagem mais ampla, com uma visão integrada do comportamento das aplicações em relação a infraestrutura, redes e serviços.

Neste cenário evidencia-se o conceito de observabilidade, que é implementado mediante a evolução das soluções de APM (Application Processing Monitoring). Este conceito oferece um conjunto abrangente de ferramentas que monitoram e correlacionam métricas, logs e rastreamentos distribuídos nas aplicações e em toda a infraestrutura, proporcionando uma visão holística e em tempo real dos sistemas. Neste contexto tem-se ainda aspectos relacionados a segurança da informação e defesa cibernética por meio da identificação precoce de comportamentos anômalos e potenciais incidentes de segurança, como acessos não autorizados, movimentações laterais e tentativas de exploração de vulnerabilidades.

O uso de IAOPs (Inteligência Artificial para Operações de TI) torna-se imprescindível considerando as milhares de informações geradas pelos ambientes que estão cada vez mais complexos. A IOps aplica técnicas de inteligência artificial e machine learning para analisar dados de observabilidade, como métricas, logs e traces, em tempo real, permitindo assim o correlacionamento de eventos, automação de respostas e predição de falhas.

A solução deverá seguir as Diretrizes da Entic-Jud, de dezembro de 2020, Seção II - Da Infraestrutura Tecnológica e Serviços em Nuvem, devendo ser disponibilizada em plataforma de nuvem (cloud) pública, na modalidade SaaS (Software as a Service). Deve também atender a Seção III - Da Transformação Digital, com destaque para IV - Estratégia de monitoramento, como serviço, integrando hardware, software, armazenamento, sistema operacional, banco de dados, comunicação de rede e demais componentes.

Com esta aquisição, pretende-se implementar uma solução de observabilidade que permita detectar de anomalias de forma proativa, resolver incidentes com maior eficiência e otimizar o uso de recursos de forma contínua. Esse redirecionamento estratégico garantirá uma abordagem mais robusta e integrada, alinhada às necessidades atuais de monitoramento em ambientes de TI modernos e complexos.

3. Requisitos da contratação

3.1 Requisitos legais da contratação:

(X) Não há conhecimento de nenhuma legislação que exija critérios especiais para contratação do objeto.

() Aplicação de margem de preferência. Informar a legislação:

(X) Outras legislações afetas ao objeto a ser contratado:

Diretrizes da Entic-Jud, de dezembro de 2020.

3.2 Apresentação de certidão e/ou atestado:

() Não há necessidade de apresentação de certidão e/ou atestado.

(X) Sim. Quais?

- De que a Licitante já forneceu a quantidade de subscrições e prestou serviços de instalação e configuração em ambiente equivalente a 14 (quatorze) subscrições;
- De que já prestou serviços técnicos especializados no quantitativo mínimo de 700 horas de serviços.

Justificativa:

Em função da diversidade tecnológica e a complexidade funcional de cada solução, é vital que o fornecedor demonstre não só ter capacidade de fornecer o objeto, mas também de configurar e prestar os serviços continuados de manutenção dos equipamentos. Por outro lado, o conhecimento técnico de produto de um fabricante é diverso do mesmo produto de outro fabricante, o que pode ser constatado pelas certificações específicas em cada caso.

Considerando o nível de complexidade das necessidades relatadas neste estudo técnico, é imprescindível que a empresa demonstre a capacidade técnica na implementação e implantação de projetos em organizações do porte do STJ. A demanda implica em conhecimentos que vão desde a arquitetura de aplicações, passando pelo ambiente de virtualização, sistemas operacionais e redes.

A funcionalidade e disponibilidade desses objetos requer, além do conhecimento e procedimento técnico operacional, executado internamente com gestão da STI e operação terceirizada, um suporte por especialistas exclusivos das ferramentas, devidamente credenciados pelo fabricante, para soluções de alta complexidade, suporte a problemas não conhecidos, assistência a novas implantações, análise de desempenho, realinhamento e ajustamento de configurações, etc.

3.3 Exigência de garantia contratual:

☒ (X) Sim.

Será exigida a garantia da contratação de que tratam os Arts. 96 e seguintes da Lei nº 14.133/21, no percentual de 5% sobre o valor anual e condições descritas nas cláusulas do contrato. Como terão obrigações futuras durante a vigência contratual, é necessário a garantia contratual para:

- ressarcimento da Administração Pública por prejuízos decorrentes da não execução;
- pagamento das multas devidas à Administração Pública;

A solução a ser contratada apresenta alta complexidade técnica, exigindo do fornecedor:

- Instalação e configuração customizadas, compatíveis com a infraestrutura e as políticas específicas do STJ;
- Prestação contínua de suporte técnico e operacional, além de treinamento e capacitação das equipes internas do STJ;
- Prestação de serviços técnicos que exigem alto nível de especialização técnica na execução dos serviços, integração entre múltiplas equipes e precisão na execução, o que naturalmente eleva o risco de falhas, atrasos ou entrega insatisfatória dos resultados contratados.

A garantia contratual atua, portanto, como mecanismo de mitigação desses riscos, conferindo maior segurança à Administração.

Portanto, diante da alta complexidade técnica, da relevância estratégica do objeto contratual e dos riscos envolvidos em sua implementação e operação, será exigida a garantia da contratação de que tratam os Arts. 96 e seguintes da Lei nº 14.133/21, no percentual de 5% sobre o valor anual e condições descritas nas cláusulas do contrato. Como terão obrigações futuras durante a vigência contratual, é necessário a garantia contratual para:

- ressarcimento da Administração Pública por prejuízos decorrentes da não execução;
- pagamento das multas devidas à Administração Pública;

☐ () Não. **Justificativa:**

3.4 Requisitos de acessibilidade para equipamentos e acessórios de TIC:

☒ (X) Não há requisitos de acessibilidade.

☐ () Sim. Quais?

Justificativa:

3.5 Deslocamento de técnica/o ou disponibilidade em unidade de prestação de serviço local para serviços de manutenção e assistência técnica:

☐ () Não se aplica.

☒ (X) Especificação da garantia exigida e das condições de manutenção e assistência técnica acompanhada da justificativa:

Suporte de configuração, análises de desempenho, estatísticas, orientação na resolução de dúvidas, solução de problemas, parametrização de funcionalidades dos softwares, bem como, o direito de atualização da ferramenta, disponibilização de patches, releases e versões, para correção de erros, evolução do sistema podem ser realizados remotamente;

Os deslocamentos ou não das equipes de suporte ficarão a cargo da contratada, avaliando qual melhor modelo para atender o SLA de atendimento.

3.6 Demais requisitos da contratação:

Necessidade de vistoria:

☒ (X) Sim. **Justificativa:**

Deverão vistoriar a plataforma atualmente instalada, os locais de realização dos serviços, as instalações de infraestrutura, as condições ambientais e demais informações relacionadas com a disponibilidade da solução.

☐ () Não.

Foram avaliadas as diretrizes previstas no art. 11 da [IN STJ/GDG n. 4/2023](#) para a elaboração do ETP:

☒ (X) Sim.

☐ () Não. **Justificativa:**

Será exigida carta de solidariedade da/o fabricante:

☐ () Sim. **Justificativa:**

☒ (X) Não. Mas será exigido comprovação de que a vencedora esteja credenciada junto ao fabricante para contratação com o setor público, tendo em vista que a instalação e a configuração serão realizados pelo fabricante da solução.

Exigência de prova de conceito:

☐ () Sim. **Justificativa:**

☒ (X) Não.

Serão indicadas regras externas de fabricantes, fornecedoras/fornecedores ou prestadoras/prestadores de serviços que possam acarretar alteração unilateral do contrato por parte da contratada:

☐ () Sim. **Justificativa:**

☒ (X) Não.

Foi identificado, na base de dados da Plataforma de Governança Digital Colaborativa do Poder Judiciário (Connect-Jus), objeto similar à contratação pretendida:

(X) Sim. **Discriminar objeto:** Foram encontradas contratações similares de ferramentas de APM/Observabilidade (6043858).

() Não.

Aplicação do Guia de Contratações de TI da [Resolução CNJ n. 468/2022](#):

(X) Sim.

() Não.

Haverá pagamento antecipado?

() Não - REGRA

(X) Sim. **Justificativa:**

As ferramentas de APM avaliadas são comercializadas na forma de subscrições pagas antecipadamente aos fabricantes. O cliente escolhe o prazo entre um e cinco anos, paga o valor da subscrição integral, e terá acesso aos serviços contratados. Quanto maior o prazo, menor será o custo por ano. Os fabricantes comercializam desta forma. Qualquer outra forma de pagamento será mais onerosa pois as licitantes irão repassar os custos de financiamento. Somente as subscrições serão pagas antecipadamente.

3.7 Requisitos de Negócio

A Subscrição da aplicação deverá ser realizada no modelo SAAS (software as a service) para monitorar o desempenho de infraestrutura e de aplicações em nuvem pública do próprio fabricante ou de terceiros.

A capacidade de monitorar as sessões dos usuários das aplicações deverá estar incluída no licenciamento.

Todos os componentes de software, licenças e suporte necessários para utilização da solução, considerando requisitos recomendados pelo fabricante para uma adequada monitoração do ambiente, incluindo os bancos de dados para armazenamento das informações, deverão estar incluídos na solução ofertada;

A solução deve permitir licenciamento flexível de agentes independentemente de tecnologia ou linguagem de aplicação, possibilitando reutilização de licenças entre diferentes tecnologias e aplicações, respeitando os limites contratuais estabelecidos, sem restrições por tipo de componente monitorado.

A empresa contratada deverá prestar o suporte técnico da ferramenta quando de defeitos na prestação do serviço.

3.7.1 Requisitos Gerais

1. A solução deve monitorar as aplicações indicadas, instaladas em ambientes híbridos on-premises e cloud, garantindo visibilidade unificada sobre: desempenho de transações, consumo de recursos, interações com bancos de dados, dependências externas, logs de execução, código-fonte e deploys de novas versões devendo ainda correlacionar automaticamente essas métricas com degradação de serviços, permitindo diagnóstico integral em arquiteturas altamente distribuídas;
2. A solução deve monitorar a experiência do usuário final em nível de frontend, coletando dados de ambiente do cliente, interações com a interface, métricas de desempenho de carregamento de página e requisições HTTP originadas no cliente, garantindo correlação automatizada entre essas ações e as transações correspondentes no backend;
3. A solução deve ser disponibilizada como serviço em nuvem, garantindo alta disponibilidade, escalabilidade elástica sob demanda, acesso remoto seguro via protocolos criptografados e conformidade com padrões de segurança de dados em ambientes multi-tenant, sem prejuízo da capacidade de monitoramento do ambiente descrito;
4. A solução deve disponibilizar interface gráfica web, com mecanismos integrados de autenticação segura e controle de acesso individualizado, permitindo visualização centralizada unificada dos dados monitorados, além de funcionalidades para criação e personalização ágil de dashboards, widgets, gráficos e alertas, garantindo representação contextualizada das métricas essenciais;
5. A solução deve possuir capacidade de descoberta automatizada da arquitetura das aplicações e infraestrutura subjacente, incluindo ambientes físicos, virtualizados e containerizados, com mapeamento dinâmico de dependências e atualização em tempo real da topologia;
6. A solução deve prover gestão proativa do ambiente monitorado, mediante detecção automatizada de anomalias e indisponibilidades, com diagnóstico granular, análise de impacto em cascata disponibilizando insights operacionais e tendências históricas que viabilizem decisões estratégicas para otimização contínua de serviços, planejamento de capacidade e prevenção de degradação futura;
7. A solução deve realizar análise contínua de segurança das aplicações em tempo real, mediante detecção automatizada de vulnerabilidades críticas, considerando a topologia da aplicação e dados recebidos de ferramentas externas de segurança, gerando alertas automatizados contextualizados com os riscos identificados;
8. A solução deve possuir capacidade de criação automática de incidentes em ferramentas ITSM integradas, por meio de métodos nativos ou webhooks, incluindo informações que determinem o problema e seu contexto (ex: causa raiz, componentes afetados), sem dependência de desenvolvimento externo customizado;
9. A solução deve ser capaz de ser integrada em esteiras de CI/CD, detectar automaticamente mudanças de versões e configurações, realizar validação de métricas de desempenho pós-deploy e ser capaz de se integrar nas fases de testes das aplicações e ser utilizada em estratégias de deploy;
10. A solução deve disponibilizar todas as métricas coletadas através de APIs padronizadas, garantindo interoperabilidade com outras ferramentas;
11. Todo processamento de dados para consolidação, análise e geração de relatórios deve ocorrer exclusivamente na plataforma de gerenciamento do provedor em datacenter localizado em território brasileiro, sem utilização de recursos computacionais dos ambientes monitorados.

3.7.2 Monitoramento das Aplicações

1. A solução deve oferecer suporte nativo ao monitoramento de aplicações backends desenvolvidas em linguagens Java, Spring Boot, .NET, PHP, Python, em versões oficialmente suportadas pelos respectivos desenvolvedores das linguagens, mediante instrumentação automatizada sem modificações manuais no código-fonte, manifestos específicos ou reinicialização de serviços, garantindo coleta de métricas sem impacto significativo na operação dos ambientes monitorados e sem a necessidade de agentes adicionais externos à solução ofertada;
2. A solução deve oferecer suporte nativo ao monitoramento de aplicações frontend JavaScript hospedadas no servidor Apache HTTP, mediante instrumentação automatizada sem modificações manuais no código-fonte ou configuração de servidores web, garantindo coleta de métricas de experiência do usuário final;
3. A solução deve identificar o usuário autenticado associado a cada requisição, coletando dados do navegador sem modificação do código-fonte ou

configuração de servidores. Dados sensíveis (ex: credenciais, informações pessoais) devem ser mascarados ou excluídos da coleta, garantindo conformidade com políticas de privacidade;

4. A solução deve coletar e correlacionar todas as requisições de usuários em tempo real, sem amostragem (sampling), rastreando integralmente a jornada desde interações no navegador até operações em bancos de dados;
5. A solução deve coletar e correlacionar todas as transações em tempo real, sem amostragem (sampling), com suporte a transações síncronas, assíncronas, multi-thread e eventos concorrentes em arquiteturas distribuídas, rastreando desde a origem até os componentes finais envolvidos (internos ou externos);
6. A solução deve indicar chamadas oriundas de hosts não monitorados e chamadas enviadas a destinos não monitorados sem perder a capacidade de rastreabilidade e possibilitando que novos agentes sejam instalados para aumentar a cobertura de monitoração;
7. A solução deve permitir classificação hierárquica de transações, métricas e eventos nos níveis: aplicação, serviços (item implantável) e endpoints (URLs específicas), com consolidação estatística por camada;
8. Para cada componente descoberto, a solução deve disponibilizar histórico temporal de disponibilidade (ex: status online/offline) e métricas de desempenho (ex: tempo de resposta, uso de recursos), com visualização em dashboards configuráveis e capacidade de análise em períodos personalizados (ex: últimas 24 horas, 7 dias). Além disso, o período de retenção desse histórico deve atender com métricas precisas de aplicativos, serviços e endpoints mantidas por 1 mês e com subconjunto de chamadas, rastreamentos e métricas aproximadas mantido por 12 meses;
9. A solução deve disponibilizar mapa interativo da topologia de aplicações, representando dependências entre componentes, fluxos de comunicação e status operacional em tempo real;
10. A solução deve mapear transações e requisições com todas as camadas da aplicação (servidores, pods, microsserviços, APIs), correlacionando-as automaticamente com eventos e métricas. Deve permitir navegação hierárquica entre os níveis da aplicação (aplicação > serviço > endpoint) e exploração contextual integrada a logs, traces associadas à transação;
11. A solução deve classificar transações por faixas de tempo de resposta (ex.: <1s, 1-3s, >3s) e gravidade de erros, permitindo análise temporal via linha do tempo interativa com filtros por criticidade;
12. A solução deve prover o mapeamento entre os logs da aplicação com todas as suas camadas (servidores, pods, microsserviços, APIs), correlacionando-as automaticamente com eventos e métricas;
13. A solução deve correlacionar automaticamente as métricas de desempenho dos servidores com todas as camadas da aplicação (pods, microsserviços, APIs), integrando-as a eventos de erro ou degradação para análise contextualizada;
14. A solução deve correlacionar automaticamente as métricas de bancos de dados (incluindo comandos SQL, variáveis de bind e objetos de conexão) com todas as camadas da aplicação e infraestrutura, integrando-as a eventos de erro ou degradação para análise contextualizada;
15. A solução deve identificar e registrar erros de JavaScript em runtime, identificando o contexto de execução (páginas afetadas, navegadores, sistemas operacionais) e correlacioná-las automaticamente com todas as camadas da aplicação (pods, microsserviços, APIs) e calcular métricas quantificando impactos operacionais, número de usuários afetados, frequência de ocorrências e páginas com maior incidência de falhas;
16. A solução deve correlacionar automaticamente componentes de tecnologias distintas (ex: frontend PHP com backend Java e Kafka), garantindo rastreabilidade transacional unificada;
17. A solução deve calcular o índice APDEX (ou outro índice semelhante de satisfação de usuário) para transações web (HTTP/HTTPS), considerando tolerâncias configuráveis de tempo de resposta e impacto de erros na satisfação do usuário final;
18. A solução deve prover funcionalidade nativa para criação e execução de testes sintéticos, validando endpoints web mediante verificações de disponibilidade, integridade de APIs, códigos de status HTTP e interações complexas. Os testes devem ser executados a partir de agentes distribuídos geograficamente, garantindo medição de desempenho e disponibilidade sob perspectivas regionais;
19. A solução deve monitorar e analisar métricas de ativação e execução de Garbage Collection em tempo real, além de outras métricas de performance de threads, pools e uso de memória da JVM;
20. A solução deve monitorar e instrumentar a JVM (Java Virtual Machine) sem a necessidade de reinicialização ou modificação de parâmetros de inicialização;
21. A solução deverá disponibilizar visualização gráfica da distribuição de tempos de resposta, taxa de erros, consumo de recursos, throughput e outras métricas críticas agregadas por aplicação, requisição e componentes de infraestrutura, com capacidade de priorização automática dos padrões mais frequentes, impactantes ou críticos para operação, garantindo correlação contextualizada com eventos de degradação e integração aos painéis de diagnóstico;
22. A solução deve realizar análise contínua de vulnerabilidades em tempo de execução mediante instrumentação automatizada da aplicação, identificando padrões de risco em fluxos reais de dados (parâmetros de entrada/saída, interações externas) e classificando-as conforme critérios de mercado devendo ainda gerar pontuação de risco dinâmica baseada em contexto operacional (topologia, criticidade do componente) para priorização e mitigação de ameaças, considerando ainda dados vindos de ferramentas externas de segurança (ex: SIEM, WAF);
23. A solução deve identificar dependências e vulnerabilidades de softwares de código aberto (OSS) em aplicativos, suas bibliotecas e pacotes de terceiros, gerando classificações de impacto automatizadas, considerando critérios dinâmicos como exposição em produção, criticidade do componente, tráfego afetado e topologia da aplicação;
24. A solução deve correlacionar automaticamente as vulnerabilidades identificadas com todas as camadas da aplicação (microsserviços, APIs, servidores), indicando a localização e o contexto da vulnerabilidade;
25. A solução deve disponibilizar um painel unificado de segurança, apresentando visão consolidada de vulnerabilidades com métricas quantitativas, lista detalhada de itens e a capacidade de filtrar por criticidade ou status;
26. A solução deve aplicar filtros automatizados para dados confidenciais em logs e traces antes do envio à plataforma, utilizando regras pré-configuradas e detecção de padrões sensíveis garantindo conformidade com políticas de privacidade;
27. A solução deve realizar monitorar continuamente logs heterogêneos, analisando de forma inteligente, gerando eventos e alertas contextualizados mediante detecção de padrões;
28. A solução deve monitorar certificados digitais utilizados pela aplicação, identificando validade, renovação e expiração, com geração de alertas proativos para mitigação de riscos de interrupção ou vulnerabilidades relacionadas a certificados inválidos ou comprometidos;
29. A solução deverá ter a capacidade de excluir a instrumentação de todos os componentes/recursos (resources) em determinado namespace através da configuração do nome do namespace em lista de exclusão na configuração do agente ou através de rótulo (label) ou anotação (annotation) no namespace.

3.7.3 Monitoramento da Infraestrutura

1. A solução deve operar sem dependência de técnicas de espelhamento (mirror/span) de tráfego de rede para coleta de dados, utilizando exclusivamente métodos de instrumentação não intrusivos e agentes leves para captura de métricas e transações;
2. A solução deve realizar a descoberta de forma automática de novos hosts que estabeleçam comunicação com componentes já monitorados e coletar, no mínimo, informações de uso de CPU, consumo de memória, taxa de transmissão e disponibilidade, atualizando o inventário de recursos de infraestrutura monitorados com os novos itens;
3. A solução deve monitorar servidores físicos, máquinas virtuais e ambientes Kubernetes associados às aplicações especificadas, coletando eventos, erros e métricas de desempenho em sistemas operacionais Linux e Windows Server, correlacionando-as com as métricas de aplicação em granularidade de até 1 minuto;
4. Uma vez instalado o agente de monitoração padrão da solução, este deve ser utilizado para todas as funcionalidades de coleta (desempenho, segurança, logs), realizando descoberta contínua e automática de tecnologias, processos, serviços e dependências em servidores monitorados, sem necessidade de configuração prévia ou intervenção manual, incluindo identificação de componentes em containers Kubernetes sem rebuild de imagens ou modificação de workloads;
5. A solução deve suportar nativamente a coleta de métricas em ambientes de containerização e orquestração, incluindo serviços Docker (containers, imagens, redes) e Kubernetes (pods, namespaces), sem dependência de agentes extras que já não componham a solução;
6. A solução deve coletar e disponibilizar métricas de desempenho de servidores físicos e virtuais, abrangendo uso de CPU, consumo de memória, atividade de disco, utilização de sistemas de arquivos, estatísticas básicas de rede com granularidade configurável;
7. A solução deve integrar-se a ambientes VMware, monitorando desempenho de hosts, máquinas virtuais e clusters vSphere, com detecção automática de migrações (vMotion), realocação de recursos e eventos de configuração, devendo correlacionar essas métricas com o desempenho das aplicações;
8. A solução deve monitorar o desempenho de interfaces de rede em servidores, coletando métricas de tráfego de entrada/saída, taxa de retransmissão TCP, perda de pacotes e disponibilidade de enlaces, com correlação automática a gargalos em transações distribuídas;
9. A solução deve prover uma forma de integração com a CDN Cloudflare, coletando métricas de desempenho e outros eventos, com capacidade de segmentar o tempo gasto na rede Cloudflare, correlacionando esses dados com os eventos e métricas da aplicação;
10. A solução deve prover uma forma de integração com o BIG-IP ASM (Application Security Manager), coletando métricas de desempenho e outros eventos, com capacidade de segmentar o tempo gasto no WAF, correlacionando esses dados os eventos e métricas da aplicação;
11. A solução deve monitorar o desempenho de todas as chamadas a bancos de dados realizadas pelas aplicações, com suporte nativo a Microsoft SQL Server, PostgreSQL, MySQL, Oracle DB, incluindo monitoração via agentes locais e remotos para ambientes especializados como Oracle Exadata, garantindo coleta de métricas sem impacto no desempenho das operações;
12. A solução deve exibir métricas detalhadas para conexões de banco de dados, incluindo taxa de falhas, tempo de resposta médio, volume de requisições e métricas do pool de conexões, com contextualização por aplicação, serviço e ambiente em serviços Java/Spring, Python, correlacionando esses dados com os eventos e métricas da aplicação;
13. A solução deve contextualizar automaticamente consultas a bancos de dados com o aplicativo/serviço correspondente, exibindo número de execuções, taxa de falha, tempo médio de resposta e gráficos de distribuição temporal, além de identificar queries lentas e seu impacto em transações críticas;
14. A solução deve classificar comandos de banco de dados por tipo de operação, agregando métricas por categoria e permitir rastreamento reverso até a origem na aplicação, correlacionando automaticamente com os diversos níveis da aplicação e ao contexto operacional para análise de impacto;
15. A solução deve monitorar disponibilidade e desempenho de serviços externos acessados via Internet (ex: APIs públicas, gateways de pagamento), permitindo cadastro dinâmico de novos endpoints com configuração de checks sintéticos e alertas personalizados;
16. A solução deve prover integração nativa com métricas do Prometheus, garantindo compatibilidade com exporters padrão sem necessidade de adaptação.

7.3.4 Administração e Atualizações

1. A solução SaaS deve prover atualizações automáticas de versão durante a vigência do contrato, sem impacto operacional ou necessidade de intervenção manual em componentes centrais;
2. Os agentes de monitoramento devem possuir mecanismos simplificados de atualização, permitindo automação via ferramentas de gestão de configuração;
3. A solução deve oferecer zero ou mínima necessidade configuração com características de agente único ou prover um local central de configurações de instrumentação que seja capaz de alterar os agentes de coletas sem necessidade de realizar alterações ou configurações diretamente na aplicação, servidores ou em agentes instalados, ou ainda oferecer alternativa de distribuição de configuração para os agentes via git;
4. A solução deve iniciar automaticamente o monitoramento de aplicações e componentes de infraestrutura após inicialização de servidores, hosts ou nós, sem necessidade de intervenção manual ou reinicialização de serviços;
5. A solução deve disponibilizar acesso a dados históricos sem dependência de arquivos externos, garantindo consulta integrada de métricas, logs e eventos armazenados em repositório próprio com mecanismos de busca e filtragem temporal;
6. A solução deve manter dados históricos por no mínimo 12 meses para métricas críticas, eventos de infraestrutura, garantindo retenção configurável por tipo de dado e compliance com políticas de governança;
7. A solução deve disponibilizar API RESTful documentada para exportação programática de dados coletados em formato JSON, com suporte a filtros temporais, por aplicação e por tipo de métrica, garantindo interoperabilidade com ferramentas externas;
8. A solução deve integrar-se a Microsoft Active Directory via LDAP com suporte a autenticação multifatorial (MFA) ou OpenID Connect (OIDC) com Azure Entra para autenticação, mapeando também os grupos dos usuários com os perfis da ferramenta para autorização;
9. A solução deve prover gestão de acesso baseada em papéis (RBAC) com criação de perfis customizáveis, definindo permissões granulares para visualização, configuração e administração de recursos monitorados.

7.3.5 Visualização e Dashboards

1. A solução deve disponibilizar interface de operação e administração via navegador web, com compatibilidade comprovada com as versões estáveis mais recentes de no mínimo dois dos seguintes: Microsoft Edge, Mozilla Firefox ou Google Chrome;
2. A solução deve permitir segmentação lógica de dados monitorados por critérios configuráveis (ambiente, aplicação, unidade organizacional), com visualização isolada de topologias, entidades e métricas em zonas de gerenciamento hierárquicas, integradas a políticas de controle de acesso individualizado;
3. A solução deve prover correlação visual automática entre componentes descobertos, com filtros dinâmicos para exibição de relações diretas e

- indiretas (consumidores/provedores), garantindo navegação contextual em grafos interativos;
4. A solução deve permitir criação de dashboards personalizáveis, combinando métricas, logs e transações em widgets arrastáveis, com capacidade de salvar templates reutilizáveis e compartilhá-los via controle de acesso granular;
 5. A solução deve disponibilizar visualização gráfica pré-definida das principais métricas críticas (tempo de resposta, taxa de erro, throughput), com filtros por aplicação, ambiente e camada tecnológica;
 6. A solução deve prover diagrama integrado de desempenho aplicação infraestrutura, relacionando serviços monitorados (ex: microsserviços) aos recursos subjacentes (ex: pods, nós Kubernetes, storage), com overlay de métricas de consumo;
 7. A solução deve apresentar estrutura hierárquica de tecnologias inventariadas, detalhando tipo, versão e quantidade de componentes por categoria (ex: 15 serviços Java 11 ou 03 databases PostgreSQL 8);
 8. A solução deve exibir mapa geográfico interativo de origens de acesso, correlacionando localização geográfica de usuários finais a latência de rede e disponibilidade regional;
 9. A solução deve disponibilizar linha do tempo histórica ajustável (de minutos a meses), permitindo análise comparativa de métricas em períodos customizáveis;
 10. A solução deve gerar mapas de volume de transações e tempo médio de resposta por componente, com estratificação por percentis (P90, P99);
 11. A solução deve destacar visualmente desvios de comportamento da aplicação mediante comparação com baseline dinâmica;
 12. A solução deve monitorar a experiência do usuário final em navegadores web, coletando dados de interações, métricas de desempenho de carregamento de páginas e eventos de JavaScript, garantindo rastreabilidade integral desde ações no frontend até transações correspondentes no backend;
 13. A solução deve permitir criação e execução de testes sintéticos para validação de endpoints, APIs e interações complexas em aplicações web, incluindo verificações de disponibilidade, códigos de status HTTP e medição de desempenho, devendo ainda suportar disparo de testes a partir de agentes distribuídos em múltiplas localizações geográficas, configuração de alertas personalizados e correlação automática com métricas de aplicação e infraestrutura monitoradas;
 14. A solução deve integrar-se a workflow de resolução pré-definidos ou bases de conhecimento técnico, garantindo a geração de sugestões de mitigação para incidentes e anomalias com base em documentação validada. As sugestões devem incluir etapas de correção considerando o contexto.

3.7.6 Incidentes Alertas e Notificações

1. A solução deve dispor de funcionalidades de correlação e contextualização de eventos com inteligência artificial, incluindo deduplicação automática para eliminar eventos repetitivos associados ao mesmo elemento de infraestrutura monitorado;
2. A solução deve implementar mecanismos de supressão e correlação de alertas para evitar notificações redundantes, agrupando automaticamente eventos relacionados a um mesmo problema subjacente que afete múltiplos componentes ou serviços, com identificação unificada de causa raiz e representação consolidada no painel de incidentes;
3. A solução deve correlacionar eventos relacionados entre si, identificando o evento disparador de incidentes e estabelecendo relações causais entre componentes de aplicação e infraestrutura;
4. A solução deve disponibilizar informações contextualizadas sobre eventos ativos ou anteriores em aplicações, com detalhamento técnico do ambiente monitorado, incluindo aplicação, serviços e componentes de infraestrutura impactados;
5. A solução deve auxiliar na identificação automatizada de causas raiz de eventos, vinculando degradações de experiência do usuário a componentes técnicos específicos como consultas SQL, APIs REST ou chamadas de WebServices;
6. A solução deve garantir sincronismo temporal entre os dados dos componentes de infraestrutura e de aplicação;
7. A solução deve 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, ou API /REST);
8. A solução deve permitir análise da evolução de eventos na aplicação em uma linha de tempo, mostrando os como os serviços impactados no período;
9. A solução deve prover mecanismos nativos para definição e monitoramento contínuo de Service Level Objectives (SLOs) e Service Level Indicators (SLIs), permitindo configuração de métricas personalizadas (disponibilidade, latência, tempo de resposta) com notificação automática de violações e cálculo de burn rate para gestão proativa de riscos;
10. A solução deve analisar logs de aplicações para criar regras de notificação baseados em ocorrência de palavras-chave ou padrões textuais;
11. A solução deve coletar logs de aplicações automaticamente, com capacidade de busca irrestrita, análise contextualizada e visualização integrada às mensagens de log originais;
12. A solução deve ingerir e contextualizar automaticamente logs de pods Kubernetes com aplicações/serviços correspondentes, sem exigir mudanças nos manifests para associação;
13. A solução deve correlacionar eventos operacionais como reinicializações, deploys ou alterações de configuração com incidentes, permitindo associação causal com problemas no ambiente monitorado;
14. A solução deve estabelecer baselines dinâmicos para métricas de aplicação mediante aprendizado contínuo do comportamento operacional histórico, permitindo configuração de janelas temporais de referência (ex: últimas 24 horas ou 7 dias) para detecção automatizada de anomalias e ajuste adaptativo de thresholds de alertas sem intervenção manual;
15. A solução deve identificar e automaticamente componentes, endpoints, requisições e queries SQL com baixo desempenho, lentidão ou travamentos mediante análise contínua do comportamento operacional e baseline dinâmico, gerando alertas inteligentes que considerem critérios multidimensionais como histórico de métricas, padrões sazonais e impacto potencial ao usuário, com supressão de falsos positivos e sua priorização contextualizada sem necessidade de configuração manual;
16. A solução deve disponibilizar sistema de alertas em tempo real com notificações eficazes, garantindo identificação clara e direta de problemas sem necessidade de drilldown adicional e provendo painel exclusivo para visualização centralizada de alertas ativos e históricos;
17. A solução deve permitir a criação de alertas baseados em métricas estáticas e dinâmicas, utilizando valores fixos ou adaptativos derivados de baseline gerado automaticamente pela solução, com configuração de thresholds ajustáveis conforme padrões históricos e comportamento do ambiente;
18. A solução deve incluir eventos pré-configurados para métricas essenciais incluindo utilização de CPU, memória, disco, rede, tempo de resposta de aplicação, taxas de erro e ações de usuário, com possibilidade de personalização e expansão conforme necessidades específicas;
19. A solução deve executar notificação de alertas e incidentes, incluindo envio de e-mails, integração com aplicativos de mensagens instantâneas e comunicação entre aplicações via APIs, com suporte a configuração de múltiplos canais de notificação e gatilhos personalizáveis;
20. A solução deve prover integração nativa com ferramentas externas de notificação e colaboração via webhooks, permitindo encaminhamento

automatizado de abertura e fechamento de alertas e incidentes para sistemas de terceiros, com suporte a protocolos padrão e configuração de payloads personalizáveis;

21. A solução deve suportar automação de ações corretivas a partir de alertas ou incidentes, executando requisições HTTP customizadas ou scripts pré-definidos em ambientes monitorados, com controle de segurança e permissões granulares para operações críticas;
22. A solução deve permitir criação de alertas baseados em regras predefinidas com aplicação automática a novas transações e componentes descobertos, estendendo configurações de alertas existentes para entidades similares sem necessidade de reconfiguração manual por aplicação ou por tipo de componente;
23. A solução ser capaz de apresentar análise de pilhas de erros de serviços monitorados, interpretando padrões técnicos e contextualizando-os com métricas de ambiente, propondo explicações em linguagem natural e sugestões de correção baseadas em diagnósticos automatizados;
24. A solução deve gerar alertas proativos mediante análise contínua de métricas, padrões históricos e tendências, identificando desvios de comportamento que indiquem riscos potenciais à operação antes que impactem serviços críticos. As regras de alerta devem utilizar modelos dinâmicos (ex.: baseline adaptativo, machine learning) para ajustar thresholds automaticamente conforme contexto operacional, garantindo notificação antecipada de degradações, gargalos ou indisponibilidades iminentes;
25. A solução deve permitir a configuração de ações automatizadas relativas a eventos detectados, incluindo execução de scripts ou playbooks ansible além de requisições http ou outra forma de envio dos dados do evento para um sistema externo.

3.8 Requisitos de Capacitação e Treinamento

O treinamento será ministrado no modelo repasse de conhecimento, em língua portuguesa e terá uma turma com servidores da infraestrutura e do desenvolvimento, bem como deverá promover workshop promovendo entendimento entre teoria e prática.

O repasse de conhecimento deve seguir ementa e material oficial do fabricante;

O repasse de conhecimento abordará os seguintes tópicos:

- Visão detalhada das capacidades e funcionalidades da plataforma.
- Atividades fundamentais de gestão, configuração, monitoramento e manutenção.
- Diretrizes completas para a instalação, configuração técnica e operação dos componentes do sistema.
- Procedimentos para a manutenção regular dos elementos do sistema. Panorama geral e análise da arquitetura subjacente da solução.
- Implementação contínua e integração permanente com o uso da plataforma.
- Identificação e resolução de incidentes e problemas por meio da solução.
- Estratégias de alocação de recursos para a implantação efetiva.
- Aplicação de experiências práticas em ambientes de aprendizado como suporte ao conhecimento.
- Ênfase na supervisão e acompanhamento constante do ambiente de produção.
- Ampla cobertura dos conhecimentos requisitados para administração, configuração, otimização, solução de problemas e utilização integral da plataforma.

3.9 Requisitos de Manutenção e suporte técnico pelo fabricante

- Assistência técnica especializada, seja por meio de suporte remoto ou presencial, sem geração de custos ou encargos adicionais para o CONTRATANTE.
- Disponibilidade de suporte remoto 24 horas por dia, 7 dias por semana, fornecido pelo fabricante da solução.
- O suporte abrangerá assistência técnica para resolver problemas e dúvidas relacionadas à solução. Isso pode incluir suporte telefônico, chat ao vivo, sistema de tickets ou outros meios de comunicação.
- O suporte abrangerá a disponibilização regular de atualizações, incluindo melhorias funcionais, novas versões, correções e patches de segurança para a solução.

3.10 Requisitos de Conformidade

- A solução deve ser um componente ativo do portfólio de produtos oferecidos pelo fabricante e não deve ter sido descontinuada.
- Durante o período contratado, a solução deve permitir o uso completo de todas as funcionalidades, tecnologias e recursos especificados, sem restrições e sem a necessidade de subscrições ou custos adicionais
- A ferramenta deve estar em conformidade com as leis e regulamentos locais de proteção de dados, garantindo a privacidade e a segurança das informações pessoais.

3.11 Requisitos Temporais

- Apresentar um **plano de implementação** que inclua os requisitos de instalação e um cronograma abrangendo a entrega, instalação, configuração e disponibilização da solução em até **30 dias corridos** após a assinatura do contrato.
- Entregar as **subscrições** (licenças) em um prazo máximo de **5 dias úteis** a contar da aprovação do plano de implementação, com a confirmação formal da CONTRATADA para o CONTRATANTE.
- A confirmação da entrega será comunicada por escrito pela CONTRATADA ao CONTRATANTE.

- Realizar uma verificação conjunta das subscrições (licenças) conforme especificado, com representantes da CONTRATADA, para emitir o Termo de Recebimento Provisório.
- Se necessário, antes do prazo estabelecido, a CONTRATADA poderá formalizar um pedido de prorrogação de prazo devidamente justificado. A administração do CONTRATANTE avaliará e decidirá sobre a prorrogação do prazo ou a aplicação de penalidades.
- A confirmação de entrega dos itens no CONTRATANTE e a ausência de pendências de responsabilidade da CONTRATADA, esta receberá uma cópia do "Termo de Recebimento Provisório" em até 5 (cinco) dias úteis, contados a partir do primeiro dia imediatamente posterior à confirmação de entrega dos itens no CONTRATANTE.
- Concluir, dentro do prazo de **30 dias corridos**, a partir da emissão do termo de recebimento provisório das subscrições, a **implantação e configuração** dos produtos, garantindo total compatibilidade com o ambiente computacional do CONTRATANTE e em estrita conformidade com a proposta técnica apresentada. Isso inclui o cumprimento de todas as cláusulas de garantia e atendimento técnico estabelecidas no contrato, de acordo com os prazos e termos ali especificados.
- A CONTRATADA receberá uma cópia do "Termo de Recebimento Definitivo", o qual deverá ser providenciado pelo CONTRATANTE em até 5 (cinco) dias úteis após a manifestação da CONTRATADA sobre a conclusão dos serviços e comprovação do atendimento de todas as fases, desde que a CONTRATADA tenha atendido a todas as solicitações e não existam pendências de sua responsabilidade.
- Os serviços de suporte e garantia estarão disponíveis para atendimento durante todos os 7 (sete) dias da semana, 24 (vinte e quatro) horas por dia. Considerar o horário de expediente normal no tribunal nos dias úteis das 07:00 às 21:00 horas.

3.12 Requisitos de Segurança da Informação

Assegurar a confidencialidade contínua, mesmo após o término da vigência ou rescisão do contrato, de informações relacionadas:

- À política de segurança adotada.
- Ao processo de instalação, configuração e personalização de produtos, ferramentas e equipamentos.
- A implementação dos mecanismos de criptografia e autenticação no ambiente do CONTRATANTE.
- Adesão aos critérios, padrões, normas e procedimentos operacionais estabelecidos pelo CONTRATANTE.
- Manutenção do sigilo absoluto, sujeito a penalidades civis, penais e administrativas, referente a qualquer assunto de interesse do CONTRATANTE ou de terceiros que seja conhecido durante a execução deste contrato. A CONTRATADA deve também instruir seus funcionários nesse sentido.
- A ferramenta deve permitir a configuração de níveis de acesso baseados em funções, assegurando que somente pessoas autorizadas tenham acesso às informações sensíveis.
- A ferramenta deve ser capaz de registrar atividades e ações realizadas pelos usuários, possibilitando a identificação de qualquer atividade suspeita ou não autorizada.
- A autenticação dos usuários deve ser reforçada, garantindo que apenas usuários autorizados possam acessar a ferramenta.
- A ferramenta deve receber atualizações regulares para corrigir falhas de segurança e vulnerabilidades, mantendo um ambiente seguro.
- Garantir a disponibilidade, a integridade, a confidencialidade, o não-repúdio e a autenticidade dos conhecimentos, informações e dados hospedados em ambiente tecnológico sob custódia e gerenciamento do prestador de serviços, mesmo após o prazo de vigência ou rescisão contratual.
- Toda informação confidencial gerada e/ou manipulada em razão desta contratação, seja ela armazenada em meio físico, magnético ou eletrônico, deverá ser devolvida, mediante formalização entre as partes, ao término ou rompimento do contrato, ou por solicitação da CONTRATANTE.
- Obedecer a todas as normas e procedimentos de segurança implementados no ambiente de TIC do Superior Tribunal de Justiça.
- O representante legal da CONTRATADA deverá assinar documento TERMO DE CONFIDENCIALIDADE, ou similar, e garantir que os funcionários envolvidos na implementação da solução assinem o TERMO DE CIÊNCIA.
- Os serviços deverão ser executados em conformidade com a legislação aplicável, em especial as certificações sobre segurança da informação, sem prejuízo de outras exigências, objetivando mitigar riscos relativos à segurança da informação.
- A solução deverá respeitar as normas nacionais de proteção de dados e informações vigentes, sobretudo considerando a possibilidade de custódia de conhecimentos, informações e dados pelo prestador de serviços, observadas as seguintes diretrizes:
 - I - Garantia de foro brasileiro;
 - II- Garantia de aplicabilidade da legislação brasileira (NC 14/IN01/DSIC/GSIPR Revisão 01, de 13 de março de 2018), sobre os princípios, diretrizes e responsabilidades relacionados à segurança da informação para o tratamento da informação em ambiente de computação na nuvem;
 - III - Garantia da territorialidade única na prestação do serviço, em vez de um ambiente tecnológico multinacional (NC 14/IN01/DSIC/GSIPR, Revisão 01, de 13 de março de 2018);
 - IV - Garantia de licenciamento compatível com as necessidades do Superior Tribunal de Justiça;
 - V - Garantia que, em qualquer hipótese, o Superior Tribunal de Justiça tem a tutela absoluta sobre os conhecimentos, informações e dados produzidos pelos serviços;
 - VI - Vedado o não uso corporativo dos conhecimentos, informações e dados pelo prestador de serviço, bem como a redundância não autorizada;
- A prestadora deve possuir Plano de Continuidade, Recuperação de Desastres e Contingência de Negócio, que possa ser testado regularmente, objetivando a disponibilidade dos dados e serviços em caso de interrupção.
- Deve desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços.

- A infraestrutura do provedor deve, ainda, implementar controles para isolamento e segurança de sistema operacional, utilizar soluções de virtualização que sejam padrões ou referências de mercado, bem como implementar política de atualização de versão de software e aplicação de correções.
- A CONTRATADA deve comunicar tempestivamente a CONTRATANTE sobre incidentes relevantes e interrupções dos serviços prestados que venham ocorrer e configurem uma situação de crise.
- A empresa fornecedora deverá observar plenamente requisitos de segurança e procedimentos definidos para o acesso às dependências do STJ, bem como requisitos de segurança da informação e de vedação de acesso e divulgação, conforme se aplique, a informações classificadas ou privilegiadas, isto é, aquelas que por qualquer motivo possam vir a representar vantagem mercantil competitiva.
- A contratação deve observar todos os requisitos de segurança digital, regidos no STJ pela sua Política de Segurança da Informação - PSI, bem como demais normas do Governo Federal, como a Lei Geral de Proteção de Dados Pessoais - LGPD.
- O acesso às instalações do Contratante onde serão realizados os serviços deverá ser controlado e permitido somente às pessoas autorizadas.
- A Contratada deverá substituir imediatamente aquele profissional que seja considerado inconveniente à boa ordem ou que venha a transgredir as normas disciplinares do STJ.
- Os profissionais disponibilizados pela Contratada para a prestação dos serviços deverão estar identificados com crachá de identificação, estando sujeitos às normas internas de segurança do STJ, inclusive àqueles referentes à identificação, trajes, trânsito e permanência em suas dependências.
- Os profissionais deverão utilizar a conta que lhe for atribuída, de forma controlada e intransferível, mantendo secreta a sua respectiva senha, pois todas as ações efetuadas através desta, serão de responsabilidade do profissional da Contratada.
- A Contratada deverá manter os seus profissionais informados quanto às normas disciplinares do STJ, exigindo sua fiel observância, especialmente quanto à utilização e segurança das instalações.
- Em relação aos requisitos de Confidencialidade, a solução deverá:
 - Identificar e restringir a alteração de dados de todas as iterações não humanas, como sistema ou processos batch, a não ser que explicitamente autorizadas.
 - Em relação aos requisitos de Autenticação, a solução deverá:
 - Suportar autenticação no serviço de diretórios do STJ: Microsoft Active Directory.
 - Em relação aos requisitos de Autorização, a solução deverá:
 - Segmentar o acesso a usuários com níveis de permissão definidos;
 - Permitir a definição de, pelo menos, os seguintes papéis de usuários: administrador e operador.
- A solução contratada deve permitir que todas as APIs e interfaces do sistema sejam protegidas nos acessos utilizando, no mínimo, padrão TLS 1.2.
- A CONTRATADA deve manter implementadas rotinas que garantam o registro de operações de acesso às informações da CONTRATANTE e eventos relevantes do sistema contratado para auditoria, monitoramento de segurança ou resposta a incidentes e necessidade de análise; esses registros devem conter, no mínimo, o autor, a data/hora e a descrição do evento.
- A CONTRATADA deve possuir mecanismos de proteção dos registros de auditoria (logs) contra modificações e exclusões não autorizadas, em especial por parte de usuários administradores, bem como contra problemas operacionais.
- A solução deve possibilitar a implementação rotinas que mantenham o registro de eventos relevantes do sistema para auditoria ou monitoramento de segurança (SIEM) através de integração (API, JSON, XML ou syslog); esses registros devem conter, no mínimo, o autor, a data/hora, descrição do evento, origem e destino.
- Devem ser adotados controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do sistema ou aplicativo.
- Para sistemas ou serviços de tecnologia providos fora dos datacenters do STJ, a solução contratada deve ser instalada em ambiente certificado de acordo com a norma ABNT NBR ISO/IEC 27001:2013 ou superior.
- Datacenter deve ser locado em território brasileiro, conforme dispõe a Resolução CNJ n. 335, de 29 de setembro de 2020.
- A solução contratada deve prover mecanismos para a proteção contra a detecção de vazamento de dados do CONTRATANTE que estiverem sob sua custódia ou possibilitar a conectividade de forma nativa ou via API com a solução de CASB (Cloud Access Security Broker) em execução na CONTRATANTE a fim de identificar e combater ameaças cibernéticas na nuvem.
- A CONTRATADA deve disponibilizar relatório de vulnerabilidades da solução contratada e previamente à liberação de novas versões das aplicações, evidenciando a ausência de vulnerabilidades declaradas no OWASP API Top 10, sempre que solicitado pela CONTRATANTE.
- A CONTRATADA deve permitir o acesso do CONTRATANTE, a qualquer tempo, aos dados e informações processadas e/ou armazenadas referentes aos serviços prestados.
- A CONTRATADA deve prover mecanismos para auditoria pelo CONTRATANTE ou sob sua indicação, dos serviços prestados em conformidade com sua regulamentação.
- A CONTRATANTE pode solicitar evidências técnicas dos atendimentos aos itens de segurança da informação durante a vigência deste contrato. A CONTRATADA deve fornecer estas evidências em até 5 (cinco) dias úteis.
- A Solução deve apresentar alta disponibilidade, conforme especificado neste documento, garantindo a continuidade do serviço em níveis aceitáveis para o negócio da CONTRATANTE, em eventuais cenários de crise ou indisponibilidade do serviço prestado, e o Fabricante da Solução (Provedor de SaaS) deve possuir estratégias de continuidade e contingência de negócios adequados.
- Em caso de substituição da CONTRATADA, deve ser possível a exclusão dos dados armazenados, processados e gerenciados pela Solução contratada.
- A CONTRATADA deve se adequar continuamente para assegurar que possíveis mudanças de regulamentações estejam perfeitamente em conformidade com os serviços e ações da CONTRATADA.
- O Fabricante da Solução (Provedor de SaaS) deve manter estratégias de backup e/ou retenção capazes de garantir a recuperação de informações

necessárias, conforme os critérios pertinentes à prestação do serviço e de acordo com o objeto do contrato.

- A solução deve permitir a detecção automática e em tempo de execução, de vulnerabilidades nas aplicações sem a necessidade de configuração prévia de escaneamentos periódicos, utilizando o mesmo agente único.
- Deve descobrir automaticamente os problemas de segurança no ambiente e fornecer avaliações de risco automatizadas e contextualizadas.
- Deve identificar vulnerabilidades que precisem de investigação imediatamente.
- Deve utilizar Inteligência Artificial para gerar automaticamente uma pontuação de risco exclusiva para cada vulnerabilidade potencial com base na topologia em tempo real e na análise de vetores de transações.
- Detectar vulnerabilidades no mínimo nas tecnologias JAVA, NEY, Node.js, PHP, kubernetes, Pytohn.
- Deve fornecer uma visão geral dos problemas de segurança atuais no ambiente monitorado.
- Deve exibir o número de problemas de segurança abertos atualmente no ambiente monitorado.
- Deve exibir a porcentagem de hosts cobertos pela detecção de vulnerabilidade de tempo de execução durante a última hora.
- Deve listar todas as vulnerabilidades detectadas no ambiente monitorado.
- Deve pontuar as vulnerabilidades de acordo com o nível de riscos.
- Deve listar a situação de cada vulnerabilidade identificada no ambiente.
- Deve permitir a definição de regras personalizadas de monitoramento de segurança por meio da interface do usuário WEB ou API.
- Deve permitir a transmissão de problemas de segurança às equipes para fins de alerta e correção.
- A plataforma deve utilizar dados de observabilidade em tempo de execução para priorizar vulnerabilidades com base no contexto de ambiente de tecnologia e negócios.
- Através do agente de APM, deve ser possível analisar:
 - Se o código vulnerável está realmente implantado;
 - Se o código vulnerável está em execução;
 - Se a vulnerabilidade pode ser acessada por meio de uma API voltada para a Internet;
 - Se o código vulnerável está implantado em uma infraestrutura mal configurada (mapas de serviços de APM com Infraestrutura).
- Deve fornecer ampla visibilidade no ambiente de TI e a capacidade de encontrar riscos de um ataque de "dia-zero".
- Deve validar se patches de vulnerabilidade de pré-produção estão implantados em produção.
- A solução deve identificar dependências e vulnerabilidades de softwares de código aberto (OSS) em aplicativos, suas bibliotecas e pacotes de terceiros.
- Deve identificar CVEs (exposições comuns de vulnerabilidade) e gerar automaticamente classificações de impacto, associadas a bibliotecas OSS.
- A instrumentação deve ser em tempo de execução e permitir a criação de consultas e alertas.
- Deve fornecer contexto para resultados de vulnerabilidade com base no contexto de negócios e no impacto da vulnerabilidade usando dados de observabilidade, orientando assim a priorização de resoluções.
- Deve fornecer possibilidade de criar relatórios automatizados que fornecem perspectivas e visões executivas de vulnerabilidades e riscos.
- Deve informar opções de mitigação efetiva para as vulnerabilidades identificadas, com indicação de correção.
- Deve manter uma lista atualizada das vulnerabilidades que foram corrigidas.
- Deve possibilitar a integração com IDEs e sistemas de tickets, ajudando a evitar interrupções do desenvolvedor, acelerando a velocidade do desenvolvimento.
- A solução deve estender a análise de fluxo de vulnerabilidade usando o módulo de APM em combinação com o módulo de Infraestrutura para confirmar o risco em entidades que se estendem por vários outros microsserviços em suas diversas camadas.
- Deve disponibilizar interface onde seja possível explorar e recuperar dados detalhados de observabilidade e obter maior perspectiva sobre seus aplicativos afetados por determinadas vulnerabilidades.
- Deve ter uma interface que facilita a visualização e classificação de aplicativos como seguros, exploráveis, prontos para serem testados ou não testados
- Possuir uma interface onde seja possível visualizar todas as camadas de aplicativos, serviços back-end e APIs envolvidas na análise de vulnerabilidade.

3.13 Requisitos Sociais, Ambientais e Culturais

- É necessário confirmar o conhecimento e a conformidade com a Política de Sustentabilidade do CONTRATANTE, seguindo as diretrizes estabelecidas na Instrução Normativa STJ/GDG nº 4, datada de 16 de janeiro de 2024, que estabelece a Política de Sustentabilidade no STJ. Além disso, os profissionais designados para trabalhar localmente devem estar cientes das boas práticas relacionadas ao consumo responsável, à redução do desperdício de recursos naturais e à prática de coleta seletiva.
- Quando estiver atuando no STJ, o preposto ou representante técnico assume a responsabilidade pela preservação e higiene dos espaços onde

desempenham suas funções.

- Além disso, é obrigatório que eles façam a disposição adequada de qualquer resíduo gerado durante a execução do contrato, contribuindo assim para a preservação do meio ambiente.
- Os profissionais que prestam serviços no STJ devem estar bem informados sobre as boas práticas relacionadas ao consumo consciente, à redução do desperdício e à coleta seletiva, tudo isso com o intuito de preservar o meio ambiente e os recursos públicos.

3.14 Requisitos de arquitetura tecnológica

- A solução de APM deve ser plenamente compatível com arquiteturas de microserviços, oferecendo a capacidade de monitorar e avaliar o desempenho de micro serviços individuais em ambientes distribuídos.
- A solução de APM deve ser capaz de maneira nativa e automática, realizar a descoberta dos serviços presentes no ambiente monitorado.
- A solução de APM deve ser habilitada para integrar-se eficientemente ao Active Directory, proporcionando controle de acesso.
- A solução de APM deve possuir uma integração fluida com ambientes Kubernetes, permitindo o monitoramento de contêineres e aplicativos.
- A solução de APM deve ser capaz de armazenar dados de monitoramento a longo prazo para análises históricas e cumprimento de requisitos de retenção de dados.
- A arquitetura da solução de APM deve ser altamente eficaz na coleta de dados de desempenho, minimizando qualquer impacto sobre o desempenho dos aplicativos monitorados.
- A arquitetura da solução de APM deve ser cuidadosamente projetada para garantir alta disponibilidade, assegurando que o sistema de APM permaneça acessível e operacional, mesmo diante de falhas de hardware ou software.
- A solução de APM deve permitir a configuração de vários perfis de acesso, com diferentes níveis de permissões para os usuários.
- O suporte técnico fornecido pelo fabricante da solução de APM deve estar disponível no Brasil, oferecendo a capacidade de abrir chamados de suporte em língua portuguesa.
- O atendimento deve ser contínuo, 24 horas por dia, todos os dias do ano, incluindo sábados, domingos e feriados (24x7x365), e não deve haver limitações no número de incidentes que podem ser relatados.

3.15 Requisitos de projeto e de implementação

- Apresentar o plano de implementação conforme o prazo estipulado no contrato. Esse plano deve detalhar o cronograma de todas as fases de implementação da solução, incluindo a alocação de recursos, a equipe envolvida, os pré-requisitos de instalação, as atividades atribuídas a cada parte e a identificação dos principais riscos, bem como as estratégias de mitigação.
- O projeto deve abranger, no mínimo, os seguintes aspectos:
 1. Verificação das subscrições (licenças) durante o período estabelecido no contrato, diretamente no site do fabricante em nome do STJ;
 2. Preparação do ambiente de instalação, quando necessário;
 3. Execução das etapas de instalação e configuração;
 4. Realização de testes de operação;
 5. Ativação da solução, incluindo a aplicação do licenciamento;
 6. Entrega da documentação atualizada;
- O cronograma de instalação e configuração deve ser elaborado, considerando realizar atividades fora do horário comercial, aos fins de semana e em feriados.
- Atividades executadas na produção deverão ocorrer preferencialmente em período fora do expediente, finais de semana e feriados.
- Deve ser especificada a infraestrutura de hardware e software necessária para suportar o sistema de APM, incluindo servidores, redes e bancos de dados.

3.16 Requisitos de implantação

- Realizar a atualização dos equipamentos da solução sem causar interrupções nas operações diárias dos usuários.
- Executar o escopo contratual de forma rigorosa, em conformidade com as leis aplicáveis, a proposta apresentada e as orientações do CONTRATANTE, assegurando padrões elevados de qualidade.
- Cumprir o escopo de acordo com as diretrizes dos fabricantes, normas técnicas pertinentes e as especificações detalhadas na proposta original, bem como conforme as instruções fornecidas nas Ordens de Serviço emitidas pelo CONTRATANTE.
- Realizar quaisquer adaptações ou serviços nos ambientes do CONTRATANTE que sejam necessários para a instalação dos equipamentos, mediante prévia autorização do STJ.
- Entregar as subscrições de ativação e os componentes correspondentes às suas próprias despesas, efetuando a instalação e conduzindo todos os testes

requeridos para garantir o funcionamento perfeito dos produtos especificados.

- Efetuar a instalação das subscrições de ativação nos prazos e horários definidos pela equipe técnica do CONTRATANTE, que supervisionará os procedimentos.
- Executar todos os trabalhos sem a necessidade de paralisação do ambiente de produção, com exceção das situações preestabelecidas com a equipe do CONTRATANTE. Ademais, é essencial respeitar as operações internas da Organização, garantindo que não sejam afetadas em decorrência de nenhuma das atividades contratadas.
- Implementar adequadamente o planejamento, a execução e a supervisão contínua das tarefas atribuídas, visando a assegurar um funcionamento adequado e eficiente. Todos os serviços devem ser realizados com precisão e cuidado, mantendo todas as instalações do CONTRATANTE em perfeitas condições.
- prontamente responder a todas as solicitações de esclarecimentos feitas pela equipe de fiscalização do CONTRATANTE, relacionadas ao cumprimento do objeto do contrato.
- Permitir o acesso exclusivo de técnicos autorizados em horários determinados, de acordo com os procedimentos de controle e manutenção estabelecidos.
- Após a implantação, o sistema de APM deve ser verificado para garantir que todos os componentes estejam funcionando conforme o esperado.
- É fundamental que após a implantação o APM já seja capaz de realizar a descoberta de todos os serviços a serem monitorados no ambiente, de maneira automática.
- Toda a atividade de implantação deve ser documentada detalhadamente, incluindo qualquer configuração específica ou ajustes feitos durante o processo.

3.17 Requisitos de garantia e manutenção

- Disponibilizar acesso ao portal de suporte online do fabricante da solução para verificar o status das subscrições, atualizações de software, recomendações e alertas relacionados ao funcionamento de todos os elementos da solução.
- Facilitar o acesso às atualizações e aprimoramentos de software desenvolvidos pelo fabricante por meio de downloads a partir do portal de suporte do fabricante.
- Oferecer acesso às correções desenvolvidas pelo fabricante (Hot Fixes e Patches) para abordar questões de desempenho ou segurança do software, também por meio de downloads no portal de suporte do fabricante.
- Disponibilizar acesso ao portal de suporte online do fabricante da solução para rastrear o progresso dos tickets de suporte abertos para os componentes da solução.
- Providenciar toda a equipe qualificada necessária para a execução das tarefas de instalação e configuração.
- Refazer as tarefas que forem rejeitadas pelo CONTRATANTE.
- Assumir todas as despesas relacionadas à realização dos serviços, incluindo custos com mão de obra, ferramentas, equipamentos, taxas, despesas administrativas e encargos sociais.
- Colocar à disposição do CONTRATANTE a equipe técnica para prestar orientação sobre a execução dos serviços, sempre que solicitado.
- Não transferir, de forma integral ou parcial, o escopo do contrato sem a prévia e expressa autorização do CONTRATANTE.
- Assumir total responsabilidade por danos ou prejuízos que possam ocorrer ao CONTRATANTE ou a terceiros como resultado de ações ou eventos atribuíveis aos técnicos da empresa.
- Abster-se de realizar qualquer publicidade relacionada aos serviços contratados sem a autorização prévia por escrito do CONTRATANTE.
- Manter, ao longo de toda a prestação dos serviços, os requisitos de qualificação e habilitação estipulados na licitação.
- Fornecer informações técnicas à equipe do CONTRATANTE sobre a operação do ambiente conforme necessário.
- Oferecer avaliação e realizar ajustes nas novas instalações no ambiente quando solicitado pelo CONTRATANTE.
- Realizar análises e propor soluções adequadas para o ambiente contratado sob a orientação da equipe técnica do CONTRATANTE.
- Conceder acesso à base de conhecimento mantida pelo fabricante da solução.
- Registrar e identificar todas as ações autorizadas, possibilitando a responsabilização dos profissionais que acessaram os ambientes em questão em caso de eventos específicos.
- O sistema deve garantir um tempo de resposta máximo aceitável para as operações de monitoramento e consulta, conforme definido em contrato.
- Deve ser fornecido suporte técnico contínuo, 24 horas por dia, 7 dias por semana, para lidar com problemas críticos de operação.
- A solução de APM deve ser continuamente monitorado para identificar possíveis problemas de desempenho ou indisponibilidade.
- Deve ser fornecido um relatório regular de desempenho do sistema, incluindo métricas de disponibilidade, tempo de resposta e incidentes de segurança.

3.18 Requisitos de Capacitação Técnico-Profissional

- Repasse de conhecimento relacionado à administração e monitoramento utilizando a solução.
- Repasse de conhecimento sobre o uso da solução de observabilidade, incluindo a configuração e análise de resultados.
- Repasse de conhecimento sobre como identificar e resolver problemas de desempenho usando a solução de observabilidade.
- Repasse de conhecimento sobre como configurar e gerenciar alertas de desempenho de acordo com as necessidades do tribunal.
- Repasse de conhecimento sobre como implementar atualizações de software e realizar a manutenção regular do sistema.
- Repasse de conhecimento sobre as melhores práticas de monitoramento de desempenho e segurança de aplicativos.

3.19 Requisitos de Experiência Profissional

- A execução do planejamento, instalação e configuração deve ser conduzida por técnicos certificados pelo fabricante da solução, que também apresentem uma comprovada experiência nessas tarefas.

3.20 Requisitos de Configuração

- Realizar a instalação e configuração da solução levando em consideração a infraestrutura disponível no ambiente do CONTRATANTE:
 - a) Para máquinas virtuais, utilizar aquelas fornecidas pelo software de virtualização da VMware ou HyperV.
 - b) Caso necessário, o sistema operacional a ser utilizado será o Oracle Linux.

3.21 Requisitos de Desempenho

A solução de observabilidade deve:

- Garantir um tempo de resposta máximo aceitável para consultas e relatórios, por exemplo, 15 segundos para relatórios padrão.
- Ser capaz de lidar com um aumento significativo na carga de trabalho sem degradação significativa do desempenho
- Possibilitar que o tempo de latência entre a coleta de dados de monitoramento e a disponibilidade desses dados para análise deve ser mantido em um nível mínimo, por exemplo, menos de 1 minuto.
- Ser capaz de coletar dados de desempenho em intervalos específicos (por exemplo, a cada 1 minuto) sem afetar negativamente o desempenho dos aplicativos monitorados
- Manter uma alta disponibilidade, com um objetivo de, por exemplo, 99,9% de disponibilidade ao longo do ano.
- Ser capaz de reter dados de monitoramento de longo prazo, conforme exigido pelas políticas do STJ, sem impacto significativo no desempenho.
- Permitir que as consultas aos dados de monitoramento possam ser executadas de forma eficiente, garantindo que os relatórios e análises sejam gerados em tempo hábil.
- Ser escalável horizontalmente, permitindo adicionar recursos conforme necessário para acomodar o crescimento das operações do tribunal.
- Permitir que os dados de monitoramento possam ser armazenados de forma eficiente, minimizando os requisitos de armazenamento sem comprometer a qualidade dos dados.
- Ser capaz de processar dados em tempo real e fornecer alertas imediatos quando forem detectados problemas de desempenho.
- Permitir que coleta de dados de monitoramento pela solução de observabilidade não cause um impacto significativo no desempenho dos aplicativos monitorados.
- Ser capaz de acomodar aplicativos e serviços que exigem uma quantidade significativa de recursos, escalando verticalmente quando necessário.
- Ser capaz de se recuperar, e retomar a coleta de dados e a geração de alertas dentro de um tempo especificado, nos casos em que ocorrerem falhas.
- Ser capaz de monitorar simultaneamente múltiplos aplicativos e serviços em execução no ambiente do STJ.

3.22 Demais requisitos aplicáveis

- Estabelecer os termos de gestão do contrato e as responsabilidades das partes envolvidas.
- Garantir que os serviços sejam prestados conforme os parâmetros e procedimentos definidos neste processo de contratação, aderindo às melhores práticas reconhecidas, normas e regulamentações, bem como mantendo uma conduta apropriada na utilização de recursos de software e hardware.
- Manter, ao longo de todo o período de validade do contrato, as condições que ensejaram sua celebração.
- Realizar inspeções regulares de seus recursos e equipe técnica designada para a prestação dos serviços, assegurando que as atividades estejam sendo executadas nas condições adequadas.
- Refazer quaisquer serviços que, mediante justificativa válida em um documento elaborado pelo representante do CONTRATANTE, não atendam aos requisitos estabelecidos, sem implicar em custos adicionais, independentemente das penalidades definidas nas Ordens de Serviço e Níveis de Qualidade acordados.
- Executar o objeto do contrato de forma diligente, em conformidade com a legislação vigente, a proposta apresentada e as diretrizes do CONTRATANTE, sempre aderindo aos padrões de qualidade estabelecidos.

4.1 Diferentes soluções de TIC que, com base em levantamento de mercado, possam atender à necessidade do Tribunal*:

4.1.1 Alternativas no mercado de TIC

O avanço tecnológico tem desempenhado um papel notável na otimização de processos e na ampliação da eficiência operacional em várias esferas, incluindo o campo judiciário. Consciente dessa evolução e buscando garantir a excelência na prestação de serviços, o Superior Tribunal de Justiça reconheceu a necessidade premente de incorporar uma ferramenta de Monitoramento de Desempenho de Aplicativos (APM) dedicada à gestão e supervisão das aplicações essenciais utilizadas diariamente em suas operações.

Inicialmente, realizou-se uma análise do Quadrante Gartner de Gerenciamento de Desempenho de Aplicativos (APM) com o propósito de identificar as empresas que se destacavam nesta área. Baseada nessa informação, foram conduzidas, em 2023, Provas de Valor (POVs) individuais para avaliar cada uma das soluções oferecidas pelas empresas líderes identificadas no Quadrante Mágico, tais como Dynatrace, Datadog, IBM Instana e Cisco AppDynamics.

Uma das considerações fundamentais nessa etapa recaía sobre as características do ambiente em questão, englobando informações como a Quantidade de Hosts, Quantidade de Máquinas Físicas e Virtuais no ambiente, Pods no ambiente, Quantidade de Microsserviços, Especificações das Máquinas, como Capacidade de Memória RAM, Número de Usuários que Acessam as Aplicações e o Volume de logs gerados, entre outros aspectos relevantes. Destaca-se a relevância dessas informações em virtude da variação nos modelos de licenciamento oferecidos por cada fornecedor. Portanto, era imperativo a obtenção de todos esses detalhes a fim de permitir que cada fornecedor realizasse estimativas precisas referentes aos licenciamentos necessários.

Outra consideração de suma importância está relacionada ao escopo a ser contemplado tanto nas Provas de Valor quanto no processo licitatório em si. Inicialmente, foi deliberado que o escopo abrangeria exclusivamente o sistema "Justiça Web", "CPE", "Administrativo" e "EPro". Porém, posteriormente ficou decidido que o escopo que a ferramenta de APM deverá observar será de todo o ambiente de containers do Tribunal.

Ao estabelecer comunicação com a Dynatrace, nos foi solicitado uma avaliação das condições atuais do ambiente, conforme explicitado anteriormente. Essa estimativa preliminar das especificações do ambiente foi elaborada, com o propósito de fornecer informações essenciais à Dynatrace e às outras empresas no momento da preparação das Provas de Valor. Nesse contexto, foi estabelecido contato com a empresa Dynatrace para dar início a uma POV, informando-os a estimativa preliminar das especificações do ambiente. O principal objetivo dessa iniciativa consistia em viabilizar a exploração da ferramenta de APM fornecida pela Dynatrace, ao mesmo tempo em que permitia a obtenção de dados detalhados relacionados às características do ambiente, ao número de usuários e às aplicações em questão.

Estimativa preliminar das especificações do ambiente:

ESPECIFICAÇÃO	VALOR
Unidades de Host Total (Dynatrace)	241 Hosts
Quantidade de Sessões de Usuário por Ano	6.000.000 Sessões
Quantidade de Logs por dia	7,2 GB

Com base nas informações coletadas e fornecidas à Dynatrace, procedemos à execução da Prova de Valor (POV - 3877102). A POV teve início em 13 de março de 2023 e culminou em uma reunião realizada em 14 de abril de 2023, na qual os resultados obtidos nos foram apresentados. É importante ressaltar que a Dynatrace utiliza uma tecnologia na qual é instalado apenas um único agente uma única vez por host para começar a coletar todas as métricas relevantes em toda a cadeia de entrega de sua aplicação.

É salutar destacar que a POV revelou-se altamente benéfica. Durante esse período, tivemos a oportunidade de empregar a ferramenta no ambiente de produção e esclarecer incertezas acerca de seu funcionamento, além de explorar melhores práticas para a observação e monitoramento de aplicações. Importante mencionar que a Coordenadoria de Desenvolvimento de Soluções de Software (CDES) desempenhou um papel ativo na POV, também empregando a aplicação e participando das reuniões de acompanhamento para solucionar dúvidas e acompanhar as discussões relevantes.

Através dessa POV inicial, conseguimos obter uma estimativa mais precisa do ambiente, enriquecida com informações de relevância significativa. Esses dados foram compartilhados entre os participantes envolvidos no processo de licitação sendo submetidos à validação das partes interessadas. Estimativa das especificações do ambiente após a primeira POV:

ESPECIFICAÇÃO	VALOR
Nodes	16
CPU	376
Memória	3.2TB
Pods	980
Requisições	2.600.000/dia
Mensagens de Log	17.600.000/dia
Quantidade de Log (GB)	28GB/dia
Real User Monitoring (RUM) sem replay de sessão	127.333/dia

Concomitantemente à realização da POV com a Dynatrace, procedeu-se ao levantamento de requisitos junto à Coordenadoria de Desenvolvimento de Soluções de Software. Nesse contexto, foram identificados requisitos considerados como essenciais, desejáveis e aqueles que estariam fora do âmbito da licitação. Os requisitos apurados estão detalhados a seguir:

•Disponibilizar Logs Centralizados (ESSENCIAL)

- o A ferramenta deve oferecer uma visualização centralizada dos logs das aplicações, permitindo a agregação de logs de diferentes pods de um serviço em um único local.
- o Deve fornecer filtros com parâmetros como nome do Workload, usuário, URL, Namespace, etc.
- o Manter um histórico de logs por pelo menos uma semana, sendo flexível quanto à possibilidade de ajustar esse período.

•Identificação de Problemas em Tempo Real (ESSENCIAL)

- A ferramenta deve detectar problemas em tempo real no ambiente, associando serviços, requisições, usuários e aplicações de front-end, fornecendo informações detalhadas como stacktrace e análise de logs.
- Deve alertar sobre serviços que estejam fora do ar ou apresentando erros.

·Identificação de Causa Raiz de Problemas (ESSENCIAL)

- A ferramenta deve ser capaz de identificar a causa raiz dos problemas detectados, correlacionando o erro com todo o ambiente.

·Análise de Sessões de Usuários (ESSENCIAL)

- A ferramenta deve permitir a visualização das sessões de usuários abertas em cada aplicação.
- Deve fornecer informações detalhadas sobre cada sessão, incluindo sucesso e falhas, satisfação do usuário, tempo de sessão, ações realizadas e stacktrace.
- Deve ser possível acompanhar as diversas sessões de um usuário específico em uma data e horário específicos, trazendo informações tanto do front-end quanto do back-end.
- Os dados das sessões devem ser armazenados por pelo menos sete dias.

·Stacktrace (ESSENCIAL)

- A ferramenta deve disponibilizar um stacktrace completo de chamadas, requisições, problemas e sessões, proporcionando observabilidade abrangente.
- O stacktrace deve incluir informações sobre chamadas de código, timeline, tempo de resposta, requisições, códigos com erro e quantidade de falhas, permitindo classificação desses dados.
- As instruções SQL utilizadas nas chamadas devem estar registradas no stacktrace, incluindo os parâmetros para análise.

·Monitoramento de Frontend (ESSENCIAL)

- A ferramenta deve possibilitar a visualização das aplicações web do ambiente, fornecendo informações sobre problemas, requisições com erro, stacktrace associado, tempo de resposta, erros de console, erros de Javascript, etc.
- Deve permitir a organização das diferentes aplicações de front-end em projetos.

·Monitoramento de Backend (ESSENCIAL)

- A ferramenta deve possibilitar a visualização dos serviços do ambiente, apresentando informações sobre problemas, requisições com erro, stacktrace associado, desempenho de chamadas, tempo de resposta, erros associados, etc.
- Deve permitir a organização das diferentes aplicações de backend em projetos.

·Integração entre os Serviços (ESSENCIAL)

- A ferramenta deve oferecer uma visão da integração entre os serviços, incluindo integrações com outros serviços, bancos de dados, servidores, requisições, etc.
- Deve permitir análises verticais e horizontais das chamadas de um serviço.

·Mapa de Integração (DESEJÁVEL)

- A ferramenta pode oferecer uma visualização gráfica da integração das aplicações, serviços, processos, hosts, etc.

·Dashboards (ESSENCIAL)

- A ferramenta deve fornecer dashboards que possam conter todas as informações analisadas do ambiente.
- Deve ser possível configurar novos dashboards de acordo com as preferências do usuário.

·Análise de Vulnerabilidade das Aplicações (FORA DO ESCOPO)

- A análise de vulnerabilidades de aplicações não faz parte do escopo.

·Automação de Releases (FORA DO ESCOPO)

- A automação de releases não está incluída no escopo do projeto.

·Replay de Sessões de Usuários (FORA DO ESCOPO):

- O replay das sessões de usuários não faz parte do escopo.

É importante ressaltar que esses requisitos são considerados preliminares, e estão sujeitos a revisões futuras para possível inclusão no Termo de Referência.

A seguir, a empresa IBM entrou em contato com o objetivo de conduzir uma POV com sua ferramenta de APM denominada Instana. Seguindo o mesmo protocolo utilizado na POV anterior, a empresa solicitou informações preliminares para dar início à POV. Após o fornecimento dessas informações, a POV foi iniciada em 22 de maio de 2023 e concluída em 05 de junho de 2023. É igualmente relevante mencionar que o Instana coleta dados dos sistemas monitorados por meio de um único agente hospedeiro em cada host.

Mais uma vez, a POV demonstrou ser altamente proveitosa, destacando a facilidade de uso da ferramenta Instana e sua interface intuitiva. A CDES também desempenhou um papel ativo na avaliação da ferramenta durante a POV.

Em 06 de junho de 2023, ocorreu uma apresentação da ferramenta de APM Cisco AppDynamics. Embora não tenha sido conduzida uma POV com esse fornecedor, a apresentação da ferramenta foi valiosa para adquirir conhecimento sobre a mesma.

Após isso, demos início a uma POV com a Datadog. Após o preenchimento das informações necessárias para o início da POV, iniciamos as atividades em 14 de junho de 2023. A POV foi concluída em 04 de julho de 2023, com a apresentação dos resultados. Durante essa POV, tivemos a oportunidade de conhecer a ferramenta, embora algumas funcionalidades não tenham sido acessíveis devido a diversos fatores, como a dificuldade na instalação e configuração da ferramenta em nosso ambiente.

Durante as POVs realizadas, a EPC percebeu que a configuração manual de quais serviços seriam monitorados pelo APM envolvia diversas unidades do Tribunal, tendo que ser feita individualmente e de forma contínua. Assim, sempre que um novo serviço surgisse no ambiente seria necessário inserir as configurações do agente do APM nas configurações do serviço para que este fosse monitorado, demandando sempre novo esforço da equipe de implantação/moniração. A EPC também teve dificuldades em realizar essas configurações manuais, houve problemas para colocar serviços para serem monitorados nas POVs da Datadog, por exemplo. Por outro lado, as ferramentas que possuem a ferramenta de descoberta automática se mostraram eficientes e demonstraram na prática a facilidade do processo de descoberta automática e também que os esforços de configuração seriam mitigados ao se ter esse procedimento realizado de forma automática. Devido aos benefícios oferecidos pela descoberta automática de serviços a serem monitorados e as dificuldades encontradas quando essa descoberta é feita de forma manual, entende-se que a plataforma de corporativa de APM deve realizar a descoberta automática dos serviços do ambiente. Este requisito é de suma importância pois, como foi verificado nas POVs realizadas, a configuração manual de quais sistemas devem monitorados pelo APM por muitas vezes não é trivial, envolve diferentes unidades pelo Tribunal, além de demandar grande tempo e esforço. Com a descoberta automática é possível ter uma maior economicidade pois não será necessário atribuir as tarefas de configuração dos serviços para serem monitorados aos servidores responsáveis pelo ambiente e também teremos uma maior confiabilidade do ambiente, pois diminui-se a possibilidade de esquecimento de inclusão de serviços para serem monitorados.

Concomitantemente a todo o trabalho relacionado às POVs, estabelecemos contato com a empresa Central IT, que já mantém um contrato vigente com o STJ. Fomos informados de que o contrato existente contemplava a possibilidade de disponibilização de uma ferramenta de APM por parte dessa empresa, o SIMON Divedot. Com base nessa informação, iniciamos o processo de instalação da ferramenta em nosso ambiente para avaliar se ela poderia satisfazer todos os requisitos identificados no processo de licitação, especialmente os requisitos essenciais. Nesse contexto, a CDES desempenhou um papel fundamental, conduzindo uma análise minuciosa da ferramenta e emitindo uma avaliação final sobre sua adequação.

Durante a instalação e os primeiros estágios de utilização da ferramenta, identificamos que algumas funcionalidades não estavam disponíveis ou não atendiam aos critérios de qualidade estabelecidos. Diante dessa constatação, solicitamos à empresa que realizasse ajustes na ferramenta, visando incorporar essas funcionalidades de maneira satisfatória à nossa operação. No entanto, após o prazo acordado, observamos que as melhorias solicitadas não haviam sido implementadas conforme o esperado.

Diante dessa situação, tomamos a decisão de prosseguir com o processo de licitação. Isso ocorreu porque a ferramenta SIMON Divedot não atendia às nossas necessidades e as tentativas de aprimoramento não se mostraram suficientes dentro dos prazos estabelecidos.

4.1.2 Projetos similares de outros órgãos

Foram encontrados os seguintes contratos com objetos análogos:

Órgão	PE	Objeto	Empresa	Contrato	Vigência	Fabricante	SEI
Anvisa	PE 90014/2024	Contratação de solução de software de Application Performance Monitoring (APM), por subscrição de software por assinatura da solução Dynatrace de Observabilidade (Observability), na modalidade SaaS (Software como Serviço) em nuvem, consistente em subscrições do software para o período contratado, em nome da Anvisa, com suporte e garantia por 24 (vinte e quatro) meses, além dos serviços de instalação, configuração, transferência de conhecimento, suporte e atualização tecnológica, conforme condições e exigências estabelecidas no Edital e seus anexos.	Global Sec	Homologado	-	Dynatrace	6351328
Banestes	PE 3003/2022	Aquisição de solução de APM - Application Performance Monitoring, incluindo serviço de instalação e configuração, treinamento, consultoria e suporte técnico.	AR2 Tecnologia da Informação Ltda	CT 151258	16/03/2026	App Dynamics	6351339
Dataprev	PE 90979/2024	Contratação de Subscrição de Solução APM AppDynamics, por um período de 24 (vinte e quatro) meses, incluindo prestação do serviço de capacitação técnica a ser utilizado sob demanda.	PTLS Serviços de Tecnologia e Assessoria Técnica Ltda	Homologado	-	App Dynamics	6351355
Detran DF	PE 26/2022	Contratação de Solução de Application Performance Monitoring – (APM), com garantia, operação assistida e suporte técnico, bem como fornecer informações necessárias para subsidiar o respectivo processo, conforme condições, quantidades e exigências estabelecidas no Termo de Referência, Anexo A deste Edital.	Very Tecnologia Ltda	1 TA CT 02/2023	07/02/2025	Dynatrace	6351532
		Contratação de pessoa jurídica especializada para a expansão da Solução de Monitoramento de Performance de Aplicações e Observabilidade (APM - Application Performance Management) Dynatrace,					

Estado Goiás	PE 14/2023	através do fornecimento de subscrição de licenças de uso, com suporte e garantia pelo período de 36 (trinta e seis) meses, para atendimento das necessidades de visibilidade fim-a-fim das aplicações hospedadas na Nuvem Privada Corporativa Estadual, e análise da experiência digital dos usuários dessas aplicações.	-	-	-	Dynatrace	6351535
MP BA	PE 12/2023	Contratação de solução de APM, conforme condições estabelecidas neste edital e seus anexos.	Rike Is Inteligência de Software Ltda	CT 087/2023	16/07/2025	Dynatrace	6351823
Prodabel	PE 90018/2024	Promover registro de preços, pelo prazo de 12 (doze) meses, para contratação de empresa especializada em tecnologia da informação para prover serviços de solução de avaliação de performance (APM), qualidade e segurança de aplicações, bem como serviços técnicos especializados de operação e análise, conforme definições e especificações contidas no termo de referência e anexos deste edital.	IT One	ARP 954/2024	12/11/2025	Dynatrace	6351836
STF	PE 90057/2024	Aquisição de solução de monitoração de performance de aplicação (APM) na modalidade SaaS (Software as Service) para monitoração fim-a-fim do ambiente Java, PHP e componentes de infraestrutura.	VS Data	CT 172/2024	30/12/2026	Instana	6351861
TCE RJ	PE 70/2022	Aquisição da ferramenta DYNATRACE incluindo suporte, manutenção e treinamento.	Global Red Tecnologia da Informação Ltda	CT 05/2023	01/06/2026	Dynatrace	6466416
TCU	PE 13/2023	Contratação de solução de Application Performance Monitoring/Management (APM)	Security Data Tecnologia da Informação Ltda	CT 32/2023	23/08/2023	New Relic	6351889
TJ BA	PE 51/2023	Contratação de Serviços de Centro de Monitoramento e Observabilidade para o ambiente de TIC do Tribunal de Justiça do Estado da Bahia - TJBA, incluindo as ferramentas e sistemas necessários, os serviços de instalação, configuração, treinamento e suporte técnico, conforme exigências estabelecidas neste documento e em seus anexos.	Teletex	CT 08/2025	13/02/2027	App Dynamics	6351946
TJ MT	PE 30/2024	Contratação de Subscrição de Software Dynatrace de Observabilidade (Observability), Automatizado e Inteligente de Análise e Otimização Contínua do Negócio, das Aplicações e Serviços Digitais, das Experiências dos Clientes e Colaboradores, dos Logs e da Análise de Vulnerabilidades, no modelo SaaS (Software as a Service, com serviços de instalação e configuração, Capacitação Técnica (Treinamento Oficial do Fabricante), Serviços Técnicos Especializados sob demanda e o Serviço de Consultoria TAM.	Extreme Digital Consultoria e Representações Ltda	CT145/2024	19/09/2026	Dynatrace	6351962
TJ RO	PE 90080/2024	Registro de preços para eventual fornecimento de subscrições de Solução de Monitoramento de Performance de Aplicações (APM - Application Performance Monitoring/Management), na modalidade de Software como Serviço (SaaS - Software as a Service) em nuvem, incluindo suporte técnico, instalação e configuração, serviços técnicos especializados e treinamento Oficial, para atender o Tribunal de Justiça do Estado de Rondônia, conforme as disposições deste Edital e seus Anexos.	Imperial Comércio	Homologado	-	Dynatrace	6352104
		Registro de preços para contratação de empresa especializada para renovação e aquisição de subscrição de solução de					

TRF 5	PE 10/2022	monitoramento de performance de aplicações (APM) DYNATRACE, para monitoração fim a fim de aplicações JAVA, .NET e PHP hospedadas em ambientes de data center, com flexibilidade de reutilização dos agentes contratados, incluindo treinamento e suporte técnico da ferramenta para o Tribunal da 5ª Região (Órgão gerenciador) e Justiça Federal de 1ª Instância em Pernambuco (Órgão participante).	IT-One Tecnologia da Informação S.A.	2 TA CT 82/2022 CT 44/2022	16/12/2025	Dynatrace	6466416
TRT 8	PE 90046/2024	Contratação de solução de monitoramento de performance de aplicações (APM - Application Performance Management) para observabilidade automatizada e inteligente que proporciona uma visão unificada e em tempo real sobre toda a cadeia de entrega de TI da fabricante Dynatrace, na forma de subscrição, pelo período de 36 (trinta e seis meses) meses, até o limite de 60 (sessenta) meses, com serviço de implantação, para atender a demanda do TRT da 8ª Região, nos termos da tabela abaixo, conforme condições e exigências estabelecidas no ANEXO I - Termo de Referência.	IT-One Tecnologia da Informação S.A.	CT 57/2024	19/12/2027	Dynatrace	6352169
BACEN	PE 90090/2024	O objeto da presente licitação é a contratação de subscrição de licenças da solução Dynatrace, incluindo suporte, garantia técnica e de atualização e treinamento oficial, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.	Global Red Tecnologia da Informação Ltda	CT 90975/2024	28/11/2027	Dynatrace	6352175
PRODERJ	PE 10/2023	Registro de Preços para a contratação de empresa especializada em tecnologia da informação para subscrição de licenciamento de solução de Análise do Desempenho de Aplicações, incluindo a instalação e configuração, com garantia do fabricante pelo período de 12 (doze) meses (LOTE I) e para consultoria especializada e treinamento de solução de Análise do Desempenho de Aplicações pelo período de 12 (doze) meses (LOTE II), conforme as especificações contidas no Termo de Referência – Anexo I	Risk Is Inteligência de Software Ltda	ARP 07/2023	22/11/2024	Dynatrace	6352198
Estado Rondônia	PE 90099/2024	Registro de preços para futura e eventual Contratação de empresa especializada no fornecimento de solução de Observabilidade Avançada para atender as necessidades de monitoramento e diagnostico das aplicações desenvolvidas pela equipe de Desenvolvimento desta Gerência de Tecnologia da Informação e Comunicação da Secretaria de Estado de Finanças de Rondônia.	Clear IT	Homologado	-	Dynatrace	6352214
Sefaz MG	PE 105/2024	Contratação de empresa especializada no fornecimento de solução de observabilidade como subscrição de licenças, assim como instalação, configuração, treinamento e prestação de serviços especializados.	VS Data	CT 1900011228/2025	17/02/2026	Instana	6465789
TJ RJ	Adesão ARP 07/2023	Registro de Preços para a contratação de empresa especializada em tecnologia da informação para subscrição de licenciamento de solução de Análise do Desempenho de Aplicações, incluindo a instalação e configuração, com garantia do fabricante pelo período de 12 (doze) meses (LOTE I) e para consultoria especializada e treinamento de solução de Análise do Desempenho de Aplicações pelo período de 12 (doze) meses (LOTE II), conforme as especificações contidas no Termo de Referência – Anexo I	Risk Is Inteligência de Software Ltda	CT 003/221/2024	02/04/2025	Dynatrace	6465850

- **Desafios na Alocação de Recursos:** A falta de visibilidade pode dificultar a alocação eficiente de recursos para projetos, atualizações e manutenção.

Em resumo, a não contratação de uma solução de APM pode resultar em inúmeros desafios que afetam diretamente a eficiência operacional, a experiência do usuário e a capacidade de atender às demandas de um ambiente de TI em constante evolução.

Cenário 2: Aquisição de ferramenta de observabilidade incluindo suporte, garantia e atualização, operação assistida e treinamento.

A aquisição de uma ferramenta de observabilidade com suporte completo, garantia e atualizações contínuas, além de operação assistida e treinamento, traz várias vantagens significativas, mas também pode envolver desafios em termos de custos e integração. A seguir estão alguns pontos de análise para este cenário:

Vantagens:

1. **Visibilidade Completa do Ambiente:** Com a ferramenta de APM, a visibilidade sobre o desempenho das aplicações e da infraestrutura é significativamente melhorada. Isso permite identificar gargalos e problemas de forma proativa, antes que impactem a operação.
2. **Suporte e Garantia:** A inclusão de suporte técnico e garantia assegura que eventuais problemas técnicos possam ser resolvidos rapidamente, com a assistência de especialistas no produto. Além disso, as atualizações periódicas garantem que a ferramenta se mantenha atualizada com as melhores práticas e novas funcionalidades.
3. **Treinamento da Equipe:** O treinamento da equipe interna para o uso adequado da ferramenta é uma vantagem importante. Ele capacita os colaboradores a utilizarem a solução de forma eficiente, otimizar o tempo de resolução de problemas e melhor interpretar as métricas de desempenho.
4. **Maior Eficiência Operacional:** A operação assistida oferece a possibilidade de contar com a expertise de profissionais externos para configurar, monitorar e ajustar a ferramenta conforme necessário. Isso garante que o ambiente de TI seja otimizado para o desempenho máximo.
5. **Redução de Custos com Tempo de Inatividade:** Com a identificação precoce de falhas, a ferramenta ajuda a reduzir o tempo de inatividade, garantindo que os sistemas funcionem de maneira contínua e sem interrupções prolongadas, resultando em uma maior produtividade.
6. **Escalabilidade e Crescimento Planejado:** Com a visibilidade detalhada do ambiente, a escalabilidade pode ser planejada de forma mais precisa, antecipando a necessidade de recursos adicionais antes que ocorra qualquer impacto significativo na performance.

Desafios:

1. **Investimento Inicial:** O custo de aquisição da ferramenta, além do treinamento e do suporte, pode ser considerável, resultando em melhor custo-benefício a longo prazo.
2. **Integração com Sistemas Existentes:** A integração da ferramenta de observabilidade com a infraestrutura de TI existente pode exigir esforços adicionais, tanto em termos de tempo quanto de recursos técnicos.
3. **Dependência de Suporte Externo:** Embora o suporte seja uma vantagem, também pode gerar uma certa dependência externa. A empresa pode precisar ajustar suas operações e dependência de fornecedores terceirizados para manutenção e suporte da ferramenta.

Cenário 3: Aquisição de ferramenta de observabilidade incluindo suporte, garantia e atualização, treinamento e contratação de mão de obra com dedicação exclusiva.

Este cenário é ainda mais robusto, com a inclusão de profissionais dedicados exclusivamente ao monitoramento e operação da ferramenta de observabilidade. Esse cenário traz uma série de benefícios adicionais, mas também um custo mais alto em termos de mão de obra dedicada.

Vantagens:

1. **Foco Exclusivo na Operação e Manutenção:** A contratação de profissionais dedicados exclusivamente à operação da ferramenta permite uma gestão mais eficiente e contínua dos sistemas de TI. Esses profissionais podem atuar rapidamente em eventuais problemas e otimizar o ambiente constantemente.
2. **Proatividade e Antecipação de Problemas:** Profissionais exclusivos têm a capacidade de acompanhar mais de perto a performance, antecipando problemas antes que eles afetem os usuários finais. Isso resulta em uma redução significativa de falhas e de interrupções nos serviços.
3. **Maior Eficiência na Alocação de Recursos:** Com uma equipe dedicada, a alocação de recursos internos pode ser melhor direcionada, garantindo que os profissionais internos não precisem interromper suas atividades principais para lidar com questões de infraestrutura de TI.
4. **Escalabilidade e Melhoria Contínua:** A presença de uma equipe dedicada pode facilitar a escalabilidade, além de possibilitar ajustes contínuos no ambiente, garantindo que o sistema acompanhe o crescimento da demanda.
5. **Desempenho Ideal e Otimização Constante:** A equipe dedicada terá um foco constante em otimizar a infraestrutura e as aplicações, visando sempre o desempenho ideal. Isso inclui a análise constante de logs, o ajuste de configurações, a correção de falhas e a implementação de melhorias contínuas.

Desafios:

1. **Custos Elevados:** A contratação de uma equipe exclusiva envolve um custo significativo, tanto com salários quanto com benefícios. Este cenário é geralmente mais caro e pode ser inviável para empresas com orçamentos mais limitados.
2. **Gestão de Equipe Especializada:** A equipe dedicada precisará ser bem gerenciada e atualizada constantemente em relação às novas tecnologias e práticas de observabilidade. A falta de um gerenciamento eficaz pode resultar em ineficiência e subutilização.
3. **Dependência de Profissionais Internos:** Embora a equipe dedicada traga muitos benefícios, ela também cria uma dependência em relação aos conhecimentos e habilidades desses profissionais. Se houver rotatividade na equipe, a continuidade do serviço pode ser comprometida.
4. **Complexidade no Planejamento e Integração:** Adicionar uma equipe dedicada à operação da ferramenta pode criar desafios adicionais de integração com outras equipes internas da empresa, exigindo uma coordenação muito mais rigorosa.

Cenário 4: Aquisição de ferramenta de observabilidade incluindo suporte, garantia e atualização, treinamento e serviços técnicos especializados sob demanda.

Este cenário busca oferecer uma solução flexível e robusta, combinando a aquisição de uma ferramenta de observabilidade com suporte e monitoramento contínuo, treinamento da equipe, e a possibilidade de contar com serviços técnicos especializados conforme necessário. Esta abordagem oferece uma combinação entre controle interno e a capacidade de acessar expertise externa quando necessário.

Vantagens:

1. **Solução Flexível e Sob Demanda:** A contratação de serviços técnicos sob demanda permite que a equipe interna acesse especialistas quando houver necessidades específicas de personalização, configuração avançada ou resolução de problemas críticos. Isso garante que se pague apenas pelos serviços que realmente necessita, sem comprometer o orçamento com uma equipe dedicada permanente.
2. **Suporte e Garantia:** Com o suporte técnico contínuo e garantia do fornecedor, é possível garantir a resolução rápida de problemas e o funcionamento contínuo da ferramenta. Além disso, as atualizações periódicas asseguram que a solução se mantenha alinhada com as melhores práticas do mercado e novas funcionalidades.
3. **Treinamento da equipe:** O treinamento da equipe interna para o uso adequado da ferramenta é uma vantagem importante. Ele capacita os colaboradores a utilizarem a solução de forma eficiente, otimizar o tempo de resolução de problemas e melhor interpretar as métricas de desempenho.
4. **Maior Eficiência Operacional com Menor Custo:** A combinação de suporte contínuo e serviços sob demanda reduz a necessidade de contratar uma equipe interna exclusiva. A equipe técnica do STJ pode se concentrar nas suas operações principais enquanto conta com apoio especializado em momentos críticos, sem sobrecarregar os recursos internos.
5. **Escalabilidade e Flexibilidade:** Com a capacidade de contratar serviços sob demanda, o STJ pode se adaptar de forma mais ágil a mudanças nas demandas e no crescimento do ambiente de TI. Isso facilita a escalabilidade sem a necessidade de grandes investimentos em infraestrutura ou mão de obra permanente.
6. **Menor Dependência de Recursos Internos:** A solução permite que a equipe interna se concentre em suas atividades principais, enquanto a experiência externa é acessada conforme necessário para resolver problemas mais complexos, sem a necessidade de gerenciamento contínuo de uma equipe especializada interna.
7. **Integração com Sistemas Existentes:** A integração da ferramenta de observabilidade com as infraestruturas de TI já existentes pode exigir um esforço adicional, tanto em termos de tempo quanto de recursos técnicos, que podem ser mitigados com o apoio dos serviços especializados.

Desafios:

1. **Complexidade no Gerenciamento de Contratos:** A gestão de serviços sob demanda pode exigir uma coordenação mais rigorosa para garantir que a ajuda especializada seja acessada de maneira oportuna e eficiente. Além disso, pode haver desafios na definição e no controle de escopo para evitar custos inesperados.
2. **Possíveis Custos Variáveis:** Embora o modelo sob demanda seja flexível, ele pode resultar em custos variáveis dependendo da frequência com que os serviços especializados forem necessários.
3. **Dependência do Fornecedor para Serviços Especializados:** A dependência de serviços sob demanda pode gerar um risco se o fornecedor não for capaz de atender rapidamente às necessidades emergenciais ou se houver questões relacionadas à qualidade do serviço prestado.

Em resumo, o quarto cenário oferece uma solução equilibrada entre controle interno e suporte especializado externo, permitindo flexibilidade e escalabilidade. A combinação de uma ferramenta de APM com suporte contínuo e serviços sob demanda oferece o melhor de ambos os mundos: autonomia operacional e acesso a expertise quando necessário.

4.1.4 Políticas, Premissas e Especificações Técnicas Definidas para o Poder Judiciário

Não existem políticas específicas no Poder Judiciário relacionadas à sustentação do objeto deste projeto.

4.1.5 Aderência à regulamentação da Infraestrutura de Chaves Públicas Brasileira

Não se aplica. A solução possui políticas nativas de proteção e controle de acesso.

4.1.6 Premissas e especificações técnicas definidas no Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus)

Não se aplica. Trata-se de aquisição de solução de monitoramento de performance de aplicações (APM)

4.1.7 Modelos da Prestação de Serviços

Os produtos serão entregues e os serviços serão prestados nas dependências do STJ, em Brasília, Distrito Federal.

4.1.8 Orçamento Estimado

Valor estimado em R\$ 8.000.000,00, conforme DFD.

Nas próximas fases do planejamento será realizada pesquisa de preços aprofundada, com análise detalhada de contratações de outros órgãos e cotações de empresas.

4.2 Análise e comparação entre os custos totais das soluções de TIC avaliadas:

O descarte dos outros três cenários se dá por critérios técnicos e requisitos de negócio que se espera atender com a contratação da solução. Por isso, não será realizada comparação entre as soluções baseadas no custo, pois o Cenário 4 evidencia a melhor alternativa para o Tribunal.

4.3 Avaliação das necessidades de adequação do ambiente do Tribunal:

Os cenários em questão não demandam modificações na infraestrutura do Tribunal.

4.4 Justificativa da solução de TIC escolhida, considerando o ciclo de vida do objeto:

4.4.1 Descrição da solução de TIC escolhida

O processo de contratação implica na aquisição de subscrições que abrangem direitos de utilização, garantias, suporte técnico e atualizações de versões. Não está incluída a aquisição de hardware. Ao término do período contratado, o STJ possui a opção de renovar as subscrições ou encerrar o uso do produto.

A solução de TIC escolhida é o **Cenário 4** por ser a mais adequada para atender às necessidades do Tribunal de forma equilibrada e eficiente, levando em consideração a flexibilidade, custo e a complexidade do ambiente de TI, pois equilibra **eficiência operacional, custos controlados, escalabilidade e suporte técnico especializado**. Ele proporciona ao Tribunal a visibilidade necessária para melhorar o desempenho de seus sistemas, sem sobrecarregar o orçamento ou criar dependência excessiva de fornecedores externos. Esse modelo atende de forma ágil e eficaz as demandas de TI do Tribunal, permitindo

que a organização continue evoluindo com o ambiente de TI de forma planejada e segura. Os principais motivos que justificam a escolha deste cenário:

1. Flexibilidade e Custos Controlados

A opção por serviços técnicos especializados sob demanda permite que o Tribunal tenha acesso a expertise especializada apenas quando necessário, evitando a necessidade de manutenção de uma equipe interna dedicada, o que implicaria em custos recorrentes elevados. Esse modelo proporciona flexibilidade para escalar os serviços conforme a demanda, sem comprometer o orçamento com custos fixos e elevados, como no Cenário 3, que requer a contratação de uma equipe exclusiva.

2. Eficiência Operacional

Com a ferramenta de APM, o Tribunal obterá visibilidade proativa do desempenho de suas aplicações e infraestrutura, permitindo identificar e corrigir falhas de forma antecipada, o que se traduz em menor tempo de inatividade e maior produtividade. Além disso, o suporte técnico e as atualizações periódicas garantem que a solução permaneça alinhada às melhores práticas e evoluções tecnológicas, minimizando riscos de obsolescência.

3. Treinamento e Capacitação

O treinamento oferecido pela ferramenta de observabilidade capacita a equipe interna para operar e gerenciar a solução de forma eficiente. Isso não apenas melhora o tempo de resolução de problemas, mas também permite que a equipe aproveite ao máximo as funcionalidades da ferramenta, sem depender exclusivamente de fornecedores externos.

4. Escalabilidade Planejada

A visibilidade detalhada do ambiente proporcionada pela ferramenta de APM facilita o planejamento de escalabilidade, permitindo que o Tribunal antecipe necessidades de recursos adicionais à medida que o ambiente cresce. Esse planejamento de crescimento é essencial para garantir que o Tribunal esteja preparado para lidar com aumentos na demanda sem comprometer a performance ou a qualidade dos serviços prestados.

5. Menor Risco e Dependência Externa

Embora o suporte e os serviços técnicos especializados envolvam a contratação de fornecedores externos, a dependência não é tão elevada quanto no Cenário 3, onde uma equipe exclusiva seria necessária para manter a operação contínua. O Tribunal pode contar com o suporte especializado para demandas complexas, mas continua com controle sobre a operação do dia a dia, permitindo uma gestão mais eficiente dos recursos internos.

6. Custo-Benefício

O quarto cenário representa uma excelente relação custo-benefício. Comparado ao Cenário 3, que exige custos elevados com uma equipe exclusiva, o quarto cenário oferece uma solução robusta e escalável a um custo mais controlado, sem sacrificar a qualidade ou a eficiência. Além disso, a não contratação de uma equipe interna dedicada significa menos sobrecarga de gestão e maior foco nas atividades-chave do Tribunal.

7. Menor Complexidade de Implementação

A integração da ferramenta de APM no Cenário 4 não exigirá o mesmo nível de coordenação e complexidade operacional do Cenário 3, onde a presença de uma equipe dedicada exigiria um gerenciamento ainda mais apurado. A contratação de serviços especializados sob demanda reduz as dificuldades de integração e proporciona maior agilidade na implementação.

Baseada nessa análise, serão objeto dessa contratação os seguintes itens:

- Solução de APM na forma de subscrição, com suporte técnico especializado do fabricante, com ferramentas que ofereçam a capacidade de monitorar, analisar e otimizar o desempenho de aplicativos críticos para o Tribunal, garantindo uma operação eficiente e confiável dos sistemas de TI.
- Realização do processo de instalação e configuração da ferramenta de monitoramento.
- Treinamento destinado aos usuários da solução, capacitando-os a operar e gerenciar a plataforma de maneira eficaz.
- Prestação de serviços técnicos especializados para atender as demandas técnicas da unidade interna, permitindo um uso mais eficiente da ferramenta.

Além das justificativas já apresentadas, destaca-se que diversos fabricantes foram considerados durante o processo de avaliação técnica, incluindo **Dynatrace, IBM Instana, Cisco AppDynamics, Datadog e SIMON Divedot**. Foram realizadas Provas de Valor (POVs) com as principais soluções identificadas no Quadrante Mágico do Gartner, com o objetivo de validar a aderência das ferramentas aos requisitos técnicos e operacionais do STJ.

Durante essas avaliações, foi possível constatar que apenas a solução da fabricante Dynatrace atendeu integralmente aos 104 requisitos definidos no item 3.7, especialmente no que diz respeito à descoberta automática de serviços (autodiscovery), à correlação de métricas de banco de dados com as camadas de aplicação (*bind variable*), e à eficiência na coleta e correlação de métricas, logs e rastreamentos.

A funcionalidade de autodiscovery representa uma abordagem avançada de instrumentação automática, permitindo que a solução de observabilidade identifique e monitore, de forma dinâmica e contínua, todos os componentes do ambiente de TI — como hosts, contêineres, microserviços e APIs — sem necessidade de intervenção manual ou alterações no código-fonte das aplicações. Essa característica viabiliza uma instrumentação não intrusiva, em que o agente de monitoramento pode ser instalado de maneira simples e segura, sem exigir reinicializações de serviços ou modificações nas configurações dos sistemas em produção. Isso é especialmente relevante em ambientes de alta complexidade e rápida escalabilidade, como o do STJ, pois elimina a sobrecarga operacional de configuração manual, reduz riscos de falhas durante a implantação e garante maior confiabilidade e cobertura de monitoramento.

A adoção de uma solução com autodiscovery é, portanto, um fator crítico para assegurar a eficiência, agilidade e segurança na observação de ambientes distribuídos e dinâmicos, como os baseados em microserviços e Kubernetes. O cenário de microserviços e ambientes híbridos adotado pelo STJ demanda uma solução de observabilidade que ofereça automação, escalabilidade e facilidade de uso. Nesse contexto, a funcionalidade de autodiscovery representa um diferencial técnico essencial, pois permite à ferramenta identificar e instrumentar automaticamente os componentes do ambiente — como hosts, contêineres e microserviços — sem necessidade de intervenção manual, alterações de código ou reinicializações. Essa abordagem garante maior agilidade na implantação, reduz riscos operacionais e assegura cobertura completa do monitoramento, alinhando-se às exigências de ambientes complexos e em constante evolução como o do Tribunal. A solução Dynatrace, por exemplo, utiliza o OneAgent para fornecer um monitoramento profundo e automatizado, com configuração mínima e sem alterar o código-fonte das aplicações. A instalação do agente ocorre de forma simples, através da execução de apenas um arquivo instalador. Esse agente é capaz de identificar as tecnologias das aplicações e configurá-las para monitoração de forma automática, sem a necessidade de qualquer configuração manual nem apoio de outra ferramenta e instalação.

Outro requisito identificado como indispensável para a observabilidade em seu ambiente de TI a capacidade da solução de capturar e correlacionar automaticamente as variáveis de bind (*bind variable*) utilizadas em consultas SQL. Esse requisito é considerado crítico para o objeto a ser licitado, pois permite uma análise granular e contextualizada do desempenho e da segurança das transações realizadas nos bancos de dados — elemento central para o funcionamento de sistemas complexos, como os de processo judicial eletrônico. A captura de *bind variables* possibilita a identificação precisa de gargalos, comandos ineficientes e padrões de acesso que impactam diretamente a performance das aplicações. Além disso, essa funcionalidade é essencial para o rastreamento da causa raiz de problemas, permitindo que a equipe técnica atue de forma proativa e eficiente na resolução de incidentes, com base em dados reais e detalhados das interações entre aplicações e bancos de dados.

As demais soluções apresentaram limitações técnicas relevantes, como dificuldades de configuração manual, ausência de funcionalidades críticas ou não conformidade com os padrões exigidos pelo STJ. Dessa forma, a escolha pela solução da Dynatrace se justifica não apenas pela sua liderança no mercado, mas também pela efetiva capacidade de atender às necessidades específicas do Tribunal, conforme demonstrado nas avaliações práticas realizadas.

Com base no art. 41, inciso I, alínea “c” da Lei nº 14.133/2021, que permite a escolha do fornecedor com base em critérios técnicos e de desempenho, justifica-se a seleção da fabricante Dynatrace como fornecedora da solução. A Dynatrace foi a única fabricante que atendeu integralmente aos requisitos técnicos e operacionais exigidos pelo STJ, destacando-se por:

- Descoberta automática de serviços, reduzindo esforço manual e mitigando riscos operacionais;
- Monitoramento fim-a-fim de aplicações e infraestrutura com alta granularidade;
- Integração nativa com ferramentas de segurança, rede e DevOps;
- Interface intuitiva e facilidade de configuração, comprovadas durante a POV;
- Capacidade de escalar conforme o crescimento do ambiente de microserviços do STJ.

As demais soluções apresentaram limitações técnicas relevantes, como ausência de funcionalidades críticas, dificuldades de integração ou não conformidade com os padrões exigidos pelo Tribunal. Dessa forma, a escolha pela solução da Dynatrace está fundamentada em critérios técnicos objetivos, desempenho comprovado em ambiente real e aderência plena aos requisitos do STJ, garantindo a economicidade, eficiência e segurança da contratação. A solução da Dynatrace entrega a simplificação da plataforma, que buscamos, que facilita os desafios de oferecer serviços com mais rapidez em ambientes complexos, bem como a identificação célere de ocorrências e o diagnóstico precoce de indisponibilidades e vulnerabilidades.

Além dos requisitos técnicos, a contratação deve estar em conformidade com normativos que regulam a governança e a soberania de dados do poder judiciário que asseguram a integridade, a rastreabilidade e a soberania dos dados que são confiados a terceiros. A Resolução CNJ nº 335, de 29 de setembro de 2020 exige expressamente que a solução seja mantida em datacenter localizado em território brasileiro e está intrinsecamente vinculada à Política de Governança Digital do Poder Judiciário (PDPJ-Br) e à recomendação da Resolução CNJ nº 363/2021 para a preservação de dados institucionais em solo nacional. Portanto, trata-se de requisito que se descumprido, comprometeria a missão institucional do STJ.

Dessa forma, a escolha da fabricante Dynatrace está fundamentada em critérios técnicos objetivos, desempenho comprovado em ambiente real e aderência plena aos requisitos do STJ, atendendo ao disposto na Lei nº 14.133/2021 e garantindo a economicidade, eficiência e segurança da contratação.

4.4.2 Alinhamento em relação às necessidades de negócio e requisitos tecnológicos

- A solução selecionada está em conformidade com as exigências de negócios delineadas na seção 2.1 e satisfaz integralmente todos os requisitos tecnológicos descritos na seção 3.10.

4.4.3 Benefícios a serem alcançados com a solução escolhida

- A solução escolhida resultará em benefícios significativos para o STJ. O monitoramento proativo permitirá a detecção precoce de problemas de desempenho, garantindo ações corretivas imediatas antes que afetem os usuários e os processos judiciais. Além disso, a identificação eficiente de gargalos de desempenho nas aplicações possibilitará otimizações que resultarão em tempos de resposta mais rápidos e eficazes, melhorando a experiência tanto dos usuários internos quanto dos externos. A capacidade de análise de tendências oferecerá informações valiosas para aprimorar continuamente as operações do tribunal, garantindo uma entrega eficaz da justiça e um ambiente mais estável e responsivo.

4.4.4 Relação entre demanda e quantidades a contratar

Baseado no levantamento realizado no mês de abril/2025, no Processo 035932/2024 que trata da aquisição da plataforma de kubernetes, apurou-se as necessidades atuais e uma previsão de crescimento para os próximos 2 anos no ambiente.

A demanda atual da plataforma kubernetes (início de 2025):

	Gerência Managed	Produção Worker	Produção Managed	Total
Hosts	5	48	5	52
Pods	76	2.258	76	2.410
vCPUs	60	960	60	1.080
Memória (GiB)	160	8.660	160	8.980

A partir do levantamento de crescimento de ambientes, que foi realizado por meio de entrevistas com as áreas do STJ no processo citado, podemos realizar uma projeção anual considerando um crescimento linear desse ambiente:

	Tamanho atual	Crescimento anual	Crescimento em 2 anos	Tamanho em 2 anos
Hosts	52	8	17	69
Pods	2.410	464	928	3.338
vCPUs	1.080	134	269	1.349
Memória (GiB)	8.980	1.779	3.558	12.538

Foram levantados mais 2 recursos que podem ser importantes para a determinação da aquisição da subscrição do APM: workloads e Logs por dia. A quantidade de workloads nos clusters de produção e gerência, é de 846. Já a quantidade de logs foi obtida no graylog, sendo em média 28 GiB/dia nos dois clusters mencionados. A quantidade desses recursos é intimamente ligado à quantidade de Pods do ambiente. Sendo assim podemos aplicar, como previsão de crescimento de 38%.

	Tamanho Atual	Tamanho em 2 Anos
Workloads	846	1.167
Logs GiB/dia	28	39

Também foi levantada a quantidade de aplicações ativos que utilizam o ambiente Kubernetes. No Gitlab são 45 aplicações da CDES na plataforma de Kubernetes. Dado o histórico de projetos da CDES, não será considerada a tendência de crescimento de 20% anual na quantidade de aplicações do STJ como é visto no ambiente, pois percebe-se que a tendência é de as aplicações já existentes crescerem, ao invés de serem criadas aplicações.

As aplicações levantadas dependem de outros ambientes fora do kubernetes para funcionar, sendo importante que esses ambientes também sejam monitorados. Da mesma forma, não vamos considerar que tenham um crescimento significativo porque a tendência é que todas as novas aplicações sejam implantadas no ambiente de kubernetes.

Servidor de aplicação J2EE: servidor WildFly 26 com 10 instâncias 4 vCPU e 32 GB cada um:

	Atual
Hosts	10
CPUs	40
Memória (GiB)	320

Bancos de Dados: Oracle, PostgreSQL, MySQL, considerando que para cada aplicação temos ainda 1 instância de banco de dados 4CPU e 16GB:

	Atual
Hosts	45
CPUs	180
Memória (GiB)	720

Somando esses ambientes com o Kubernetes, temos:

	K8s	J2EE	DB	Total
Hosts	52	10	45	107
Pods	2.410	0	0	2.410
vCPUs	1.080	40	180	1.300
Memória (GiB)	8.980	320	720	10.020
Workloads	846	0	0	846
Logs (GiB/dia)	28	0	0	28

E finalmente, com a taxa de crescimento para 2 anos:

	Ambiente atual	Crescimento em 2 anos	Tamanho em 2 anos
Hosts	107	17	124
Pods	2.410	928	3.338
vCPUs	1.300	269	1.569
Memória (GiB)	10.020	3.558	13.578
Workloads	846	321	1.167
Logs (GiB/dia)	28	11	39

Outro levantamento realizado foi a quantidade de sessões por dia. Essa métrica foi obtida já algum tempo e pode estar discrepante com a realidade atual do ambiente. Entretanto, com as ferramentas que temos hoje, esse levantamento não é possível de ser realizado. Além disso, essa métrica pode variar já que “sessão dia” não possui regra única de cálculo pela indústria. Mas como estimativa, vamos usar o número obtido na POC da Dynatrace que é de 224.224 sessões de usuários por dia.

Considerando o conjunto de aplicações em utilização no Superior Tribunal de Justiça (STJ), informa-se que as soluções vinculadas à área judiciária serão tratadas com prioridade. Dessa forma, as aplicações que impactam diretamente a atividade-fim do Tribunal, especialmente aquelas que envolvem o trâmite processual, visualização, consulta e gestão de informações judiciais, serão priorizadas na fila de implantação, assegurando que os recursos disponíveis atendam com celeridade às necessidades da Justiça. Baseada no dimensionamento das aplicações do Sistema Justiça e na análise técnica dos ambientes envolvidos, estima-se que serão executadas de imediato 20 subscrições.

Baseado nesse levantamento estima-se que, serão necessárias 32 unidades de subscrições para atender às necessidades atuais e futuras para o ambiente do STJ. De imediato, serão executadas 20 subscrições e previsão consumo de mais 12 subscrições para atender as demandas futuras. Sendo que **cada unidade de subscrição** deverá ter a capacidade de coletar e analisar as informações de um ambiente com o seguinte dimensionamento:

Item	1 Subscrição	20 Subscrições imediatas	12 Subscrições durante vigência da Ata
Hosts Monitorados	5	100	60
Pods	82	1.640	984
CPU Monitoradas	41	820	492
Memória (GiB)	352	7.040	4.224
Workloads	26	520	312
Logs Coletados (GB/Dia)	2	40	24
Sessões de Usuários (por dia)	7.500	150.000	90.000

Considerando o conjunto de aplicações previstas para implantação no âmbito do Superior Tribunal de Justiça (STJ), informa-se que as soluções vinculadas à área judiciária serão tratadas com prioridade. Dessa forma, as aplicações que impactam diretamente a atividade-fim do Tribunal, especialmente aquelas que envolvem o trâmite processual, visualização, consulta e gestão de informações judiciais, serão priorizadas na fila de implantação, assegurando que os recursos disponíveis atendam com celeridade às necessidades da Justiça. Baseada no dimensionamento das aplicações do Sistema Justiça e na análise

técnica dos ambientes envolvidos, estima-se que serão executadas de imediato 20 subscrições.

Além de fornecer as subscrições, a Contratada deverá instalar e configurar a solução no ambiente do STJ, e oferecer um repasse de conhecimento para que os técnicos da STI possam iniciar a utilização do produto. Esses três serviços serão demandados uma única vez no início do contrato. Já para o serviço técnico especializado, foram estimadas 4.160 horas para 24 meses (2.080 horas por ano), que serão demandadas pela equipe técnica. Essas horas podem ser mais utilizadas no início do contrato e gradativamente, ao aumentar a maturidade na utilização da ferramenta, passarão a ser menos utilizadas. Essas horas serão destinadas ao atendimento das seguintes atividades:

- Serviço de Criação de Painéis;
- Serviço de Análise e Otimização de aplicações, bancos de dados e logs;
- Serviço de Análise e Recomendação de resolução de incidentes;
- Serviço de Análise e Otimização da experiência digital;
- Serviço de Análise e Otimização de vulnerabilidades;
- Serviço de Análise e Simulação de desempenho de aplicações e bancos de dados;
- Serviço de Gestão e Administração da solução.

4.4.5 Aquisição de bens x contratação como serviço

- As subscrições para soluções de APM são, em sua maioria, disponibilizadas exclusivamente por meio de modelos de subscrição. É notável que os fabricantes adotam variados métodos de licenciamento, considerando distintas características, como o número de sessões de usuários reais, a quantidade de registros de logs gerados e o escopo do ambiente (abrangendo o número de hosts, pods, namespaces, etc.).
- O custo inicial do modelo de subscrição tende a ser mais baixo, pois o Tribunal paga apenas pela licença de uso, com a manutenção e as atualizações incluídas no contrato de serviço.
- O fornecedor oferece suporte contínuo e atualizações regulares como parte do pacote de subscrição, garantindo que o Tribunal tenha acesso às versões mais recentes da ferramenta, sem custos adicionais. Isso inclui correções de bugs, melhorias no desempenho, novas funcionalidades e atualizações de segurança, assegurando que o ambiente de APM esteja sempre otimizado e protegido.
- O treinamento capacita a equipe interna do Tribunal para utilizar a ferramenta de forma eficiente e tirar o máximo proveito das funcionalidades, além de garantir uma transição mais suave e rápida para a solução.
- Ao contratar serviços, o Tribunal tem a possibilidade de requisitar serviços técnicos especializados, como personalizações, integrações complexas e análises específicas de desempenho, quando necessário. Isso permite que a ferramenta APM seja ajustada de acordo com as necessidade do Tribunal, sem a necessidade de contratar e manter uma equipe interna especializada ou depender de recursos externos para problemas específicos.

4.4.6 Contratação de mão de obra especializada para operação da ferramenta

- A análise da manutenção das soluções já implementadas foi conduzida na sessão 4.1.1. Nesse cenário, já foi evidenciada uma certa complexidade na resolução de problemas relacionados ao ambiente da forma como o ambiente vem sendo monitorado. Além disso, a importância crítica desse ambiente está aumentando devido ao processo de modernização dos sistemas administrativos e judiciais, acentuando-se assim a necessidade de uma plataforma corporativa de APM com manutenção e suporte técnico, bem como a prestação de serviços técnicos especializados para otimizar a utilização das funcionalidades e melhorar o desempenho dos sistemas.

4.4.7 Ciclo de vida do objeto:

Os profissionais destacados para prestação de serviços no STJ deverão estar informados sobre as boas práticas voltadas ao consumo consciente, redução de desperdício e coleta seletiva, com o objetivo de contribuir para a preservação do meio ambiente e dos recursos públicos.

A CONTRATADA deverá adotar as normas federais, estaduais e distritais e declarar ter conhecimento da Política de Sustentabilidade do STJ, dando cumprimento aos dispositivos da Instrução Normativa STJ/GDG 15, de 12 de novembro de 2020. Os seus profissionais deverão estar informados sobre as boas práticas voltadas ao consumo consciente, à redução de desperdício e à coleta seletiva, com o objetivo de contribuir para a preservação do meio ambiente e dos recursos públicos.

4.5 Sustentação do contrato:

4.5.1 Recursos Materiais:

Recurso	Qtde	Disponibilidade	Ação para obtenção do Recurso	Responsável
Infraestrutura tecnológica (servidores de rede, sistema operacional, servidores de aplicação e de banco de dados, rede de comunicação de dados, link internet)	Deve ser avaliada a quantidade de servidores quando da ativação do serviço.	Ambiente tem que estar disponível quando da assinatura do contrato.	O recurso já existe no STJ	STI

4.5.2 Recursos Humanos:

Função	Formação	Período	Atribuições
Gestor e Fiscais do Contrato	Designados por Portaria	Assinatura do Contrato	Fazer reunião inicial com a CONTRATADA para alinhamento da execução contratual, apresentação das equipes responsáveis pela execução e fiscalização, análise dos pontos críticos da execução e levantamento de fatores que possam impactar a execução do objeto.

Fiscais Requisitantes, Técnicos e Administrativo	Designados por Portaria	Da assinatura até o fim da vigência contratual. Recebimento provisório da Instalação e Configuração	Repassar as informações técnicas para elaboração do plano de implantação. Receber o plano de implantação, analisar e propor as correções técnicas necessárias se for o caso. Aprovar o plano de implantação, com os ajustes propostos. Acompanhar a instalação da solução. Apoiar as comissões de recebimento quanto a quesitos técnicos. Controlar o prazo para entrega da solução. Receber e conferir os objetos entregues se em conformidade com a proposta aprovada. Emitir documentos de não conformidade, em caso de objetos divergentes. Emitir termo de recebimento provisório, identificando os bens entregues, cumprimento dos prazos contratados e atestando a conformidade com a proposta.
Comissão de Recebimento Definitivo	Designada por Portaria	Recebimento definitivo da Instalação e Configuração	Acompanhar e controlar os prazos contratados previstos para cada etapa de execução, até a emissão do Termo de Recebimento Definitivo. Fiscalizar o processo de instalação e configuração. Emitir documentos de não conformidade, em caso de divergência observada. Acompanhar os testes de compatibilidade da solução com as especificações técnicas do Edital. Conferir, validar e aprovar os produtos e serviços executados. Atestar a instalação e configuração mediante emissão de Termo de Recebimento Definitivo.
Fiscais Requisitantes e Técnicos	Designados por Portaria	Recebimento provisório dos serviços de manutenção e suporte técnico até fim de vigência do contrato	Acompanhar e fiscalizar a execução dos serviços e anotar em registro próprio todas as ocorrências relacionadas com a execução, sob os aspectos quantitativos e qualitativos, comunicando as ocorrências de quaisquer fatos que exijam medidas corretivas por parte da empresa. Determinar as datas e os horários para realização das manutenções, prevendo o mínimo de impacto nas atividades dos usuários. Abrir chamados para solicitação de suporte. Analisar e verificar se os níveis de qualidade contratados foram alcançados e aplicar as glosas estipuladas para cada caso. Consolidar mensalmente, emitir e encaminhar os Relatórios de Serviços para providências de faturamento.
Gestor do Contrato	Designado por Portaria	Vigência Contratual	Atestar a nota de cobrança encaminhada pela empresa e enviar, juntamente, com as Ordens de Serviços e os Relatórios de Atividades, à área administrativa para providências. Autorizar a aplicação das glosas/descontos propostas pelos fiscais. Encaminhar a documentação comprobatória de penalizações ou multas administrativas para os setores responsáveis e solicitar providências.

4.5.3 Continuidade da Solução de TIC

A continuidade de prestação dos serviços de suporte é um dos objetivos principais da contratação proposta.

Evento	Tipo de Ação	Ação	Responsáveis
	Preventiva	Acompanhamento do cumprimento das obrigações contratuais.	Comissões de Recebimento e Gestor do Contrato

Inexecução ou má prestação nos serviços de manutenção pela CONTRATADA	Preparação	Reunir equipe de planejamento para contratação, preparando nova documentação para licitação de empresa que possa dar continuidade na manutenção ou no fornecimento de nova solução substituta.	Fiscal Técnico, Gestor do Contrato
	Contingência	Avaliar possibilidade de contratação de empresa remanescente da licitação. Iniciar ações para contratação emergencial. Preparar documentação para nova licitação	Fiscal Técnico e Gestor do Contrato
Falência da empresa ou rescisão por descumprimento de obrigações contratuais (inexecução total do contrato)	Preventiva	Acompanhamento das sanções/multas administrativas no decorrer do contrato. Verificar junto à CONTRATADA sua qualificação econômico-financeira, que minimize a ocorrência do risco de falência da empresa.	Gestão do contrato e SAD
	Preparação	Desenvolvimento de novo edital para contratação de outra empresa.	Equipe de Planejamento e SAD
	Contingência	Contratação emergencial de empresa especializada para as manutenções corretivas.	Gestor do Contrato, CIEP, STI e SAD
Encerramento normal do Contrato	Preventiva	Por se tratar de ambiente crítico que necessita de manutenção continuada, preventiva e reativa, preparar nova contratação para dar continuidade aos serviços de manutenção.	Fiscal Técnico, Gestor do Contrato
	Preparação	Desenvolvimento de edital para nova contratação.	Equipe de Planejamento da Contratação e Gestor do Contrato
	Contingência	Contratação emergencial de empresa especializada para as manutenções corretivas.	Gestor do Contrato, CIEP, STI, SAD e AJU

4.5.4 Transição contratual

4.5.4.1 Avaliação de Continuidade Contratual

Ação	Formação	Início	Final
Avaliar mensalmente os serviços prestados no período e os resultados obtidos, efetuando os descontos, descon siderações e multas necessárias quando for o caso, para resultados não conformes.	Fiscais e Gestor do Contrato	Assinatura do Contrato	Encerramento da Vigência
Acompanhar os serviços e exigir a transferência de conhecimento entre as equipes de colaboradores técnicos e a CONTRATADA.	Fiscal Técnico	Assinatura do Contrato	Encerramento da Vigência

Por ser uma solução de mercado consolidada e robusta, presente no mercado há vários anos, líder no Quadrante Mágico do Gartner, adotada por diversas entidades privadas e públicas no mundo todo, o risco é mínimo em relação ao atendimento do produto, visto que a disponibilização e o suporte serão realizados pelo fabricante após a entrega da subscrição. No caso de descontinuidade do atendimento por parte da contratada, haverá necessidade de realizar novo procedimento licitatório para continuidade da contratação.

4.5.4.2 - Ações para Encerramento Contratual

Ação	Formação	Início	Final
Analisar a existência de atualização de versionamentos, fixes e evoluções dos softwares e hardwares da solução e solicitar as correções finais.	Fiscal Técnico	30 dias antes do fim da vigência do contrato	Encerramento da Vigência
Executar a transferência de conhecimento entre as equipes de colaboradores técnicos do atual fornecedor de serviços para a nova CONTRATADA, de forma a minimizar a possibilidade de interrupção ou degradação na operação e prestação desses serviços no âmbito do STJ.	Fiscais e Gestor do Contrato	30 dias antes do fim da vigência do contrato	Encerramento da Vigência
Os custos de desmobilização para encerramento do contrato correrão por conta da CONTRATADA.	Gestor do Contrato	Dia seguinte ao encerramento do contrato	Devolução da garantia contratual
Elaborar documentos e avisos para comunicar à STI e à Central de Suporte que a CONTRATADA não possuirá mais acesso para manutenção no ambiente do STJ.	Gestor do Contrato	30 dias antes do fim da vigência do contrato	Dia seguinte ao encerramento do contrato
Efetuar descadastramento das contas de serviço da empresa, impedindo acesso às instalações e equipamentos da STI.	Fiscal Técnico	Dia seguinte ao encerramento do contrato	Dia seguinte ao encerramento do contrato
Garantir que todas as manutenções previstas no plano até a data de encerramento do contrato sejam atualizadas.	Fiscais Técnico	30 dias antes do fim da vigência do contrato	Encerramento da Vigência
Solicitar à administração a liberação da garantia contratual.	Gestor do Contrato	Encerramento do Contrato	Dois meses após encerramento do contrato

Atividades de encerramento contratual consistirão em:

- a. Apresentação de relatório sobre o estado da solução com indicações de possíveis problemas e recomendações;
- b. Remoção dos acessos das contas de suporte da empresa contratada;
- c. Não se aplica ao objeto a devolução de recursos materiais ou eliminação de caixas postais;
- d. Desinstalar os agentes do ambiente;
- e. Excluir as regras de firewall que permitiam os acessos à internet.

A transição contratual incluirá, pelo menos, as seguintes atividades:

- a. Inclusão no plano de aquisições de previsão de contratação ou renovação da solução;
- b. Elaboração e acompanhamento do processo de contratação, com os artefatos necessários.

No encerramento do contrato, atingido o limite estipulado por lei, haverá interrupção do serviço após 30 dias, em caso de não renovação. Neste caso, todos os dados deverão ser copiados/migrados para outra infraestrutura com a configuração da ferramenta até que haja outra contratação.

4.5.5 Estratégia de Independência

4.5.5.1 Transferência de conhecimento

Atividade	Forma de Transferência
Documentação do projeto da solução	Documentação atualizada do projeto da solução, compartilhada entre todos os integrantes da equipe.
Encontro de alinhamento Técnico	Realização de encontros técnicos, quando necessário, com a equipe técnica do CONTRATANTE responsável pela gestão da solução, para a transferência de conhecimento acerca das atividades.
Procedimento de instalação e configuração	Todas as instalações, configurações e manutenções deverão ser registradas e documentadas em procedimentos internos, para que possam ser reproduzidos e divulgados com a equipe técnica.
Descrição das entregas de serviços	Todas as construções de produtos através da prestação de serviços deverão ser entregues acompanhadas de descrição completa, para documentação técnica e regras de negócio.
Descrição das informações que deverão ser transmitidas pela contratada	Documentar em base de conhecimento do STJ todos os procedimentos, ocorrências e orientações que façam parte das melhores práticas de uso dos serviços objeto da contratação.
Relatório de atividades	Em todo atendimento para manutenções no ambiente, deverá ser entregue um relatório com a descrição da atividade realizada.
Direitos de Propriedade Intelectual	Todos os produtos advindos da execução contratual, incluindo, porém não se limitando a, documentos descritivos da solução, diagramas de conexão, “as-builts”, rotinas de migração e rotinas computacionais desenvolvidas, são de propriedade exclusiva do STJ. Tais produtos deverão ter tratamento confidencial por parte da CONTRATADA, que não poderá divulgá-las a terceiros sem o expresse consentimento do Tribunal.

Para alguns fabricantes, é possível a utilização do software da ferramenta na versão Community conforme as orientações e diretrizes do Conselho Nacional de Justiça para utilização de software open source (de código aberto), mesmo fora da plataforma de subscrição/licenciamento almejada. Entretanto, o software ficaria sem suporte técnico, sem manutenção de falhas ou inconformidades, colocando assim em risco os requisitos de disponibilidade e segurança e evolução dos serviços disponibilizados aos cidadãos e colaboradores do Superior Tribunal de Justiça.

Ainda, as atividades e recursos humanos necessários para manter a solução em funcionamento e atendendo a todos os requisitos de segurança, manutenções corretivas e evolutivas, ocasionarão relocação de servidores com dedicação exclusiva, bem como aumentará o custo de suporte por equipe interna ao invés da contratação de empresa especializada.

A vantagem da solução em nuvem é que ela permite que o STJ disponha de recursos e conhecimentos do fabricante/fornecedor para resolução dos problemas ou suporte técnico necessários para a manutenção da ferramenta, além do atendimento imediato quando solicitado.

4.6 Estimativa das quantidades a serem contratadas:

Conforme justificado no item 4.4.4, a demanda imediata é de 20 subscrições e para atender ao crescimento, sugere-se registrar 32 subscrições.

ITEM	DESCRIÇÃO	QUANTIDADE
1	Subscrição da ferramenta Dynatrace de observabilidade no Modelo SaaS com suporte técnico 24x7, garantia e atualização por um período de 24 (vinte e quatro) meses	32 subscrições
2	Serviço de implantação e configuração da solução	20 subscrições
3	Repasse de conhecimentos	15 pessoas
4	Serviço técnico especializado (sob demanda)	4.160 horas (2.080 horas/ano)

4.7 Estimativa do valor da contratação:

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Subscrição da ferramenta Dynatrace de observabilidade no Modelo SaaS com suporte, garantia e atualização por um período de 24 (vinte e quatro) meses	Subscrição	32	R\$ 566.890,00	R\$ 18.140.480,00
2	Serviço de implantação e configuração da solução	Subscrição	20	R\$ 30.605,00	R\$ 612.100,00
3	Repasse de conhecimentos	Unidade	15	R\$ 6.006,25	R\$ 90.093,75
4	Serviço técnico especializado, sob demanda	Horas	4.160 horas (2.080 horas/ano)	R\$ 341,70	R\$ 1.421.472,00
VALOR TOTAL					R\$ 20.264.145,75

As fontes utilizadas na pesquisa estão descritas no documento STI - Fontes da Pesquisa e Análise Crítica dos Preços (6669226), bem como a análise crítica dos preços estimados.

O valor total estimado é de R\$ 20.335.739,50 (vinte milhões, trezentos e trinta e cinco mil, setecentos e trinta e nove reais e cinquenta centavos), conforme Planilha de Avaliação de Pesquisa de Mercado (6669221).

4.7.1. Responder este item somente para as contratações abaixo de R\$ 80.000,00 (se a adjudicação for por item, esse valor deve ser considerado para cada item):

- () A licitação pode ser destinada exclusivamente à empresas ME/EPP conforme estabelece o inciso I do art. 48 da [LC 123/2006](#).
- () A licitação deverá ser de ampla participação em razão de não haver um mínimo de 3 (três) fornecedores competitivos enquadrados como microempresas ou empresas de pequeno porte sediados local ou regionalmente e capazes de cumprir as exigências estabelecidas no instrumento convocatório. **Justificativa:** *o usuário deverá demonstrar essa excepcionalidade na instrução processual.
- () A licitação deverá ser de ampla participação em razão do tratamento diferenciado e simplificado para as microempresas e empresas de pequeno porte não ser vantajoso para a administração pública ou representa prejuízo ao conjunto ou complexo do objeto a ser contratado. **Justificativa:** *o usuário deverá demonstrar essa excepcionalidade na instrução processual.
- () Não se aplica em razão da licitação ser dispensável ou inexigível.

4.8 Justificativa para o parcelamento ou não da solução:

- () Não se aplica em razão da licitação ser dispensável ou inexigível.
- () Não é possível o parcelamento, pois trata-se de apenas 1 (um) item (ADJUDICAÇÃO: () MENOR PREÇO ou () MAIOR DESCONTO).
- () É possível a contratação da solução de forma divisível observado o §2 do art. 40 da [Lei n. 14.133/2021](#) (ADJUDICAÇÃO: () MENOR PREÇO POR ITEM ou () MENOR PREÇO POR LOTE ou () MAIOR DESCONTO POR ITEM).
- (X) Todos ou alguns itens da solução devem ser agrupados para o fornecimento por uma única empresa, observado o §3 do art. 40 da [Lei n. 14.133/2021](#) (ADJUDICAÇÃO: (X) MENOR PREÇO GLOBAL ou () MENOR PREÇO POR LOTE ou () MAIOR DESCONTO GLOBAL). **Justificativa:** Trata-se de uma solução. Todos os itens são interdependentes e precisam ser compatíveis. Também precisam ser entregues ao mesmo tempo. Se um dos itens fracassar, o objeto da contratação não será alcançado.

4.9 Contratações correlatas e/ou interdependentes:

Não há.

4.9.1 Existe um contrato atual vigente ou instrumento equivalente, com objeto a ser licitado?

- (X) Não. () Sim. O contrato atual (n. ____/20____) (Processo SEI n._____) terá sua vigência finda em ____/____/20____.

4.10 Alinhamento entre a contratação e o Pcaq:

() O objeto pretendido não consta do PCAq. **Justificativa:**

(X) O objeto pretendido consta do PCAq no item STI2025-106 da planilha.

4.11 Alinhamento entre a contratação e outros instrumentos de planejamento institucional:

Plano Estratégico Institucional - PLANO STJ 2021-2026		
Perspectiva	Objetivo Estratégico	
Aprimorar a Governança Institucional	Intensificar o uso de tecnologia da informação	
Intensificar o uso de tecnologia da informação		
Plano Estratégico de Tecnologia da Informação e Comunicação - PDTIC 2025-2026		
Objetivo Estratégicos	Ações Táticas	Projeto
OE01 Evoluir e manter a infraestrutura de ativos tecnológicos	AT01.01 Sustentar a infraestrutura de TIC e buscar soluções tecnológicas inovadoras AT06.01 Aprimorar a continuidade de serviços de TIC	Projeto Previsto: Atualização de infraestrutura - ciclo 2025
OE06 Fortalecer as estratégias de continuidade de TIC		
Plano Operacional de Tecnologia da Informação e Comunicação - PLANOP 2025-2026		
Código Operacional	Descrição	
A definir no PDTIC 2025-2026	Geral: Demanda oriunda do exercício de 2024 (Código STI2024-009)	

4.12. Classificação do objeto:**Natureza:**

(X) bens e serviços comuns: aqueles cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado;

() bens e serviços especiais: aqueles que, por sua alta heterogeneidade ou complexidade, não podem ser considerados bens e serviços comuns. **Justificativa:**

Tipo de bem (apenas para serviço com fornecimento de bens de consumo):

(X) O objeto desta contratação se enquadra como sendo bem de consumo de qualidade comum, uma vez que estão presentes as características estabelecidas nos incisos II e III do § 1º do art. 22 da [Instrução Normativa STJ/GDG n. 4/2023](#).

() O objeto desta contratação se enquadra como sendo de bem de consumo de luxo, conforme art. 2º, I, do [Decreto n. 10.818, de 27 de setembro de 2021](#), e art. 22, I, da [Instrução Normativa STJ/GDG n. 4/2023](#). **Justificativa:**

Caracterização:

(X) Trata-se de serviço ou fornecimento contínuo, definido pela [Instrução Normativa STJ/GDG n. 10 de 28 de abril de 2022](#), alterada pela [Instrução Normativa STJ/GDG n. 5 de 16 de fevereiro de 2023](#).

() Trata-se de serviço ou fornecimento contínuo, AINDA NÃO definido pela [Instrução Normativa STJ/GDG n. 10 de 28 de abril de 2022](#). Nesse caso, o enquadramento deve ser autorizado pela/o titular do cargo de Diretor-Geral.

() O objeto é caracterizado como serviço não contínuo ou contratado por escopo, aquele que impõem ao contratado o dever de realizar a prestação de um serviço específico em período predeterminado, com valor acima do limite previsto para a dispensa de licitação (art. 75, incisos I e II da [Lei 14.133/2021](#)).

4.13 Participação de empresas reunidas em consórcio:

(X) Não será permitida a participação de empresas reunidas em consórcio. **Justificativa:** O objeto a ser contratado não possui condições técnicas complexas que exijam a atuação de mais de uma empresa para prestação dos serviços, uma vez que não exige junção de esforços de segmentos distintos destinados à sua prestação. Trata-se de serviços comumente prestados por diversas empresas que atuam individualmente no mercado.

() Será permitida a participação de empresas reunidas em consórcio. **Justificativa:**

4.14 Participação de pessoa física:

(X) Não.

() Sim. **Justificativa:**

5. Planejamento**5.1 Resultados pretendidos:**

1. Solução moderna, segura e dimensionada para atender as demandas para os próximos cinco anos.
2. Acompanhar o crescimento das aplicações críticas Tribunal.
3. Redução na quantidade e duração das indisponibilidades.
4. Melhora do desempenho (maior estabilidade).
5. Monitoramento completo do ambiente, capaz de acelerar a resolução de problemas.
6. Redução de Custos Operacionais - Redução significativa nos custos operacionais, pois permite a identificação precoce de problemas de desempenho e a otimização eficiente dos recursos de infraestrutura.
7. Aumento da Eficiência da Equipe - Com a automação de monitoramento e alertas proativos, toda a equipe de TI pode alocar seu tempo e esforço de

maneira mais eficaz, respondendo rapidamente a incidentes críticos e dedicando menos tempo a tarefas manuais de diagnóstico.

8. Menos Tempo de Inatividade - Ao antecipar problemas de desempenho, o Tribunal pode minimizar o tempo de inatividade dos sistemas, garantindo a continuidade das operações judiciais sem interrupções significativas.
9. Aumento da Produtividade dos Funcionários - Um ambiente de TI estável e responsivo proporciona aos funcionários do tribunal as ferramentas necessárias para realizar suas tarefas com eficiência, melhorando a produtividade geral.
10. Utilização Otimizada de Recursos de Hardware - O APM pode ajudar a identificar recursos de hardware subutilizados ou sobrecarregados, permitindo um dimensionamento adequado e uma melhor alocação de recursos.
11. Planejamento Orçamentário Mais Eficiente - Com informações claras sobre o desempenho dos aplicativos e tendências de uso, o Tribunal pode planejar seu orçamento de TI de maneira mais precisa e eficiente.
12. Melhoria da Experiência do Usuário - Uma experiência do usuário aprimorada resulta em maior satisfação dos clientes e partes envolvidas no sistema judicial.
13. Maior Conformidade e Transparência - O APM pode ajudar a manter a conformidade com regulamentações e normas internas, garantindo a transparência nas operações do tribunal.
14. Tomada de Decisões Baseada em Dados - As análises de desempenho fornecidas pelo APM permitem que a administração do tribunal tome decisões estratégicas com base em dados sólidos, em vez de suposições.

Os resultados técnicos a serem alcançados com esta contratação estão no seguinte escopo:

INFRAESTRUTURA

- Monitoramento do uso das aplicações pelos seus usuários, subsidiando análises gerais de comportamento que auxiliem nas alterações de infraestrutura, sistemas e procedimentos;
- Coleta de dados de logs, métricas e traces das aplicações e infraestrutura em um ambiente unificado de visualização, com a capacidade de correlacionar os itens de configuração no ambiente, permitindo o monitoramento em tempo real de todo o percurso das requisições e respostas até o usuário final;
- Identificação pontos de gargalos e indisponibilidade, incluindo os sistemas necessários ao funcionamento das aplicações internas como Banco de Dados, Gerenciador de Filas, etc;
- Identificação das queries de banco de dados que causam lentidão e em qual contexto elas foram são executadas, mostrando desde o pedido do usuário, até a resposta do banco de dados;
- Categorização e priorização dos problemas pelo grau de impacto aos usuários, aplicações e à infraestrutura;
- Resolução de problemas de performance e disponibilidade;
- Obtenção de alertas de degradação e indisponibilidade das aplicações e infraestrutura permitindo a atuação anterior às notificações dos usuários;
- Obtenção do roteamento de qualquer transação, não importa o caminho;
- Obtenção do histórico das monitorações até o indispensável para uma análise das causas de problemas;
- Descoberta automática da topologia deverá trazer informações de logs, traces, métricas, correlacionamento e dependências de componentes de hardware e aplicações em servidores físicos, virtualizados e ambiente de contêineres no Kubernetes sem a necessidade de intervenção manual, exceto em casos específicos justificados pelo fabricante do produto;
- A ferramenta deve receber atualizações regulares para corrigir falhas de segurança e vulnerabilidades, mantendo um ambiente seguro;
- Implementação automática dos seus agentes, onde novas versões são baixadas e instaladas sem a intervenção humana;

DESENVOLVIMENTO

- Identificação de vulnerabilidades de segurança em aplicações enquanto elas estão sendo executadas – problemas como necessidade de atualização de bibliotecas, injeções de código, configurações inadequadas de segurança a nível de código;
- Deverá permitir o detalhamento (drill down) para facilitar a análise do comportamento das aplicações;
- Tecnologias de desenvolvimento de sistemas a serem consideradas: Java, Spring, Angular, JBOSS, Wildfly, Python;
- Suporte a Microsserviços e Arquitetura Baseada em Nuvem: a ferramenta deve oferecer suporte para ambientes distribuídos e dinâmicos;
- Recursos de IA e Machine Learning: Essa ferramenta deve possuir recurso de inteligência artificial para detectar anomalias automaticamente, prever possíveis falhas e melhorar a análise de dados.

INTEGRAÇÃO COM SISTEMA EXTERNOS AO STJ

- Identificação de latência nos ativos relacionados a integração com sistemas externos ao STJ que utilizam a extranet (Infovia do STJ, Serpro, etc);
- Instalação de agentes em ambientes externos ao STJ.

SEGURANÇA

- A solução deve permitir a detecção automática e em tempo de execução, de vulnerabilidades nas aplicações sem a necessidade de configuração prévia de escaneamentos periódicos, utilizando o mesmo agente único.

Em resumo, a não contratação de uma solução de APM pode resultar em inúmeros desafios que afetam diretamente a eficiência operacional, a experiência do usuário e a capacidade de atender às demandas de um ambiente de TI em constante evolução.

Em vista dos desafios enfrentados atualmente devido à falta de monitoramento adequado das aplicações, a aquisição de uma ferramenta de *Application Performance Monitoring* (APM) se torna uma prioridade para o STJ.

Em face da complexidade do atual ambiente de produção a adoção desse tipo de suporte facilitará na identificação e ação das equipes na causa raiz do problema num menor tempo possível.

Essa medida não apenas abordará os problemas de desempenho existentes, mas também estabelecerá uma base sólida para a eficiência contínua e aprimoramento das operações do tribunal, restabelecendo rapidamente o funcionamento dos sistemas, garantindo a entrega eficaz da justiça à sociedade.

A ausência de um sistema de monitoramento abrangente que tem levado a dificuldades na detecção de problemas de desempenho, na identificação de gargalos e uma resposta lenta na resolução de problemas relacionados às aplicações de microserviços utilizadas no tribunal, afetando negativamente a experiência dos usuários e a eficiência profissional.

Portanto, a aquisição dessa ferramenta é essencial para identificar as falhas nos ambientes monitorados, bem como coletar, armazenar e disponibilizar métricas de desempenho, além da emissão de relatórios gerenciais para a descoberta da causa raiz de um problema no ambiente de rede e produção.

5.2 Providências a serem adotadas pela Administração para início da execução do objeto:

A solução em questão não demanda modificações na infraestrutura do Tribunal.

5.3 Possíveis impactos ambientais:

I – Critérios:

5.3.1 A fabricante e/ou distribuidora, e/ou importadora, e/ou comerciante e/ou consumidora deste objeto deve possuir Cadastro Técnico Federal de Atividades Potencialmente Poluidoras e/ou Utilizadoras de Recursos Ambientais (CTF/APP)?

a) ☐ Sim. A fabricante, e/ou distribuidora, e/ou importadora, e/ou comerciante, e/ou consumidora deste objeto se enquadra nas FTEs do CTF/APP.

b) ☒ Não. A fabricante, e/ou distribuidora, e/ou importadora, e/ou comerciante, e/ou consumidora deste objeto não se enquadra nas FTEs do CTF/APP.

5.3.2 A escolha foi por produtos/objetos constituídos de material (marque quantos itens forem necessários):

☐ renovável ☐ reciclado ☐ atóxico ☐ biodegradável ☐ outros: _____ ☒ não se aplica

5.3.3 Os objetos da aquisição devem estar em conformidade com os seguintes regulamento(s) técnico/legal: (marque quantos itens forem necessários):

- ☐ Etiqueta Nacional de Conservação de Energia
- ☐ Selo Ruído
- ☐ Comprovação de origem de produto de origem florestal (ex: Selo FSC ou Selo CERFLOR)
- ☐ Documento de Origem Florestal (DOF) - Transporte e armazenamento
- ☐ Ficha de Informações de Segurança de Produtos Químicos (FISPQ)
- ☐ Autorização de Funcionamento de Empresa (AFE)
- ☐ Requisitos de Avaliação de Conformidade (RAC) para bens de informática - [Portaria INMETRO n. 170/2012](#)
- ☐ Diretiva RoHS
- ☐ Autorização para o Exercício da Atividade de Revenda de GLP
- ☐ Outro(s). Especificar: _____

Deverão ser consideradas nesse item as diretivas do Guia de Licitações Sustentáveis da AGU, normativos internos e a legislação vigente.

II – Plano de Logística Sustentável do STJ (PLS-STJ):

5.3.4 Essa aquisição ou contratação demandará ou resultará em (marque quantos itens forem necessários)

- ☐ geração de resíduo.
- ☐ consumo de papel.
- ☐ consumo de outros materiais de expediente (caneta, grampos, clips, pastas etc).
- ☐ consumo de café ou açúcar.
- ☐ consumo de água mineral envasada.
- ☐ instalação de computador ou impressora.
- ☐ aparelho de telefone fixo ou móvel.
- ☐ consumo de energia elétrica.
- ☐ consumo de água.
- ☐ serviços de engenharia (instalações elétricas, hidráulicas, ponto de rede, ponto de telefone, divisórias).
- ☐ obras civis (reforma ou construção de edificação).
- ☐ serviço de limpeza - aumento da área a ser limpa no STJ.
- ☐ serviço de vigilância - aumento no número de postos.
- ☐ aumento na quantidade de veículos na frota do STJ.
- ☐ gasto com contratos de veículos (manutenção, peças, insumos, seguro, lavagem, terceirização, exceto motorista).
- ☐ consumo de combustível.
- ☐ ação de qualidade de vida.
- ☐ ação de capacitação socioambiental.
- ☒ não demandará ou resultará em nenhum dos itens acima.

Esses itens referem-se aos temas monitorados pelo PLS-STJ. A partir da seleção do item e da análise realizada pela AGS, caso confirmado impacto relevante no PLS-STJ, a gestora ou o gestor do indicador será comunicado para ciência e eventual inclusão no respectivo plano de ação.

III – Resíduos:

5.3.5 Gestão de resíduos

a) Há previsão de geração de resíduos?

(Observar todos os resíduos gerados pela aquisição e/ou contratação: embalagens, resíduos de instalação, dentre outros, inclusive quanto aos objetos no final do seu ciclo de vida):

() Sim. (X) Não.

b) Se sim, a destinação ambientalmente adequada dos resíduos será de responsabilidade:

() da CONTRATADA () do STJ

Descreva a destinação (se pela contratada, analisar os possíveis custos):

c) Descreva os resíduos que serão produzidos - sua natureza, se são classificados como resíduos perigosos (item 3 do Plano de Gestão de Resíduos Sólidos do STJ), e quando possível, incluindo estimativa de quantidade:

d) Você identifica outros impactos ambientais, além dos indicados acima? (art. 7º, inciso XII, [IN ME n. 40/2020](#)):

(X) Não. () Sim.

Descreva:

6. Viabilidade

6.1 Existe Ata de Registro de Preços em vigor que pode atender a demanda?

(X) Não. () Sim. Justificar a viabilidade técnica e econômica para a adesão:

6.1.1 A demanda poderá ser atendida por Ata de Registro de Preços?

() Não. (X) Sim. Justificar:

O APM será utilizado no ambiente de microsserviços. Esse ambiente cresce rapidamente com a criação de novos serviços e a migração de serviços legados (cliente servidor e JBoss) para lá. O crescimento é um fato e não vai parar nos próximos cinco anos. O uso do instrumento da ata de registro de preços permite atender essa demanda futura de forma rápida e com menor custo para a Administração Pública.

Outro benefício da ata de registro de preços é o uso mais eficiente e racional dos recursos públicos, já que a equipe de TI pode solicitar novas subscrições em sintonia com o crescimento do ambiente. Evita-se assim a aquisição antecipada de subscrições que ficariam ociosas por um tempo. Através da ata será possível garantir que o STJ pagou somente pelas subscrições efetivamente sendo utilizadas.

A EPC entende que a ata de registro de preços propicia economia, agilidade, uso mais eficiente do recurso público e, mais importante, garante o correto funcionamento do APM mesmo com o crescimento da infraestrutura.

Ademais, poderá atender a manifestação de interesse em participar da contratação apresentada pelo CJF (SEI [4023084](#)) fundamentado pelo inciso III, do art. 3º do DECRETO Nº 11.462, DE 31 DE MARÇO DE 2023, que regulamenta os art. 82 a art. 86 da Lei nº 14.133.

6.2 Previsão de recursos para a demanda:

(X) A contratação foi prevista na Proposta Orçamentária de 2025, na Ação: 4236 - Apreciação e Julgamento de Causas.

() Não houve previsão orçamentária para contratação.

6.3 Declaração de viabilidade:

A Equipe de Planejamento da Contratação declara a adequação da solução à necessidade e à realidade do Tribunal, sendo essencial para manutenção e bom funcionamento das soluções de TIC do Tribunal, de forma segura e eficiente.

7. Do Acesso às informações contidas no presente Estudo Preliminar:

Nos termos da [Lei n. 12.527, de 18 de novembro de 2011](#), esta unidade ou Equipe de Planejamento entende que:

(X) As informações contidas no presente Estudos Técnico Preliminar **DEVERÃO SER PÚBLICAS, estando disponíveis** para qualquer pessoa interessada, pois não se caracterizam como sigilosas.

() As informações que não tenham caráter sigiloso serão disponibilizadas na plataforma de Governança Digital Colaborativa do Poder Judiciário (Connect-Jus), conforme a [Resolução CNJ n. 468, de 15 de julho de 2022](#).

() As informações contidas nos itens _____ do presente Estudo Técnico Preliminar **ASSUMEM CARÁTER SIGILOSO**, nos termos do art. 23 da [Lei n. 12.527/2011](#), e, portanto, deverão ter acesso restrito. **Justificativa:**

() As informações contidas no presente Estudo Técnico Preliminar **ASSUMEM CARÁTER SIGILOSO**, nos termos do art. 23 da [Lei n. 12.527/2011](#), e, portanto, deverão ter acesso restrito. **Justificativa:**

8. Responsabilidade das servidoras e/ou dos servidores ou equipe de planejamento da contratação responsáveis pela elaboração e conteúdo do ETP:

Certificamos que somos responsáveis pela elaboração do presente documento que compila os Estudos Técnicos Preliminares e que este traz os conteúdos previstos na [Lei n. 14.133/2021](#).



Documento assinado eletronicamente por **Tiemi Umebara, Assistente IV**, em 30/10/2025, às 15:59, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Daniel de Souza Vasconcelos, Analista Judiciário, Área de Apoio Especializado - Suporte em Tecnologia da Informação**, em 30/10/2025, às 16:13, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Valfran Santana de Almeida**, **Chefe da Seção de Sustentação de Sistemas Judiciais**, em 30/10/2025, às 17:12, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Eronildes Ribeiro da Silva**, **Coordenador de Infraestrutura**, em 30/10/2025, às 17:19, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Rafhael Eduardo Alves de Souza**, **Assistente IV**, em 30/10/2025, às 18:58, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site https://sei.stj.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **6669227** e o código CRC **F7240BB1**.