TERMO DE REFERÊNCIA

Solução de avaliação de performance, qualidade e segurança de aplicações

PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DO PARÁ
SECRETARIA DE INFORMÁTICA

PROCESSO ADMINISTRATIVO PA-PRO-2021/01739

1. DO OBJETO

1.1. Registro de preço para eventual **contratação de serviços de solução de avaliação de performance, qualidade e segurança de aplicações, bem como serviços técnicos especializados de operação e análise**, conforme especificações e quantidades detalhadas neste termo de referência.

2. DA FUNDAMENTAÇÃO

2.1. Da motivação

2.1.1. A solução e serviços objeto deste termo de referência tem como principal requisito de negócio a disponibilização de serviços e ferramental que possibilitem a coleta, armazenamento e análise de informações integradas com o objetivo da melhoria contínua da qualidade dos serviços de TIC ofertados pelo TJPA através das plataformas (sistemas) que dispõe. Em específico, pretende-se monitorar o sistema PJE, aplicação de acompanhamento de processos judiciais mais importante do Tribunal de Justiça do Estado do Pará. Assim, a solução e serviços objeto desse estudo técnico devem oferecer os seguintes requisitos negociais ao sistema PJE:

- Coleta, armazenamento e análise, de forma integrada, dos acessos dos usuários ao PJE;
- Análise dos dados coletados para apoio à definição de estratégias e acompanhamento das melhorias na qualidade nos serviços do sistema em questão;
- Estruturar, configurar e analisar metas negociais que possibilitam a mensuração dos objetivos negociais do PJE;
- Integrar as informações coletadas de TI e negócio para possibilitar a correlação e identificação de impactos negociais causados por falhas ou diminuição de qualidade do serviço oferecido pelo PJE;
- Análise de forma inteligente e automática de problemas de infraestrutura que impactem na qualidade dos serviços ofertados pelo PJE, dimensionando, inclusive, o impacto negocial;
- Identificação, mapeamento e interconexão dos componentes das plataformas de serviços, de forma rápida, automática e dinâmica, possibilitando uma visão integrada e dinâmica das dependências dos componentes de TI do PJE;
- Análise detalhada do comportamento de uso do PJE, gerando métricas e indicadores que possibilitem a análise e estruturação de políticas e estratégias que melhorem o atendimento aos usuários deste sistema e aos cidadãos;
- Mapeamento, análise e reprodução do comportamento e uso do sistema PJE;
- Análise detalhada da segurança da aplicação em questão, com indicação das vulnerabilidades.

2.2. Dos objetivos a serem alcançados por meio da contratação

2.2.1. Esta contratação visa adquirir serviços e soluções que permitam ao JTPA, dispor de tecnologia para realizar o monitoramento e análise da aplicação PJE, visando a melhoria da sua qualidade, desempenho e segurança, bem com dispor de ferramenta que permita a visibilidade integrada do ambiente tecnológico para melhor gestão e melhor tempo de resposta em caso de incidente.

2.3. **Dos benefícios diretos e indiretos resultantes da contratação**

2.3.1. Os benefícios a serem alcançados com a solução escolhida consistem em:

- Redução do tempo de resposta a incidentes e problemas de tecnologia, que comprometam as aplicações gerenciadas;
- Otimização dos recursos de infraestrutura (servidor, memória, disco, rede e CPU) para atender às aplicações gerenciadas, resultando em economicidade de tais recursos;
- Melhoria na qualidade (performance e segurança) das aplicações gerenciadas;
- Redução de ocorrências de falhas de aplicação, às quais serão corrigidas a partir da descoberta de causa-raiz. Esta redução de falhas é proporcional ao tempo de uso da solução de monitoramento;
- Visão clara e concreta do uso das aplicações gerenciadas existentes do TJPA;
- Melhor alocação e priorização de recursos e projetos com foco no atendimento aos usuários;
- Melhoria na usabilidade e na jornada dos usuários às aplicações;
- Melhoria na utilização dos recursos tecnológicos que suportam toda a cadeia de entrega das aplicações gerenciadas;
- Melhoria na taxa de conversão (efetividade) das aplicações gerenciadas;

2.4. **Do alinhamento entre a demanda e os instrumentos de planejamento do TJPA**

Conforme o constante no subitem 1.7, b, dos Estudos Preliminares, a presente demanda está prevista no Plano Anual de Contatações do TJPA para o exercício de 2021 e vincula-se ao Plano de Gestão 2019/2021 no MACRODESAFIO 12 (FORTALECIMENTO DA ESTRATÉGICA NACIONAL DE TIC E PROTEÇÃO DE DADOS.), AÇÃO 12.1(APRIMORAR SOLUÇÕES DE SUSTENTAÇÃO DE INFRAESTRUTURA DE TIC). Também há previsão desta demanda no Plano Orçamentário do TJPA para o ano de 2021, com Notas de Reservas específicas e compatíveis com objeto a ser contratado.

2.5. **Da referência aos Estudos Preliminares**

Os estudos preliminares que evidenciam a necessidade da solução de APM estão registrados no siga PA-PRO-2021/01739.

2.6. **Da relação entre a demanda prevista e a quantidade de bens e/ou serviços a serem contratados**

Item	Descrição	Período	Métrica ou Unidade	Demanda Prevista	Critérios de Aferição da Quantidade	Documentos e outros Meios Probatórios
1	Módulo de monitoramento e análise de desempenho de aplicações	24 meses	Pacote para 4 cores ou Pacote para 16 GB RAM	49	Dimensionamento de infraestrutura do PJE	Relatórios de Infraestrutura Vcenter
2	Módulo de monitoramento e análise dos acessos a aplicação	24 meses	Pacotes de um milhão de acessos por ano	2	Monitoramento do uso do PJE	Sistema de Monitoramento Zabbix e Painel de aplicações
3	Módulo de monitoramento e análise da segurança das aplicações	24 meses	Por aplicação	3	Dimensionamento de infraestrutura do PJE	Sistema de Monitoramento Zabbix e Painel de aplicações

4	Serviços técnicos especializados	24 meses	Hh (Homem x hora)	3.840	Levantamento a partir de contratações similares	Contratações similares

2.6.1. No item 1, O módulo de monitoramento e análise de desempenho pode ser orçado tanto pela quantidade de cores de CPU, neste caso em pacotes de 4 cores; ou ainda pela quantidade de memória nos servidores de aplicação, neste caso, em pacotes de 16 GB de RAM.

2.6.2. No item 2, um acesso equivale a uma sessão de usuário em uma aplicação, independentemente do número de *views, o* orçamento será feito com base em pacotes de um milhão de acessos à aplicação por ano.

2.6.3. Uma aplicação do item 3 refere-se ao código-fonte que define a regra de negócio de um serviço de TIC completo. Nos casos em que a aplicação é separada em *frontend* e *backend*, o TJPA entende que são suas aplicações.

2.6.4. No item 4, a Hora de Serviço Técnico, "Homem x hora", representa o tempo de uma hora de trabalho de um técnico especializado conforme especificado no item 3.10 ("Da qualificação técnica dos profissionais").

2.7. Da análise de mercado de TIC

2.7.1. Analisando as soluções disponíveis no mercado, verifica-se que todas que atendem ao requerido no presente Termo de Referência, passam pela aquisição de solução de *software* do tipo "**Gerenciamento de Performance de Aplicações"** e soluções do tipo **"Análise de Vulnerabilidade de Código"**. Tais soluções são amplamente reconhecidas e difundidas no mercado, existindo diversos fabricantes e fornecedores para tais soluções.

2.7.2. Abaixo, segue referência da maior instituição que analisa soluções de TI, o *Gartner*, que reconhece as disciplinas e identificam os principais fabricantes de tais soluções.

Figura 1 - Soluções de APM
[https://www.appdynamics.com/resources/reports/gartner-magic-quadrant-apm] - acesso em 20/04/2021

Source: Gartner (April 2020)

Figura 2 - Solução de Segurança de Aplicações
[https://www.synopsys.com/blogs/software-security/gartner-mq-ast-2020/] - acesso em 20/04/2021

2.7.3. Tais disciplinas de tecnologia já estão consolidadas no mercado e, inclusive, já existem processos de contratação e licitações para aquisição de tais soluções.

2.7.4. Portanto, existem diversos fabricantes de tais soluções que podem atender de forma única ou em composição de soluções os requisitos desta contratação. É importante salientar que, a maioria dos fabricantes de solução são estrangeiros e trabalham no modelo de revenda ou distribuição. Desta forma, aumenta-se ainda mais o número de possíveis fornecedores, podendo ser tanto o próprio fabricante como qualquer uma de suas revendas ou distribuidoras. Abaixo, segue um quando com alguns dos principais fabricantes das tecnologias ora pretendida nesta contratação.

Fabricante	Monitoramento e análise de desempenho de aplicações	Monitoramento e análise dos acessos a aplicação	Monitoramento e análise da segurança das aplicações
Cisco (AppDynamics)	X	X	
Dynatrace	X	X	X
New Relic	X	X	
Broadcom	X	X	
Synopsys			X
Checkmarx			X
Veracode			X

2.7.5. Analisando os quadrantes mágicos do *Gartner* e a tabela acima, observa-se que existe um quantitativo de fabricantes e consequentemente de revendas de produtos que atendem ou de forma única ou combinada todos os requisitos desta contratação. Neste sentido, a solução, composta de 03 módulos poderá ser entregue de forma única ou em composição com mais de um produto.

2.8. **Da natureza do objeto**

2.8.1. Esta contratação trata da aquisição de serviços de natureza continuada com o fornecimento de direito de uso de *software* e mão de obra especializada. Em relação aos itens de subscrição de licenças de *software* por tempo determinado, o TJPA estará contratando o direito de uso de solução de s*oftware* por período

pré-determinado, por este motivo, não caracteriza a aquisição de bem. Além disso, trata-se de contratação de serviços continuados pois visa a avaliação contínua da qualidade, desempenho e segurança das aplicações enquanto estas estiverem em uso pelos seus usuários.

2.8.2. O objeto possui características comuns e usuais disponíveis no mercado de TI. Conforme detalhado no estudo, as disciplinas APM (*Application Performance Management*) e AST (*Application Security Testing*) são disciplinas já estruturadas e reconhecidas no mercado de TI. Além disso, existem outros processos de contratação similares que foram contratados e executados na Administração Pública. Assim sendo, os parâmetros para aferir a qualidade e o desempenho da solução e dos serviços já estão estabelecidos e foram adaptados para realidade do TJPA e para esta contratação.

2.8.3. O estudo de viabilidade técnica concluiu que a solução objeto desta contratação é necessária e suficiente para atender aos requisitos negociais e às necessidades apresentadas no referido estudo. Verificou-se ainda que existem soluções e ou composições de soluções disponíveis no mercado capazes de atender aos requisitos especificados no projeto em tela, possibilitando a participação e ampla concorrência no processo de contratação. Por fim, constatou-se que os valores estimados para este projeto estão dentro dos valores e orçamentos previstos no PDTI.

2.8.4. Assim sendo, esta contratação consiste na aquisição de serviços comuns, de natureza continuada com o fornecimento de licença de uso de *software* e mão-de-obra especializada.

2.9. **Do parcelamento do objeto**

2.9.1. A contratação ora pretendida pode ser atendida por um único fornecedor sem prejuízo a ampla concorrência. Esta abordagem, inclusive, mostra-se mais adequada, visto que se os itens fossem divididos em lotes diferentes, ocorreria a possibilidade de um fornecedor entregar uma solução e o outro entregar especialistas em uma outra solução de *software*, a qual seria diferente, portanto, da solução entregue pelo fornecedor do software. Tal situação acarretaria **incompatibilidade técnica para integração da solução com os serviços especificados.**

2.9.2. Conforme Acórdão 861/2013-Plenário - É lícito os agrupamentos em lotes de itens a serem adquiridos por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si. Além disso, a solução de TI, objeto da contratação, possui natural indivisibilidade, o que também inviabiliza a contratação de seus serviços por item de forma separada.

2.9.3. Segundo o acórdão 5260/2011 – TCU – 1ª câmara, de 06/07/2011, "Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si". A adjudicação global proposta neste documento agrupa solução e serviços de uma mesma natureza, que guardam correlação entre si, seja por similaridade técnica ou de tecnologia, bem como de aplicabilidade em busca de uma única solução, sem causar qualquer prejuízo à ampla competitividade.

2.9.4. Ademais, a opção pela contratação conjunta, e não fracionada, dos serviços, não constitui qualquer afronta aos termos da Súmula 247 do TCU. Senão, veja-se o que diz a Sumula:

> *"É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo*

objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade."

2.9.5. Tanto a disciplina legal, quanto a Súmula do TCU, indicam que a viabilidade técnica do fracionamento deve ser analisada para determinar a possibilidade de licitações distintas (ou lotes distintos na mesma licitação) do objeto que se pretende adquirir. No caso em comento, o objeto licitado envolve tratamento técnico, que demanda que o fornecedor dos serviços técnicos tenha conhecimento sobre a solução de *software* também a ser contratada. Particionar as contratações, deixando a possibilidade de empresas diferentes prestarem os serviços e o licenciamento, é assumir um grande risco para este Tribunal de Justiça, pois deixará aberta a oportunidade para problemas de integração e de administração da solução CONTRATADA.

2.9.6. Neste sendo, em respeito à legislação vigente e na busca pela economicidade e viabilidade técnica, optou-se por garantir a integração dos serviços e licenças a partir da contratação de um único prestador para execução da contratação em pauta.

2.9.7. Este Instituto entende que para manter a integração dos serviços contratados e do licenciamento, e para que o fornecedor dos serviços e licenciamento tenha conhecimento sobre toda a solução, a forma de contratação mais adequada é aquela que não necessita do parcelamento do objeto.

2.10. **Da seleção do fornecedor**

2.10.1. **Da forma e do critério de seleção**

2.10.1.1. Para efeito de julgamento dos preços no Pregão Eletrônico, o critério deverá ser do tipo menor preço GLOBAL, considerando para a formação da proposta da licitante a estimativa máxima da necessidade definida pelo TJPA, sendo declarada vencedora a licitante que apresentar o Menor Preço Global e que atender a todos os requisitos e exigências do certame.

2.10.1.2. Quanto ao critério de julgamento pelo menor preço GLOBAL, justifica-se a adoção deste critério tendo em vista que os produtos e serviços solicitados devem ser prestados em conjunto pela mesma contratada, facilitando o controle, monitoramento e gestão das Ordens de Serviços, assim como a padronização na verificação da qualidade dos produtos entregues, após a execução das atividades, bem como a uniformização e responsabilidade sobre os serviços de garantia.

2.10.2. **Da modalidade e do tipo de licitação**

2.10.2.1. A licitação será do tipo Pregão Eletrônico na modalidade aberta, por se tratar de contratação de serviços comuns de natureza continuada.

2.10.2.2. Além disso, será adotado o Sistema de Registro de Preços (SRP). A justificativa para tal escolha é a natureza do objeto e formato de metrificação dos serviços, não sendo possível definir previamente e completamente o quantitativo a ser demandado pela Administração durante o período de vigência da ata. Além disso, tal escolha permite que seja realizada a implantação e operacionalização do projeto por etapas, realizando a demanda por serviços em etapas ou Ordens de Serviços. Neste caso, devido à complexidade e especificidade dos serviços elencados neste estudo

técnico, **não é possível definir completamente e exaustivamente a quantidade de unidades** que necessitam ser contratadas para atender as demandas futuras do TJPA.

2.10.3. **Dos critérios técnicos de habilitação obrigatórios**

2.10.3.1. A LICITANTE deverá realizar a comprovação de que dispõe de habilitação e capacidade técnica de executar o projeto. Para isso deverá entregar, na habilitação:

2.10.3.1.1. Atestado (s) de capacidade técnica, fornecido (s) por pessoa (s) jurídica (s) de direito público ou privado, para as quais o LICITANTE tenha executado o fornecimento da solução com tamanho e a complexidade operacional equivalente aos especificados neste Termo de Referência, tanto em volumetria de acesso de usuários, quanto em tamanho e complexidade tecnológica.

2.10.3.1.1.1. Considera-se projeto com tamanho e complexidade operacional equivalente a este projeto, aqueles que tenham entregado ao menos 50% das quantidades especificadas neste Termo de Referência dos itens de maior relevância, sendo necessário a comprovação de pelo menos os itens 01 e 04.

2.10.3.1.1.2. A empresa participante deve disponibilizar, quando demandada, todas as informações necessárias à comprovação da legitimidade do atestado, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços.

2.10.3.1.1.3. Os atestados deverão ser emitidos em papel timbrado e conter:

- Razão Social, CNPJ e Endereço Completo da Empresa Emitente;
- Razão Social da Contratada;
- Número e vigência do contrato se for o caso;
- Objeto do contrato;
- Declaração de que foram atendidas as expectavas do cliente quanto ao cumprimento de cronogramas pactuados;
- Local e Data de Emissão;
- Identificação do responsável pela emissão do atestado;
- Cargo, Contato (telefone e correio eletrônico);
- Assinatura do responsável pela emissão do atestado;

2.10.3.1.1.4. No caso de apresentação de atestado de empresas privadas, não serão considerados aqueles apresentados por empresas participantes do mesmo grupo empresarial da contratada. Serão consideradas como de mesmo grupo, empresas controladas pela contratada, ou que tenham pelo menos uma pessoa física ou jurídica que seja sócia da empresa emitente e da contratada.

2.10.3.1.2. Comprovação, caso não seja o próprio fabricante da solução, de que está devidamente inscrito no programa de parceria do fabricante da solução ofertada. Tal comprovação poderá ser feita pela apresentação de contrato de parceria ou carta do próprio fabricante atestando a parceria e a validada da mesma. O objetivo desta comprovação é garantir que, caso a licitante não seja o fabricante, tenha meios de comprovar que possui condições e lastro para prestar os serviços de suporte técnico com garantia do fabricante. Sem uma relação formal entre a revenda e o fabricante, não há como a revenda garantir o suporte técnico do fabricante, o qual é acionado

no caso de panes mais severas, como as que necessitem revisão e atualização do código da aplicação.

2.10.3.1.3. Com o objetivo de garantir, ainda em tempo de habilitação, que o produto ofertado atende aos requisitos técnicos necessários ao TJPA, a LICITANTE mais bem classificada na etapa de lances será convocada para realizar, através de prova de bancada, a demonstração do produto ofertado. Sem esta comprovação prática, corre-se o risco da LICITANTE ser homologada ofertando um produto que não atenda a todos os requisitos definidos neste Termo de Referência.

2.10.3.1.4. Assim sendo, A LICITANTE mais bem classificada na etapa de lances será convocada para realizar teste de bancada da solução ofertada. A solução a ser demostrada pela LICITANTE não poderá ser diferente da informada na proposta.

2.10.3.1.5. A prova de bancada deverá atender a todos os requisitos abaixo:

2.10.3.1.5.1 Após convocação pelo pregoeiro, a LICITANTE convocada para prova de bancada terá o prazo máximo de 02 dias úteis para iniciar a demonstração técnica do produto ofertado;

2.10.3.1.5.2. A LICITANTE deverá disponibilizar a solução em ambiente de nuvem própria, não sendo permitida a instalação de nenhum componente na infraestrutura do TJPA para a prova de bancada. Será de total responsabilidade da LICITANTE a instalação e configuração do ambiente da prova de bancada, sem nenhum ônus para o TJPA, independente do resultado da demonstração;

2.10.3.1.5.3. A LICITANTE, após a configuração do produto ofertado, deverá realizar a demonstração dos requisitos técnicos constantes no anexo C deste termo de referência. Esta demonstração deverá ocorrer de forma presencial ou remota, a depender das questões segurança sanitárias (isolamento social) vigentes por ocasião dos testes, onde a equipe da LICITANTE deverá apresentar comprovação prática na solução ofertada de todos os itens constantes no anexo C. Essa comprovação deverá ocorrer item a item, no ambiente configurado pela LICITANTE para a demonstração.

2.10.3.1.5.4. Para cada item demostrado à equipe técnica do TJPA, a LICITANTE deverá coletar evidência inequívoca de que atente ao item demostrado.

2.10.3.1.5.5. A LICITANTE deverá realizar a demonstração de todos os itens do anexo C em um prazo máximo de 08 horas úteis, a contar do início da demonstração.

2.10.3.1.5.6. Ao final da demonstração, no prazo de 08 horas úteis após a conclusão da demonstração, a LICITANTE deverá entregar relatório com as evidências dos itens demostrados, comprovando que atende de forma inequívoca todo os itens constantes do anexo C.

2.10.3.1.5.7. O não cumprimento de qualquer dos itens da prova de bancada, seja de prazo, seja de atendimento ou requisitos técnicos, resultará na INABILITAÇÃO da LICITANTE e, automaticamente, a convocação da próxima LICITANTE classificada na etapa de lances. Abaixo, segue, em resumo, os critérios de aceitação da prova de bancada do produto ofertado:

- Prazo: Iniciar a demonstração do produto em um prazo máximo de 02 (dois) dias úteis após a convocação:

- Prazo: Realizar a demonstração dos itens constantes do anexo C em um prazo de 08 (oito) horas úteis, após o início da demonstração;
- Prazo: Entregar relatório de evidências da demonstração em um prazo máximo de 08 (oito) horas úteis após a conclusão da demonstração;
- Requisitos: Demonstrar que atende a todos os requisitos constantes no anexo C deste termo de referência;
- Requisitos: Demonstrar o mesmo produto (produto e fabricante) ofertado na proposta.

2.10.3.1.6. Após o recebimento do relatório de evidências enviada pela LICITANTE, o TJPA, no prazo de 2 dias úteis, irá emitir relatório indicando ou não a comprovação de todos os requisitos técnicos. Caso não sejam comprovado o atendimento a TODOS os requisitos técnicos solicitados, bem como todos os requisitos da prova de bancada, a LICITANTE será INABILITADA e automaticamente a convocação da próxima LICITANTE classificada na etapa de lances. O TJPA, devidamente justificado, poderá solicitar que não seja executada a prova de bancada, habilitando a licitante sem a necessidade da prova de bancada.

2.11. **Do impacto ambiental**

2.11.1. Esta contratação não gera impacto ambiental. De toda forma, toda documentação gerada pelo contrato deverá ser digital com assinatura eletrônica, evitando assim a impressão em papel.

2.12. **Da conformidade técnica e legal**

2.12.1. Este projeto deve estar em conformidade com as seguintes leis e decretos:

- Lei nº. 8666/1993 – Disciplina as normas para a licitação e contratos administrativos da administração pública e dá outras providencias;
- Decreto nº. 7.892/2013 – Disciplina o Sistema de Registro de Preços previsto no Art. 15 da Lei nº. 8.666/1993;
- Portaria nº. 265/2018 – Regulamenta o procedimento administrativo para adesão a ata de registro de preços, conforme previsto no art. 22, § 9º, do Decreto 39.103/2018;
- Instrução Normativa SLTI nº 01/2019 – Dispõe sobre o Plano Anual de contratações de bens, serviços, obras e soluções de tecnologia da informação e comunicações no âmbito da administração pública federal direta, autárquica e fundacional e sobre o sistema de planejamento e gerenciamento de contratações;
- Instrução Normativa SLTI nº 02/2008 – Dispõe sobre as regras e diretrizes para contração de serviços continuados ou não;
- Acórdão TCU nº. 1297/2015 – Plenário – O órgão gerenciador do registro de preços deve justificar eventual previsão editalíssima de adesão a ata por outros órgãos não participantes(“CARONAS”) dos procedimentos iniciais;
- Acórdão TCU nº. 2.877/2017 – Plenário – A adesão a ata de registro de preços (“CARONAS”) está condicionada, entre outros requisitos (art. 22 do decreto nº. 7.892/2013, a comprovação da adequação do objeto as reais necessidades do órgão ou da entidade aderente e a vantagem do preço registrado em relação aos preços praticados no mercado onde o serviço será prestado.

2.13. **Das obrigações**

2.13.1. **Das obrigações do contratante**

- Indicar os locais e horários em que deverão ser executados os serviços;
- Exigir o cumprimento de todas as obrigações assumidas pela contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;
- Exercer o acompanhamento e a fiscalização do fornecimento, notificando a Contratada por escrito da ocorrência de eventuais imperfeiçoes no curso da execução dos serviços, fixando prazo para sua correção de acordo com o SLA (acordo de nível de serviço estabelecido);
- Pagar à contratada o valor resultante do valor do fornecimento da solução, no prazo e condições estabelecidas no contrato;
- Emitir procuração específica com poderes para representá-lo nas ações que forem confiadas aos advogados da Contratada;
- Fornecer todos os subsídios necessários ao desempenho da atividade da Contratada, encaminhando os documentos necessários à adequada realização dos serviços.

2.13.2. **Das obrigações da contratada**

- Prestar os serviços com pessoal adequadamente qualificado e capacitado para suas atividades, conforme especificado neste Termo de Referência;
- Cumprir rigorosamente todas as programações e atividades do objeto do contrato;
- Prestar os serviços de acordo com o especificado neste instrumento;
- Levar imediatamente ao conhecimento da Fiscalização qualquer fato extraordinário ou anormal que ocorra durante a execução dos serviços a fim de que sejam adotadas medidas cabíveis, bem como comunicar por escrito e de forma detalhada todo tipo de incidente que venha a ocorrer;
- Prestar todos os esclarecimentos que forem solicitados pela Fiscalização, atendendo as solicitações de acordo com prazos estabelecidos;
- Substituir, sempre que solicitado pelo TJPA, qualquer recurso humano cuja atuação, permanência e/ou comportamento sejam prejudiciais, inconvenientes, insatisfatórios à disciplina da repartição ou ao interesse do serviço, ou ainda, incompatíveis com o exercício das funções que lhe forem atribuídas;
- Responder pelos danos causados ao TJPA ou a terceiros, decorrentes de sua culpa ou dolo, quando da execução dos serviços;
- Arcar com despesas decorrentes de infrações relacionadas ao disposto no objeto deste instrumento, durante o desempenho das funções, ainda que fora das dependências do TJPA;
- Responder pelo cumprimento dos postulados legais vigentes de âmbito federal, estadual ou municipal;
- Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às recomendações aceitas pela boa técnica, normas e legislação. Garantir a supervisão permanente dos serviços de forma a obter uma operação correta e eficaz;
- Manter suporte inerente aos serviços a serem executados, garantindo um serviço de alto padrão, sem nenhum custo adicional para o TJPA;
- Atender prontamente quaisquer exigências do representante do TJPA inerentes ao objeto do Contrato;
- Fornecer, na forma solicitada pelo TJPA, o demonstrativo de utilização dos serviços, objeto do Contrato;
- Comunicar ao TJPA, por escrito, qualquer anormalidade, sobretudo de caráter urgente, e prestar os esclarecimentos julgados necessários;

- Manter, durante toda a execução do Contrato, em compatibilidade com as obrigações a serem assumidas, todas as condições de qualificação exigidas na contratação, inclusive por meio da atualização dos seus profissionais;
- Indicar um preposto para acompanhar a execução do contrato e responder perante o Contratante;
- A Contratada deve manter Matriz, Filial ou Escritório de Representação no Território nacional, durante toda a vigência do Contrato, com condições adequadas para gerenciar a prestação dos serviços, com linha telefônica, em virtude da necessidade de o TJPA manter contato com o preposto indicado pela empresa;
- Contratada deve fornecer, no ato da assinatura contratual, endereço da matriz, filial ou escritório, bem como número de telefone comercial fixo, móvel, fax e endereço eletrônico (e-mail), devendo atualizar todos os dados sempre que houver alterações;
- Dar cumprimento a todas as determinações e especificações estabelecidas neste instrumento e assumir inteira responsabilidade pela execução dos serviços contratados, nos termos da legislação vigente;
- Manter toda documentação relativa à execução do contrato;
- Descrever as obrigações contratuais que o órgão e a empresa contratada deverão observar.

3. ESPECIFICAÇÃO TÉCNICA DETALHADA

3.1. Dos papeis a serem desempenhados

PAPEL	ENTIDADE	RESPONSABILIDADE
Equipe de Apoio da Contratação	TJPA	Equipe responsável por subsidiar a área de licitações em suas dúvidas, respostas aos questionamentos, recursos e impugnações, bem como na análise e julgamento das propostas das licitantes.
Equipe de Gestão e Fiscalização do Contrato	TJPA	Equipe composta pelo gestor do contrato, responsável por gerir a execução contratual, e pelos fiscais demandante, técnico e administrativo, responsáveis por fiscalizar a execução contratual.
Fiscal Demandante do Contrato	TJPA	Servidor representante da área demandante da contratação, indicado pela referida autoridade competente, responsável por fiscalizar o contrato quanto aos aspectos funcionais do objeto, inclusive em relação à aplicação de sanções.
Fiscal Técnico do Contrato	TJPA	Servidor representante da área técnica, indicado pela respectiva autoridade competente, responsável por fiscalizar o contrato quanto aos aspectos técnicos do objeto, inclusive em relação à aplicação de sanções.
Fiscal Administrativo do Contrato	TJPA	Servidor representante da Secretaria de Administração, indicado pela respectiva autoridade, responsável por fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.
Gestor do Contrato	TJPA	Servidor com atribuições gerenciais, técnicas ou operacionais relacionadas ao processo de gestão do contrato, indicado por autoridade competente do órgão.

Preposto	Contratada	Representante da empresa contratada, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao órgão contratante, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual.
Consultor técnico	Contratada	Consultor técnico da empresa contratada, responsável por executas os serviços técnicos demandados nas Ordens de Serviço e realizar o repasse de conhecimento quando solicitado. Deverá ter a capacitação especificada neste termo de referência.

Equipe de apoio da contratação (quando se tratar de licitação)		
Integrante Demandante Nome: Arilson Silva Matrícula: 183318 Telefone:(91)98161-3141 E-mail: arilson.silva@tjpa.jus.br	**Integrante Técnico** Nome: Paulo Lourinho Matrícula: 187445 Telefone: (91) 98366-9678 E-mail: paulo.lourinho@tjpa.jus.br	**Integrante Administrativo** Nome: Matrícula: Telefone: E-mail:

Equipe de gestão e fiscalização da contratação			
Gestor do Contrato Nome: Paulo Lourinho Matrícula: 187445 Telefone: (91) 98366-9678 E-mail: paulo.lourinho@tjpa.jus.br	**Fiscal Demandante** Nome: Arilson Silva Matrícula: 183318 Telefone:(91)98161-3141 E-mail: arilson.silva@tjpa.jus.b	**Fiscal Técnico** Nome: Marcus V. B. e Silva Matrícula: 116971 Telefone: (91) 99105-3825 E-mail: marcus.silva@tjpa.tjpa.jus.br	Fiscal Administrativo Nome: Matrícula: Telefone: E-mail:

3.2. **Da dinâmica de execução do contrato**

3.2.1. Após formalização contratual, o TJPA irá realizar a convocação da CONTRATADA para reunião inicial de contrato. Esta reunião deverá ocorrer no prazo de até 10 dias úteis, podendo ser prorrogados, por igual período, por ambas as partes, mediante apresentação de motivação.

3.2.2. Esta reunião deverá ocorrer:

- Apresentação do preposto da contratada;
- Apresentação da equipe do TJPA;
- Estabelecimento dos padrões para apresentação do plano de implantação;
- Abertura das Ordens de Serviço para as soluções de software;
- Planejamento da execução dos serviços;
- Apresentação e definição dos planos de comunicação para o contrato;
- Apresentação e assinatura de termo de responsabilidade, confidencialidade e ciência pela contratada e preposto.

3.2.3. Esta reunião deverá ocorrer nas dependências do TJPA, em Belém/PA e será registrada em ata.

3.2.4. Após a reunião inicial e emissão de Ordem de Serviço para a implantação da solução de software, a CONTRATADA deverá obedecer aos prazos estabelecidos para apresentação do plano de implantação. Após a aprovação

do plano de implantação, a CONTRATADA deverá realizar a implantação da solução. Tal implantação poderá ser acompanhada pela equipe do TJPA ou outra indicada pelo TJPA. Ao final da implantação, a CONTRATADA deverá emitir relatório técnico de implantação contendo as informações técnicas e evidencias da implantação da solução no ambiente do TJPA.

3.2.5. Após a solução implantada, o TJPA irá emitir Ordens de Serviço para a execução dos serviços técnicos especializados informando os dados da demanda. A CONTRATADA deverá alocar equipe técnica especializada, com as competências técnicas especificadas. A CONTRATADA é responsável por informar e encaminhar documentação da equipe técnica que irá atuar na execução contratual, juntamente com termo de ciência e confidencialidade.

3.2.6. Haverá um período de ambientação, que compreende o período que vai até os primeiros 60 dias após a emissão da primeira Ordem de Serviço. Durante este período, o TJPA não irá aplicar as sanções administrativas. No entanto, a CONTRATADA deverá garantir os padrões de qualidade e aderência a este termo de referência.

3.2.7. Após o período de ambientação, iniciará o período de operação continuada onde o TJPA irá emitir as Ordens de Serviço necessárias e a CONTRATADA deverá executar os serviços conforme especificado neste termo de referência.

3.2.8. Na fase de operação continuada, todos os critérios de avaliação serão avaliados e aplicadas as devidas glosas.

3.2.9. Ao final de cada Ordem de Serviço, a CONTRATADA deverá emitir relatório de atividades executadas decorrente a OS.

3.2.10. Após a entrega do relatório de atividade de cada OS, o TJPA irá emitir o Termo de Recebimento Provisório e irá realizar a avaliação dos serviços executados.

3.2.11. Após a validação dos serviços executados, caso estejam dentro dos parâmetros definidos, o TJPA irá emitir o termo de recebimento definitivo, autorizando o processo de pagamento dos serviços executados decorrente a OS. Caso os níveis mínimos de serviços não forem satisfeitos, caso seja possível saná-los, sem prejuízos na qualidade dos serviços executados, a CONTRATADA poderá ajustar e realizar nova entrega, no prazo máximo de 10 dias úteis.

3.2.12. Ao final do contrato, os procedimentos e atividades previstas no encerramento e transição contratual deverão ser executadas.

3.2.13. **Etapas**

Os serviços serão executados mediante emissão de ordem de serviço. No entanto, os seguintes eventos e prazos deverão ser mantidos:

Evento	Prazo
Reunião inicial do contrato	Em até 10 dias úteis após a assinatura do contrato
Disponibilização das soluções de software e plano de implantação	Em até 10 dias úteis após emissão de Ordem de Serviço
Período de ambientação	Até 60 dias após a emissão da primeira Ordem de Serviço
Período de operação continuada	Após 60 dias depois da emissão da primeira Ordem de Serviço
Período de transição contratual	90 dias antes do encerramento contratual, obedecendo as regas estabelecidas neste termo de referência.
Suporte e garantia do produto	Inicia imediatamente após o termo de aceite da implantação e deve permanecer durante toda a vigência contratual.
Disponibilização dos serviços técnicos	Em até 05 dias úteis após emissão de Ordem de Serviço.

3.2.14. **Dos prazos**

3.2.14.1. Prazos de entrega dos bens/execução dos serviços

O prazo de execução dos serviços de software será de 10 dias uteis após a emissão de Ordem de Serviço.

Os prazos de execução dos serviços técnicos serão mediante o definido nas Ordens de Serviços.

3.2.14.2. Prazo de vigência do contrato

A vigência do contrato será de 24 meses, podendo ser renovados até os limites definidos por lei.

3.2.15. **Logística de implantação**

3.2.15.1. Em relação à logística de implantação, como será permitida apenas a instalação de agentes coletores nos servidores do TJPA, a implantação deverá ocorrer de forma remota.

3.2.15.2. Em caso de necessidade de *restart* de servidores, estes somente poderão ocorrer fora do horário de expediente para não impactar ou gerar indisponibilidade no ambiente produtivo do TJPA.

3.2.15.3. A CONTRATADA deverá apresentar plano de implantação da solução com indicação da arquitetura e componentes da solução a ser implementada, bem como dos procedimentos operacionais, análise de risco e impactos no ambiente do TJPA.

3.2.15.4. Somente após a aprovação do plano de implantação é que a CONTRATADA poderá realizar os procedimentos de implantação, respeitando as regras e definição de acesso e mudanças no ambiente computacional do TJPA.

3.2.16. **Cronograma**

A execução do projeto será mediante emissão de Ordem de Serviço. Dessa forma, o cronograma de execução obedecerá aos cronogramas estabelecidos nas Ordens de Serviço.

3.3. **Dos instrumentos formais de solicitação**

3.3.1. Todo e qualquer serviço deverá ser autorizado formalmente pelo TJPA através de emissão de Ordem de Serviço, que indicará o escopo, datas para início, prazo, estimativas de quantidade e valores e critérios de avaliação.

3.3.2. As Ordens de Serviço terão prazo máximo de 01 mês, podendo ser solicitadas com prazos menores.

3.3.3. Após emissão de Ordem de Serviço, a mesma deverá ser autorizada pela equipe do TJPA e aceita pela CONTRATADA através de autorização formal do preposto.

3.3.4. As Ordens de Serviços serão emitidas e tramitadas em sistema eletrônico do próprio TJPA, onde terá o registro das autorizações formais das partes. Caso julgue necessário, o TJPA poderá alterar o processo de tramitação de Ordens de Serviço, mantendo as regras estabelecidas.

3.3.5. Após emitida a Ordem de Serviço, a CONTRATADA terá o prazo máximo de 05 dias úteis para aceitá-la formalmente.

3.3.6. A execução do projeto será mediante emissão de Ordem de Serviço. Dessa forma, o cronograma de execução obedecerá aos cronogramas estabelecidos nas Ordens de Serviço.

3.4. **Garantia e Nível de Serviço**

3.4.1. **Garantia do produto/serviço**

3.4.1.1. A CONTRATADA deverá realizar a instalação da solução e seus módulos em nuvem própria ou de terceiros. Será permitida, caso necessário, a instalação de agentes ou coletores nos servidores das aplicações do TJPA.

3.4.1.2. A instalação, integração e configurações iniciais deverá ser feita no prazo máximo de 30 dias corridos a partir da emissão da ordem de serviço.

3.4.1.3. A CONTRATADA deverá disponibilizar suporte técnico, no regime 8x5 (Oito horas por dia e cinco dias por semana). No entanto, deverá disponibilizar a possibilidade de canal de comunicação, site ou telefônico, para que o registro de problemas e suporte seja feito no regime 24x7 (Vinte quatro horas por dia e sete dias por semana).

3.4.1.4. A CONTRATADA deverá, durante toda vigência contratual, disponibilizar o suporte técnico do fabricante da solução, permitindo, inclusive, que o TJPA possa registrar, diretamente, chamados junto ao fabricante, obedecendo as mesmas regras de prazo estabelecidas.

3.4.1.5. A CONTRATADA deverá possuir contrato de parceria com o fabricante, ou outro instrumento que substitua, durante toda a vigência contratual, garantindo o nível de suporte da solução junto ao fabricante.

3.4.1.6. O SUPORTE TÉCNICO deverá compreender a resolução de dúvidas, quaisquer defeitos, bugs, vícios de funcionamento e problemas da solução de software disponibilizada, bem como o direito automático de atualizações durante a vigência do contrato.

3.4.1.7. Os serviços de SUPORTE TÉCNICO, INSTALAÇÃO E GARANTIA não o poderão gerar nenhum custo adicional ao TJPA.

3.4.1.8. Os chamados de suporte técnico serão classificados por severidade, de acordo com o impacto no ambiente computacional do TJPA. Os níveis de severidade são:

- Severidade 1 - Deveremos entender como Severidade 1 um incidente que cause a indisponibilidade total da solução de software.
- Severidade 2 - Deveremos entender como Severidade 2 incidentes que não impeçam o uso da solução de software, mas que impeça o uso parcial do mesmo.
- Severidade 3 - Deveremos entender como Severidade 3 incidentes que não gere indisponibilidade nem total e nem parcial da solução. Contempla também o esclarecimento de dúvidas e consultas referente ao funcionamento do software.

3.4.1.9. Os prazos para atendimento das demandas de suporte estão detalhados na tabela abaixo:

SLA de atendimento do serviço de suporte técnico			
Nível de severidade	**Descrição**	**Prazo para início de atendimento**	**Prazo para conclusão de atendimento**
1	Incidente que cause a indisponibilidade total da solução de software	02 horas úteis	04 horas úteis
2	Incidentes que não impeçam o uso da solução de software, mas que impeça o uso parcial do mesmo	04 horas úteis	12 horas úteis
3	Incidentes que não gere indisponibilidade nem total e nem parcial da solução. Contempla também o esclarecimento de dúvidas e consultas referente ao funcionamento do software	08 horas úteis	16 horas úteis

3.4.1.10. A CONTRATADA não será responsabilizada pelo prazo máximo estabelecido na Tabela de SLA, quando o chamado for originado por falha, interrupção ou qualquer outra ocorrência nos serviços de telecomunicações ou energia elétrica que atendem à infraestrutura interna do TJPA; indisponibilidade de

dados, inconsistência de dados e informações geradas pelo TJPA; infraestrutura e capacidade de ambiente de tecnologia do TJPA, não se caracterizando, nesses casos, a indisponibilidade dos serviços ou inadimplemento da CONTRATADA.

3.4.1.11. Toda e qualquer intervenção no ambiente produtivo resultante de serviços de suporte técnico deve ser executada somente mediante prévia autorização do TJPA, a partir de informações claras dos procedimentos que serão adotados/executados pela CONTRATADA.

3.4.1.12. Ao final do atendimento e resolução da ocorrência, o técnico da CONTRATADA realizará, em conjunto com representantes do TJPA, testes para verificação dos resultados obtidos, certificando-se do restabelecimento à normalidade e/ou resolução do problema.

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

3.4.1.14. Nos casos em que o atendimento não se mostrar satisfatório, o TJPA fará reabertura do chamado, mantendo-se as condições e prazos do primeiro chamado.

3.4.2. Garantia contratual

3.4.2.1. Como garantia do cumprimento integral de todas as obrigações contratuais que serão assumidas, inclusive indenizações e multas que venham a ser aplicadas, a Contratada se obriga a prestar garantia, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do TJPA, a contar da assinatura do Contrato, no valor correspondente a 5% (cinco por cento) do valor do Contrato, na modalidade de caução em dinheiro ou seguro garantia ou fiança bancária.

3.4.2.2. O valor da garantia será atualizado nas mesmas condições do valor contratual.

3.4.2.3. A garantia ficará à responsabilidade e à ordem da Diretoria Financeira da Contratante e somente será restituída após o integral cumprimento de todas as obrigações contratuais.

3.4.2.4. Se a garantia prestada pela Contratada for na modalidade de caução em dinheiro, esta deverá ser efetuada em instituição bancária definida pelo TJPA, em favor da Contratante.

3.4.2.5. A garantia poderá ser retirada/levantada, total ou parcialmente, para fins de cobertura de pagamento das multas previstas neste Termo de Referência.

3.4.2.6. Se o valor da garantia for utilizado, total ou parcialmente, em pagamento de qualquer obrigação, inclusive indenização ou pagamento de multas contratuais, a Contratada se compromete a fazer a respectiva reposição no prazo de 03 (três) dias úteis contados da data em que for notificada pela Contratante, mediante ofício entregue contrarrecibo.

3.4.2.7. Na hipótese de rescisão do Contrato, o TJPA executará a garantia contratual para seu ressarcimento, nos termos do art. 80, III, da Lei nº 8.666/93 e alterações posteriores.

3.4.2.8. O TJPA executará a garantia na forma prevista na legislação que rege a matéria.

3.4.2.9. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

- Prejuízos advindos do não cumprimento do objeto do contrato;
- Prejuízos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;
- Multas moratórias e punitivas aplicadas pela Administração à Contratada.

3.4.2.10. A modalidade “seguro-garantia” somente será aceita se contemplar todos os eventos indicados no item acima, observada a legislação que rege a matéria.

3.4.3. Nível de Serviço

3.4.3.1. Abaixo, seguem os requisitos do nível mínimo de serviço:

- Para a solução de software:

Indicador	Métrica	SLA	Penalidade

Disponibilidade da solução de software	% de disponibilidade da solução	98%	De 90% a 98%: Glosa de 1% do valor do licenciamento. De 85% a 90%: Glosa de 3% do valor do licenciamento. Abaixo de 85%: Glosa de 5% do valor do licenciamento.
Estabilidade da solução de software	Número de chamados de severidade 1	03	De 04 a 06: Glosa de 1% do valor do licenciamento. De 06 a 08: Glosa de 3% do valor do licenciamento. Acima de 08: Glosa de 5% do valor do licenciamento.
Tempo de início atendimento de suporte	% de chamados com início de atendimento nos prazos previstos	90%	De 85% a 90%: Glosa de 1% do valor mensal dos serviços especializados. De 75% a 85%: Glosa de 3% do valor mensal dos serviços especializados. Abaixo de75%: Glosa de 5% do valor mensal dos serviços especializados.
Tempo de término de atendimento de suporte	% de chamados com fim de atendimento nos prazos previstos	90%	De 85% a 90%: Glosa de 1% do valor mensal dos serviços especializados. De 75% a 85%: Glosa de 3% do valor mensal dos serviços especializados. Abaixo de75%: Glosa de 5% do valor mensal dos serviços especializados.
Prazo para implantação da solução	% máximo de atraso para finalizar a execução da implantação, após emissão de OF.	10%	De 10% a 20%: Glosa de 1% do valor do licenciamento. De 20% a 30%: Glosa de 3% do valor do licenciamento. Acima de 30%: Glosa de 5% do valor do licenciamento.

- Para os serviços especializados:

Indicador	Métrica	SLA	Penalidade
Aderência dos perfis da equipe técnica	Consultores totalmente aderentes ao perfil especificado	100%	De 75% a 100%: Glosa de 1% do valor mensal dos serviços especializados. De 50% a 75%: Glosa de 3% do valor mensal dos serviços especializados. Abaixo de 50%: Glosa de 5% do valor mensal dos serviços especializados.
Prazo para início da execução dos serviços técnicos	% de OSs iniciadas no prazo	90%	De 85% a 90%: Glosa de 1% do valor mensal dos serviços especializados. De 75% a 85%: Glosa de 3% do valor mensal dos serviços especializados. Abaixo de75%: Glosa de 5% do valor mensal dos serviços especializados.

3.4.3.2. As aferições dos SLAs serão feitas mensalmente e poderão ser acumulativas, limitadas a um total de 10% do valor mensal dos serviços executados.

3.4.3.3. Para aferição dos níveis mínimos de serviço, a CONTRATADA deverá apresentar mensalmente relatório de atividades executadas, bem como relatório de suporte da solução contendo todas as informações necessárias à avaliação dos indicadores.

3.4.3.4. Nos casos em que a responsabilidade pelo não cumprimento dos SLAs não for de responsabilidade da CONTRATADA, esta deverá realizar as devidas justificativas e, caso sejam consistentes, as penalidades referentes à justificativa serão desconsideradas.

3.5. **Da forma de comunicação e acompanhamento da execução do contrato**

3.5.1. A forma de comunicação e acompanhamento da execução do contrato deverá ocorrer de formalmente, utilizando meios eletrônicos. Os seguintes meios poderão ser utilizados:

3.5.1.1. Ordem de Serviço: Utilizado para autorização de execução de serviços.
3.5.1.2. Termo de Recebimento Provisório: Utilizado para formalizar o recebimento, em caráter provisório, dos serviços de uma OS.
3.5.1.3. Termo de Recebimento Definitivo: Utilizado para formalizar o recebimento, em caráter provisório, dos serviços de uma OS.
3.5.1.4. Relatório de Atividades: Utilizado para formalizar as atividades executadas em uma OS.
3.5.1.5. Relatórios Técnicos: Utilizadas como produto dos serviços técnicos.
3.5.1.6. E-mail: Utilizado para comunicação em geral, demandas, solicitações formais, devendo ser responsabilidade de ambas as partes acompanhar as caixas de e-mail durante toda execução contratual, dentro do horário comercial.
3.5.1.7. Mensagens instantâneas e ligações: Utilizado para comunicação em geral, demandas, solicitações formais, devendo ser responsabilidade de ambas as partes acompanhar os aplicativos e telefones durante toda execução contratual, dentro do horário comercial. Para comunicações que envolvam autorizações, mesmo sendo utilizado mensagens e ligações, a formalização pelos instrumentos formais deverá ocorrer.

3.6. **Do recebimento**
3.6.1. As entregas dos serviços de software deverão ser feitas mediante os relatórios técnicos definidos neste termo de referência em formato digital e local indicado pelo TJPA.
3.6.2. As entregas dos produtos dos serviços técnicos especializados deverão ser feitas formalmente em formato digital em local indicado pelo TJPA.
3.6.3. A formalização e evidencia da entrega dos produtos caracteriza a emissão do Termo de Recebimento Provisório. A partir deste momento, o TJPA irá realizar as aferições de qualidade e níveis mínimos de serviço.
3.6.4. Em um prazo máximo de 10 dias, o TJPA irá aferir os produtos e os níveis mínimos de serviço. Caso estejam em conformidade, o TJPA irá emitir, formalmente, termo de recebimento definitivo. Caso não esteja, o TJPA irá devolver à CONTRATADA para que realize as devidas correções. Se as correções não forem possíveis, o TJPA irá aplicar as glosas cabíveis.
3.6.5. No caso de devolução da entrega para a CONTRATADA, esta terá o prazo máximo de 05 dias úteis para realizar as devidas correções e realizar uma nova entrega.

3.6.6. **Do recebimento provisório**
3.6.7. O recebimento provisório se dará mediante a formalização de entrega dos produtos definidos nas Ordens de Serviço. A formalização de entrega deverá apontar o local onde os produtos foram entregues, respeitando as definições do TJPA.
3.6.8. Em um prazo máximo de 10 dias, o TJPA irá aferir os produtos e os níveis mínimos de serviço. Caso estejam em conformidade, o TJPA irá emitir, formalmente, termo de recebimento definitivo. Caso não esteja, o TJPA irá devolver à CONTRATADA para que realize as devidas correções. Se as correções não forem possíveis, o TJPA irá aplicar as glosas cabíveis.

3.6.9. **Do recebimento definitivo**
3.6.10. O recebimento em definitivo ocorrerá após a validação dos produtos entregues de cada Ordem de Serviço e será formalizada pela emissão de termo de recebimento definitivo.
3.6.11. Após a emissão do termo de recebimento definitivo, a CONTRATADA poderá iniciar os procedimentos de faturamento.

3.7. **Da forma de pagamento**

3.7.1. Os pagamentos ocorrerão após a execução das Ordens de Serviço, e emissão do Termo de recebimento definitivo da ordem de serviço em questão.

3.7.2. Para os itens 1,2 e 3 (licenças de software dos módulos de monitoramento e análise de desempenho de aplicações, acessos a aplicação e análise da segurança das aplicações) o pagamento será realizado integralmente para o período de 24 meses, trinta dias pós a emissão do termo de recebimento definitivo da Ordem de Serviço gerada para a implantação da solução de software, conforme especificado neste termo de referência.

3.7.3. Os serviços técnicos especializados serão pagos, mensalmente, mediante a conclusão e emissão de termo de aceite dos serviços demandados.

3.7.4. Todos os pagamentos serão feitos mediante a aferição dos níveis mínimos de serviço e, caso não sejam atingidos e forem passíveis de glosas, as mesmas serão aplicadas e deduzidas do pagamento.

3.7.5. Os valores para essa contratação foram previstos no Plano Orçamentário do Tribunal de Justiça do Estado do Pará, referente à Secretaria de Informática, vigente para o exercício de 2021 e no Plano de Contratações de Soluções de TIC para 2021. Os valores serão remanejados das Notas de Reservas originalmente nas 2021/497, 2021/502, 2021/536 e 2021/570 (relacionadas às ações 8651, 8652 e 8653, fontes 0101 e 0112, elemento de despesa 3.3.90.40), as quais estão rateadas em 65% no 1G, 9% no 2G e 26% no Apoio Indireto.

3.8. **Da transferência de conhecimento**

3.8.1. No prazo de até 30 dias que antecede o encerramento contratual, desde que não seja viável a renovação, a CONTRATADA deverá realizar reuniões de transferência de conhecimento para repasse à equipe do TJPA ou outra indicada pelo TJPA. Tais reuniões deverão ser orientadas pelo plano de transição contratual e focada na transferência de conhecimento da tecnologia e dos procedimentos operacionais e de gestão. Independente do encerramento contratual, a qualquer momento durante a vigência contratual, o TJPA poderá solicitar reuniões de repasse de conhecimento e a CONTRATADA deverá atender.

3.8.2. Em uma eventual interrupção contratual poderá ocorrer ou pelo vencimento do contrato ou por cancelamento/inexecução do mesmo antes do prazo de vencimento. Em cada uma das situações, as seguintes ações deverão ser tomadas:

- Encerramento contratual por vencimento do prazo:
  - Renovação contratual se possível, dentro dos limites e procedimentos permitidos por lei;
  - Iniciar procedimento de contratação, caso não seja possível a renovação. Estes procedimentos devem ser iniciados em um prazo de até 90 dias antes do encerramento contratual. Após a contratação, caso seja empresa diferente da executora atual, realizar repasse dos procedimentos e conhecimentos.
- Encerramento contratual por cancelamento ou inexecução antes do vencimento do prazo:
  - Convocar a próxima colocada no processo licitatório;
  - Acionar a atual CONTRATADA para executar os procedimentos de transição contratual.

3.8.3. A CONTRATADA deverá, após a implantação da solução, disponibilizar à equipe do TJPA usuário e senha que permita acessar de forma irrestrita todos os módulos da solução. Tais credenciais deverão ficar sob a responsabilidade

da TJPA e, caso seja necessário realizar a troca de senhas, estas devem estar sempre em posse da TJPA;

3.8.4. A CONTRATADA deverá, ao final da implantação da solução, realizar a demonstração da solução e seus módulos de forma a realizar um repasse das soluções implantadas. Além disso, deverá documentar e disponibilizar à equipe do TJPA documento que indique os endereços eletrônicos e links para acesso a todos os módulos da solução, bem como esclarecer em documentos como estes componentes se comunicam e a visão macro arquitetural da solução e seus módulos;

3.8.5. A CONTRATADA deverá, sempre que solicitado pelo TJPA e durante toda a vigência do contrato, realizar repasse de procedimentos de gestão e operação da solução e serviços executados;

3.8.6. Ao final da execução contratual, caso não seja possível a renovação por quaisquer motivos, a contratada deverá elaborar plano de transição contratual contendo ao menos as seguintes informações:

- Procedimentos técnicos operacionais referente a solução implantada;
- Acessos e senhas administrativas para uso da solução e seus módulos;
- Endereços de instalação da solução e seus módulos;
- Atualização da documentação de arquitetura da solução e de como estão integrados os módulos;
- Procedimentos de gestão e operação dos serviços de integração;
- Padrões utilizados;
- Toda e qualquer documentação necessária à operação e continuidade da solução implantada e da execução dos serviços;
- Caberá ainda à CONTRATADA, como obrigação contratual, realizar reuniões de repasse de conhecimento à equipe do TJPA ou outra indicada pelo TJPA.

3.9. **Dos direitos de propriedade intelectual e autoral**

3.9.1. Todo os produtos e conhecimentos gerados pela execução contratual são de propriedade do TJPA e não poderão ser utilizados pela contratada sem a prévia autorização do TJPA.

3.10. **Da qualificação técnica dos profissionais**

3.10.1. Os serviços devem ser executados por profissionais com as seguintes qualificações:

- Formação em nível superior na área de tecnologia, ou em outra área, desde que acompanhada de pós-graduação da área de TIC;
- Experiência na operação e configuração da ferramenta de software a ser utilizada;
- Experiência em análise de problemas de aplicações e infraestrutura, nas tecnologias utilizadas pelo TJPA;
- Experiência na avaliação e análise da qualidade dos usuários de aplicações;
- Experiência em análise de desempenho de aplicações;
- Experiência na avaliação e análise de vulnerabilidade de aplicações;
- Experiência em arquitetura de software nas tecnologias utilizadas no TJPA;
- Experiência em análise de problemas de aplicações e infraestrutura, nas tecnologias utilizadas pelo TJPA;
- Experiência na avaliação e análise da qualidade dos usuários de serviços digitais;

- Certificado oficial do fabricante, atestando competência na operação de todas as ferramentas de software que serão contratadas para este projeto.

3.10.2. As exigências de formação acadêmica, experiência profissional e certificação serão comprovadas por meio diploma ou certificado da instituição de ensino, de vínculos empregatícios (carteira de trabalho ou contrato social - no caso de sócio integrante de equipe técnica), e, caso o vínculo não comprove a experiência profissional exigida, será aceita declaração emitida pela empresa e/ou atestado de capacidade técnica emitido por órgão público ou empresa privada, sujeitando-se a diligência na sede da CONTRATADA ou do emitente do atestado para comprovação da experiência declarada, a critério do TJPA;

3.10.3. A CONTRATADA deverá apresentar toda a documentação necessária para a comprovação da formação acadêmica, experiência profissional e certificações ao TJPA, que poderá solicitar documentos adicionais para comprovação da conformidade.

3.10.4. A equipe do TJPA poderá realizar entrevista técnica com os colaboradores apresentados pela contratada, podendo aprovar ou não a alocação.

3.10.5. A qualquer momento, durante a execução, desde que devidamente justificado, o TJPA poderá solicitar a substituição de um profissional.

3.10.6. A contratada terá o prazo máximo de 10 dias úteis para realizar a substituição, caso seja solicitada e justificada pelo TJPA.

3.10.7. Os conhecimentos exigidos para cada perfil técnico serão comprovados por meio de avaliação curricular e entrevista a ser realizada pelo TJPA, a qual poderá rejeitar a indicação do profissional em avaliação;

3.10.8. Em relação à obrigatoriedade de certificações justifica-se pela necessidade de qualificação comprovada do perfil profissional, por uma entidade externa, CONSIDERANDO AS DETERMINAÇÕES DO TCU quanto à implementação das Boas Práticas em TI, conforme preconizam os acórdãos referidos abaixo, onde constam os itens específicos de capacitação e perfil profissional:

> * Acórdão 667/2005-TCU-Plenário.
> *" 9.3.12. defina, nos editais, os cursos superiores e técnicos requeridos, bem como a forma de comprovação da aptidão dos profissionais prestadores de serviço, visando a garantir a utilização de pessoal devidamente qualificado na execução do contrato.*
>
> * Acórdão 449/2005-TCU-Plenário.
> *" 9.2.2. imprecisão dos requisitos de qualificação de pessoal, pois não constam do edital indicações dos cursos superiores admitidos, ou exigidos, e das formas de avaliação da experiência na função do profissional oferecido, em desacordo com a determinação contida no item 9.3.7 do Acórdão 1094/2004 - Plenário.*
>
> * Acórdão 1.094/2004-TCU-Plenário.
> *" 9.3.7. defina, no edital e no contrato a ser celebrado, os requisitos relativos ao quantitativo e à qualificação do quadro de pessoal da empresa contratada que deverão ser satisfeitos por ocasião da execução do contrato.*

3.11. **Das sanções**

3.11.1. Com fundamento no art. 7º da Lei nº 10.520/02 e no art. 28 do Decreto nº 5.450/05, ficará impedida de licitar e contratar com a União, os Estados, o

Distrito Federal e os Municípios e será descredenciada no SICAF e no cadastro de fornecedores da CONTRATANTE, pelo prazo de até 5 (cinco) anos, garantida a ampla defesa, sem prejuízo da multa de 10% (dez por cento) sobre o valor adjudicado para quaisquer das condutas abaixo e demais cominações legais a CONTRATADA que:

- Apresentar documentação falsa;
- Ensejar o retardamento da execução do objeto;
- Falhar ou fraudar na execução do contrato;
- Comportar-se de modo inidôneo;
- Fizer declaração falsa;
- Cometer fraude fiscal;
- Não mantiver a proposta.

3.11.2. Pela inexecução total ou parcial do objeto definido neste Termo de Referência, a CONTRATANTE poderá, garantida a prévia defesa, aplicar à CONTRATADA as seguintes sanções, segundo a gravidade da falta cometida:

I - Advertência escrita quando se tratar de infração leve, a juízo da fiscalização, no caso de descumprimento das obrigações e responsabilidades assumidas nesta contratação ou, ainda, no caso de outras ocorrências que possam acarretar prejuízos à CONTRATANTE, desde que não caiba a aplicação de sanção mais grave;

II - Multas:

a) multa moratória de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, observado o máximo de 2% (dois por cento) no caso de inobservância do prazo fixado para apresentação da garantia;

a.1) O atraso superior a 25 (vinte e cinco) dias autoriza a CONTRATANTE a promover a rescisão do Contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei nº 8.666/93;

b) multa compensatória de 5 % (cinco por cento) pela não manutenção das condições de habilitação e qualificação exigidas no instrumento convocatório, a qual será calculada sobre o valor total da parcela não adimplida do Contrato;

c) multa compensatória de 20 % (vinte por cento) sobre o valor total do Contrato, no caso de rescisão por inexecução total do objeto;

d) multa compensatória de 20 % (vinte por cento) aplicada de forma proporcional à obrigação inadimplida, em caso de rescisão por inexecução parcial do objeto;

e) multas compensatórias vinculadas ao descumprimento do Nível Mínimo de Serviço, conforme descrito neste Termo Referência;

f) multa compensatória de 1% (um por cento) sobre o valor apurado para pagamento no mês de inadimplemento, no caso de não atendimento de qualquer das condições estabelecidas neste Termo de Referência, por ocorrência, no limite máximo de 10% (dez por cento) para a mesma ocorrência;

III - Suspensão temporária do direito de participar de licitações e impedimento de contratar com a Administração, por prazo não superior a 02 (dois) anos;

IV - Impedimento de licitar e contratar com a União com o consequente descredenciamento no SICAF pelo prazo de até 5 (cinco) anos; e

V - Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos que determinaram sua punição ou até que seja promovida a sua reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA

ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso III.

3.11.3. Também ficam sujeitas às penalidades III e V do item 12.2, conforme art. 87, III e IV da Lei n.º 8.666, de 1993, a CONTRATADA que:
- Tenha sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;
- Tenha praticado atos ilícitos visando a frustrar os objetivos da licitação;
- Demonstre não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

3.11.4. As sanções de multa podem ser aplicadas à CONTRATADA juntamente com a de advertência, suspensão temporária e a declaração de inidoneidade para licitar e contratar com a Administração do TJPA e impedimento de licitar e contratar com a União, Estados, Distrito Federal e Municípios.

3.11.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

3.11.6. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

3.11.7. As multas devidas e/ou prejuízos causados à CONTRATANTE serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

3.11.8. Caso a CONTRATANTE determine, a multa deverá ser recolhida no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela CONTRATANTE.

3.11.9. As penalidades serão obrigatoriamente registradas no SICAF.

4. DOS REQUISITOS TÉCNICOS ESPECÍFICOS

4.1. A solução a ser contratada consiste na aquisição de uma solução de software juntamente com serviços técnicos especializados na operacionalização e utilização da referida solução de software a fim de que se possa alavancar os resultados pretendidos. A solução foi dividida em 03 módulos, por possuírem métricas distintas de mensuração. Os serviços foram estimados em um único grupo de atividades, pois o perfil profissional para execução é o mesmo.

4.2. Abaixo, seguem os requisitos técnicos da solução, separada em módulos:

4.2.1. <u>Módulo de monitoramento e análise de desempenho de aplicações</u>
- O Módulo deverá ter controle de acesso e permissões;
- O Módulo deverá ser compatível com o ambiente computacional do TJPA;
- O Módulo deverá ser capaz de coletar, analisar e gerar informações das aplicações do TJPA;
- O Módulo deve possuir funcionalidade e ferramental para possibilitar a análise de logs de dados. Esta funcionalidade deve permitir a criação de regras de padrão para pesquisa, bem como ações a serem executadas (como por exemplo gerar um alerta) no caso de encontrar uma quantidade determinada de ocorrências no log analisado;
- O Módulo deverá disponibilizar ferramenta de análise das informações considerando a temporalidade. Desta forma, deverá permitir as análises e visualização das informações considerando:
  - Período de tempo (data/hora/minuto inicial e data/hora/minuto final);
  - Comparação entre dois períodos de tempo (antes e depois);

  - Granularidade de informações de 2 minutos ou mais;
- O Módulo deverá realizar, de forma automática sem a alteração manual de código-fonte e arquivos de configuração, o mapeamento dos componentes e seus relacionamentos que sustentam as aplicações. Tal mapeamento deve considerar, ao menos, os serviços (software), processos, infraestrutura (servidores e demais ativos) e seus relacionamentos que sustentam cada uma das aplicações do TJPA;
- O Módulo deverá permitir que seja definido critérios de sucesso para uma aplicação de forma que, a partir dessa definição o Módulo possa acompanhar as plataformas de serviço do TJPA registrando a taxa de sucesso dos usuários das aplicações;
- O Módulo deverá permitir a configuração de mais de um critério de sucesso para uma mesma aplicação;
- O Módulo deverá possibilitar que seja feita a análise das taxas de sucesso ao longo do tempo, permitindo que seja analisado a melhora ou não dos objetivos das aplicações.
- O Módulo deverá coletar e medir a taxa de abandono das aplicações. Entende-se por taxa de abandono de aplicações o percentual de acessos de usuários que acessaram a aplicação e saíram sem realizar uma transação negocial propriamente dita.
- O Módulo deverá avaliar o nível de qualidade das aplicações, possibilitando a análise temporal dessa qualidade. Além disso, deverá possibilitar a avaliação desse nível de qualidade considerando as regiões geográficas da origem do acesso.
- O Módulo deverá permitir a criação de áreas geográficas baseadas em IP's ou range de IP's, possibilitando a coleta, agrupamento e análise das informações de acesso dos usuários por área criada.
- O Módulo deverá identificar, de forma automática para uma aplicação em específico, quais serviços estão relacionados a ela. Além desta identificação, deverá registrar o tempo médio de execução, o volume de falhas e requisições.
- O Módulo deverá coletar e analisar a forma de acesso às aplicações, identificando as atividades de entrada (primeira atividade ao acessar as aplicações) e as atividades de saída (última ação executada antes de deixar a aplicação). Para estas atividades, O Módulo deverá identificar e registrar, além do volume, o tempo médio de duração.
- O Módulo deverá disponibilizar funcionalidade que permita a avaliação proativa das aplicações do TJPA. Entende-se por proativa a análise independente do uso pelos usuários finais. Para esta análise, o Módulo deverá disponibilizar:
  - Ferramenta para definição do acesso à aplicação que será avaliada, bem como a gravação de script de simulação;
  - A ferramenta deverá permitir que seja contemplado no script de gravação ações reais dos usuários, simulando, de fato, o acesso que o usuário faz ao acessar a aplicação;
  - A simulação do acesso à aplicação, conforme definição e script gravado, deverá ser executada a partir da Internet (fora das dependências do TJPA), permitindo desta forma, uma visão acurada, pelo prisma usuário, das aplicações;
  - A possibilidade de executar estas simulações a cada 5 minutos (no mínimo) e de ao menos 3 origens distintas;
  - Ferramenta para coletar os dados de tempo de cada atividade simulada, exibindo estes dados ao longo do tempo.

- Visando a avaliação da qualidade das aplicações, o Módulo deverá disponibilizar funcionalidade para identificar e analisar as falhas das aplicações. Assim sendo, o Módulo deve disponibilizar os seguintes requisitos relativos à avaliação de qualidade:
    - Avaliar, de forma automática, os níveis de qualidade das aplicações de forma que, quando algum serviço for impactado, o Módulo deverá gerar alerta automático, apontando o problema, o impacto (inclusive negocial), usuários afetados (inclusive individualmente) e a origem do mesmo;
    - Com o objetivo de evitar que sejam gerados vários alertas referentes a um mesmo problema, O Módulo deve ter a inteligência de correlacionar sub eventos a um evento "pai", gerando um único alerta;
    - Deve disponibilizar ferramenta para análise da evolução da falha, possibilitando a sua reprodução e cor relacionamento dos componentes de tecnologia impactados pela falha.
    - Com o objetivo de possibilitar uma análise multidisciplinar de uma falha, o Módulo deve disponibilizar mecanismo para a análise de todas as informações coletadas na janela de tempo da falha.
- O Módulo deve permitir a análise detalhada da qualidade dos componentes tecnológicos que suportam as aplicações, como por exemplo, serviços, servidores (hosts), banco de dados e rede. Para esta análise de qualidade, o Módulo deverá disponibilizar as seguintes informações:
    - Nível de utilização do recurso ou aplicação;
    - Tempo de resposta do recurso ou aplicação;
    - Volume de falhas;
- Estas informações devem ser disponibilizadas de forma individual para cada recurso ou serviço;
- Ainda em relação à análise detalhada da qualidade dos componentes tecnológicos, o Módulo deverá disponibilizar mecanismos integrados de avaliação de falhas para cada chamada individual a um serviço, identificando e correlacionando as chamadas aos bancos de dados e a análise em nível de código-fonte das aplicações do TJPA;
- O Módulo deverá disponibilizar ferramenta para possibilitar a criação de painéis e relatórios. Estes painéis e relatórios devem conter informações e métricas coletadas pelo Módulo e detalhada nestes requisitos. Além disso, deve disponibilizar painéis já configurados e possibilitar a configuração e adequação dos mesmos. Deve também permitir a criação de várias visões e o compartilhamento destes painéis.
- O Módulo deverá disponibilizar informações a respeito do tempo de resposta, volumetria de acesso e disponibilidade entre as aplicações do TJPA e de componentes ou serviços de terceiros. Por serviços de terceiros, entende-se serviços, acessados pelas aplicações do TJPA, que não fazem parte da infraestrutura gerenciada pelo TJPA.
- Para a geração de relatórios e painéis, o Módulo deverá permitir que os mesmos sejam gerados avaliando intervalos de tempo, correlacionando e agregando informações. Para isso, não poderá utilizar de programação de software, ou seja, deve disponibilizar mecanismos onde usuários com treinamento do Módulo possam gerar e customizar seus próprios painéis e relatórios.
- O Módulo deverá ser hospedado em nuvem, própria ou de terceiros. No entanto, caso haja a necessidade de instalação de componentes para realizar a coleta das informações, este poderá ser instalado nos servidores

do TJPA, desde que respeitado as questões de segurança e recursos já detalhados nesse elemento técnico.

- O Módulo de software utilizado pela contratada deverá garantir as questões de segurança da informação.
- O Módulo deverá dispor de mecanismos de autenticação e controle de níveis de acesso, possibilitando que seja autorizado acesso apenas para consulta aos dados.
- Para a implantação e coleta de dados do Módulo, deverão ser garantidas as questões de sigilo de senhas e dados sensíveis, não sendo permitido que estas informações fiquem disponíveis sem proteção para serem consultadas e visualizadas no Módulo. O Módulo deve permitir a configuração de dados sensíveis para que estes não sejam exibidos de forma aberta aos usuários e consultores.
- O Módulo de software fornecido deverá garantir o sigilo aos dados pessoais, estando aderente aos requisitos definidos da LGPD - Lei Geral de Proteção de dados nº 13.709/18, nos artigos 6º a 46º, 48º e 50º.
- O Módulo de software a ser fornecido, caso necessite de instalação de módulo coletor nos servidores e infraestrutura do TJPA (agente), deve garantir que não sejam geradas vulnerabilidades de criticidade elevada ao ambiente do TJPA. Além disso, a instalação de módulos coletores deverá ocorrer de forma automática, sem a necessidade de alterações manuais em arquivos fontes e arquivos de configuração da aplicação. A ativação e desativação de monitoramento de host deve ser feita a partir da console central, sem a necessidade de alteração manual de arquivos de configuração ou restart de aplicações.
- O Módulo deverá ser compatível com o ambiente tecnológico do TJPA e capaz de analisar o ambiente dimensionado.

4.2.2. Módulo de monitoramento e análise dos acessos à aplicação

- O Módulo deverá coletar e identificar o perfil dos usuários das aplicações do TJPA. Os seguintes parâmetros devem ser considerados para identificação do perfil dos usuários das aplicações:
  - Usuários regressos;
  - Localização física do usuário (UF);
  - Tipo de dispositivo para acesso;
  - Tipo de navegador utilizado para acesso;
  - Tipo de sistema operacional utilizado;
  - Operadoras utilizadas;
  - Número de ações do usuário durante o uso;
  - Tempo médio que os usuários permaneceram acessando o serviço digital;
  - Quantidade média de ações dos usuários durante o uso;
  - A sazonalidade diária no uso dos serviços digitais;
- O Módulo deverá, para as aplicações do TJPA que requerem autenticação, identificar o usuário que o está acessando.
- O Módulo deverá classificar automaticamente a qualidade dos acessos dos usuários às aplicações do TJPA. Deverá fazer isso para cada acesso de usuário. A qualidade deverá ser classifica considerando ao menos 03 níveis (ruim, bom e excelente).
- O módulo, quando a tecnologia da aplicação do TJPA permitir, deverá gravar, para até 50% dos usuários, o acesso às aplicações, possibilitando a sua reprodução. Ao efetuar tal gravação, terá como premissas as questões de

sigilo às informações, pois as informações digitadas pelos usuários devem ser mascaradas;

- Para cada acesso a uma aplicação, o Módulo deverá realizar uma análise detalhada do mesmo, identificando a região de origem, a qualidade do acesso, o tipo de navegador, a versão do sistema operacional, o IP de origem e o comportamento temporal das ações e funcionalidades acessadas no serviço digital.
- O Módulo deverá verificar o comportamento de uso das aplicações, registrando o volume de usuários que utilizam a aplicação, bem como o tempo médio que os usuários permaneceram utilizando a aplicação.
- O Módulo deverá possibilitar a coleta e análise de todas as interações (acessos, ações, cliques) do usuário com as aplicações;
- O Módulo deverá permitir a comparação do desempenho das aplicações pela perspectiva do usuário;
- O Módulo deverá detectar de forma automática, transações chaves para o negócio do TJPA que estejam apresentando problemas ou baixo desempenho;
- O Módulo deverá apresentar, no mínimo, as seguintes métricas em relação às ações dos usuários:
  - Quantidade de Bytes baixados;
  - Tempo médio de interatividade do usuário com o serviço digital;
  - Tempo no servidor;
  - Tempo no browser do usuário;
  - Tempo de tráfego de rede.
- O Módulo deve permitir a análise das ações de usuários mais lentas e mais rápidas;
- O Módulo deve coletar e analisar o tempo exato de carregamento da página até que a mesma esteja completamente pronta para utilização do usuário, separando essa métrica ainda por: localidade, tipo de dispositivo, localização, sistema operacional ou tipo de navegador;
- Buscando identificar o uso que os usuários fazem das aplicações do TJPA, o Módulo deverá prover as seguintes informações a respeito das aplicações, inclusive durante o tempo:
  - Volume de atividades/ações;
  - Tempo de atendimento (deverá permitir analisar a média e os 10% mais lento);
  - Volume de falhas dos serviços (falhas http e JavaScript);
  - Volume de uso de recursos externos ao serviço digital;
  - Tempo médio de resposta dos recursos externos ao serviço digital.

4.2.3. <u>Módulo de monitoramento e análise da segurança das aplicações</u>

- O Módulo deverá realizar teste dinâmico de segurança em aplicação web (DAST - *dynamic application security testing*), identificando falhas de segurança e vulnerabilidades contidas dentro do desenvolvimento da aplicação.
- O Módulo deve permitir a definição de uma política de segurança da aplicação, permitindo personalizações abaixo:
  - Aderência nos padrões de segurança abaixo:
    - OWASP;
    - SANS TOP 25;
    - PCI;
    - CERT;

- Lista de ID do CWE que a aplicação analisada não deve conter;
- Lista de severidades de falhas que a aplicação analisada não deve conter;
- Lista de categorias de falhas que a aplicação analisada não deve conter;
- Pontuação (score) mínima que a aplicação deve ter como resultado da verificação, tendo como base o CVSS (Common Vulnerability Scoring System);

- Aplicações devem conter um perfil/cadastro dentro do módulo, permitindo:
  - Definir um nome de identificação;
  - Definir descrição da aplicação e seu propósito;
  - Atrelar uma política de segurança do aplicativo (conforme requisitos definidos neste documento), onde a aplicação é avaliada perante os resultados não aderentes a sua política de segurança;
  - Definir quais times de desenvolvimento terão visibilidade da aplicação e seus resultados;
  - Histórico das análises DAST executadas, contendo seus resultados, bem como análise em execução.
- O motor (*engine*) de análise DAST deve realizar os testes de segurança, visando a identificação de falhas de segurança na aplicação web, atendendo os itens abaixo:
  - Origem das conexões do motor de análise deve utilizar blocos de IP previamente determinados;
  - Deve realizar análise em aplicações web disponíveis através dos protocolos HTTP e HTTPS;
  - A exclusão de determinadas URL (endereço web) deve ser permitida visando em evitar os testes de segurança em certas partes do aplicativo web;
  - A localidade da aplicação deve ser indicada através de sua URL, contendo o protocolo (HTTP ou HTTPS), a porta TCP onde o serviço está disponível e o caminho do recurso, conforme a sintaxe definida pela RFC 1738;
  - O motor da análise deve ser capaz de navegar pela aplicação web de forma automatizada, enumerando os links, páginas, cookies, parâmetros HTTP e demais componentes da aplicação web. O resultado deste procedimento deve ser alvo do teste de segurança realizado pelo motor da análise. Com base na URL fornecida, o motor de análise deve ser orientado quanto aos limites da aplicação web, evitando que o teste seja executado em outras aplicações. Deve conter ao menos os seguintes recursos:
    - Com base na URL informada, indicar se a navegação e testes de segurança podem ser executados:
      - Apenas no diretório final da URL;
      - No diretório final da URL e seus subdiretórios;
      - Remover limitação, permitindo o motor de análise a navegar em qualquer diretório.
  - O motor de análise deverá realizar autenticação na aplicação web que está sendo analisada, suportando as seguintes formas de autenticação:
    - Não autenticado;
    - Autenticação básica do HTTP;
    - Autenticação baseada em certificados de cliente em formato PKCS12.

- Identificar automaticamente formulários de autenticação e realizar a autenticação com base em usuário e senha previamente definidos;
- Importação de um roteiro de autenticação com base no Selenium IDE, onde o motor de análise repetirá o procedimento de autenticação, preenchendo formulários de autenticação e alterando opções/elementos da página de autenticação;
- Importação de roteiros de navegação personalizados devem ser suportados pela solução, onde, a partir da navegação manual pela aplicação web, seja gerado o roteiro de navegação personalizado e este seja usado pelo motor de análise para repetir as ações na aplicação web;
- Durante as requisições HTTP/HTTPS, o motor da análise deve indicar o campo "*User-Agent*" do protocolo HTTP (como descrito na RFC 2616). Este campo deve conter dados de navegadores comuns (Firefox, Chrome, Safari e Microsoft Edge), bem como suportar que seja informado um valor personalizado;
- Não deve existir um número máximo de links a serem testados e analisados pelo motor DAST, no entanto isto deve ser configurável, permitindo definir uma determinada quantidade de links máximos ou manter ilimitado;
- Durante a execução da análise, o motor DAST deve utilizar-se da tecnologia de *multithreading,* onde o teste é executado por mais que uma instância de processamento de forma simultânea e paralela;
- Visando em evitar testes desnecessários, deve ser possível informar tecnologias utilizadas pela aplicação web (como banco de dados e sistema operacional), removendo assim testes para tecnologias não utilizadas, as seguintes tecnologias devem ser suportadas: Oracle, SQL Server, PgSQL MySQL, Linux e Windows.
- Antes de realizar a execução da análise DAST, o motor deve realizar uma verificação prévia, visando em garantir os seguintes aspectos:
  - Servidor está acessível pelo motor da análise através da URL informada;
  - Dados de autenticação na aplicação web estão funcionando;
  - Motor de análise pode navegar pela aplicação.
- Tarefas de análise DAST deve podem ser executadas de imediato, bem como deve ser possível agendar um determinado dia e horário para iniciar uma tarefa.

- Relatório das falhas de segurança identificadas pela análise DAST deve conter:
  - Listagem das URL contempladas pela análise;
  - Sumário executivo listando as falhas de segurança identificadas, informando o número de identificações realizadas e agrupadas por suas severidades, seguindo o padrão CVSS (*Common Vulnerability Scoring System*);
  - Exportação do relatório em formato PDF;
  - Exportação do relatório em formato PDF seguindo os padrões do PCI;
  - Exportação dos dados que compõem o relatório em formato XML;
  - Relatório de aderência perante a política de segurança atrelada ao perfil da aplicação;
  - Estimativa de tempo de desenvolvimento para correção da falha de segurança;
  - Estimativa de linhas de código que necessitam ser alteradas para correção da falha de segurança;

  - Descritivo das falhas de segurança contendo a contextualização da mesma;
  - Recomendações para realização a correção das falhas de segurança identificadas.
- Metodologia de classificação e pontuação dos aplicativos e falhas deve estar aderente aos padrões abaixo:
  - NIST FIPS Pub. 199;
  - Common Weakness Enumeration (CWE);
  - Common Vulnerability Scoring System (CVSS).
- Falhas de segurança identificadas devem conter uma categorização atrelada a sua severidade e baseado com o CVSS (Common Vulnerability Scoring System), incluindo no mínimo as categorizações abaixo:
  - Muito alto;
  - Alto;
  - Médio;
  - Baixo;
  - Muito baixo;
  - Informativo.
- A solução deve conter as falhas definidas pelo CWE (Common Weakness Enumeration), tendo as atualizações em pelo menos 90 dias.
- Identificação de falhas de segurança tendo cobertura das categorias abaixo:
  - Problemas de autenticação;
  - Problemas de autorização;
  - Injeção de código;
  - Injeção de comandos ou parâmetros;
  - Gerenciamento de credenciais;
  - Injeção de CRLF (Carriage Return e Line Feed);
  - Cross-Site Scripting (XSS);
  - Problemas criptográficos;
  - Configuração de implantação;
  - Directory traversal;
  - Vazamento de informações;
  - Falta de validação da entrada de dados;
  - Injeção de comandos no sistema operacional;
  - Configurações do servidor;
  - Fixação de sessões;
  - Injeção de SQL.
- Identificação de falhas de segurança tendo cobertura dos itens abaixo conforme o Common Weakness Enumeration (CWE):
  - CWE 287 - Improper Authentication;
  - CWE 352 - Cross-Site Request Forgery (CSRF);
  - CWE 693 - Clickjacking/Content Security Policy insecure unsafe-inline directive used/Content Security Policy insecure unsafe-eval directive used;
  - CWE 285 - Improper Authorization;
  - CWE 98 - Improper Control of Filename for Include/Require Statement in PHP Program (PHP File Inclusion);
  - CWE 830 - Inclusion of Web Functionality from an Untrusted Source;
  - CWE 78 - Improper Neutralization of Special Elements used in an OS Command (OS Command Injection);
  - CWE 259 - Use of Hard-coded Password;
  - CWE 522 - Insufficiently Protected Credentials;
  - CWE 113 - Improper Neutralization of CRLF Sequences in HTTP Headers (HTTP Response Splitting);

- CWE 79 - Improper Neutralization of Input During Web Page Generation (Cross-site Scripting);
- CWE 80 - Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS);
- CWE 83 - Improper Neutralization of Script in Attributes in a Web Page;
- CWE 296 - Improper Following of Chain of Trust for Certificate Validation;
- CWE 297 - Improper Validation of Host-specific Certificate Data;
- CWE 298 - Improper Validation of Certificate Expiration;
- CWE 321 - Use of Hard-coded Cryptographic Key;
- CWE 326 - Inadequate Encryption Strength;
- CWE 327 - Use of a Broken or Risky Cryptographic Algorithm;
- CWE 614 - Sensitive Cookie in HTTPS Session Without Secure Attribute;
- CWE 402 - Transmission of Private Resources into a New Sphere (Resource Leak);
- CWE 668 - Exposure of Resource to Wrong Sphere;
- CWE 22 - Improper Limitation of a Pathname to a Restricted Directory (Path Traversal);
- CWE 200 - Information Exposure;
- CWE 209 - Information Exposure Through an Error Message;
- CWE 215 - Information Exposure Through Debug Information;
- CWE 526 - Information Exposure Through Environmental Variables;
- CWE 530 - Exposure of Backup File to an Unauthorized Control Sphere;
- CWE 538 - File and Directory Information Exposure;
- CWE 548 - Information Exposure Through Directory Listing;
- CWE 434 - Unrestricted Upload of File with Dangerous Type;
- CWE 601 - URL Redirection to Untrusted Site (Open Redirect);
- CWE 78 - Improper Neutralization of Special Elements used in an OS Command (OS Command Injection);
- CWE 16 – Configuration;
- CWE 642 - External Control of Critical State Data;
- CWE 757 - Selection of Less-Secure Algorithm During Negotiation (Algorithm Downgrade);
- CWE 384 - Session Fixation;
- CWE 89 - Improper Neutralization of Special Elements used in an SQL Command (SQL Injection).

- Caso a solução necessite de um servidor local para processamento e execução das tarefas de verificação DAST:
  - Deve ser fornecido junto com o as licenças, incluindo o hardware (servidor com fonte redundante, 2 interfaces de rede gigabit, para rack de 19", ocupando no máximo 1U), sistema operacional e demais custos envolvidos para permitir que o servidor local esteja em operação.
  - Deve ser capaz de executar tarefas de análise DAST em todas as aplicações simultaneamente.
- Caso a solução utilize serviço em nuvem, a mesma deve conter:
  - Comunicação segura através de TLS 1.2 ou mais recente, validando a procedência do certificado e recusando comunicação não confiável;
  - Possuir seguir e ser aprovada em auditoria quanto a SOC 2, SOC 3 e SSAE 16 tipo II SOC 1;
  - Governança da Segurança da Informação;
  - Avaliação e Tratamento de Riscos;
  - Política de segurança;
  - Organização da Segurança da Informação;

- Gestão de ativos;
- Segurança de Recursos Humanos;
- Segurança Física e Ambiental;
- Gestão de Comunicações e Operações;
- Controle de acesso.

- Deve permitir integração em esteiras de desenvolvimento, permitindo a automatização do processo de iniciar análise DAST, possuindo integração com Jenkins, bem como ferramenta de linha de comando.
- Deve possuir integração com plataformas de controle de defeitos (bug tracking), suportando:
  - Jira;
  - Jira Cloud;
  - Visual Studio Team Services;
  - Team Foundation Server (TFS);
  - BugZilla.
- Visando personalizações e integrações, a solução deve possuir API para execução de operações automatizadas na solução/plataforma, permitindo:
  - Criar, editar e deletar aplicações;
  - Criação e envio de tarefas de verificação DAST;
  - Criação, edição e deleção de times de desenvolvimento;
  - Listagem dos resultados das verificações DAST;
- Desenvolvedores devem ter acesso as falhas de segurança identificadas, contendo a contextualização da falha, local onde a falha foi identificada (URL, parâmetros e resposta do servidor), bem como as recomendações de correção.

Abaixo, seguem os requisitos dos serviços a serem executados:

- Os serviços devem compreender as seguintes atividades:
  - Operação da solução de software que for instalada para o projeto, contemplando a integração da solução com o ambiente do TJPA, a configuração de parâmetros, configuração dos usuários e acessos, configuração de painéis e relatórios, dentre outras;
  - Análise de falha ou degradação da qualidade das aplicações, contemplando as atividades de análise e avaliação de problemas e falhas que afetam as aplicações. Por problemas e falhas entende-se eventos que comprometam os índices de sucesso, o tempo de atendimento, falhas, erros e indisponibilidades das aplicações. O propósito deste serviço é identificar as causas que afetam os serviços digitais de forma rápida para que as ações de contingência e melhoria sejam implementadas há tempo de forma a não comprometer de forma significativa os serviços;
  - Análise e avaliação comportamental do uso das aplicações, contemplando as atividades de acompanhamento e avaliação de uma aplicação, observando o comportamento de uso dos usuários. Esta atividade visa o entendimento de como os usuários estão consumindo os serviços digitais do TJPA, observando os padrões comportamentais, dispositivos de acesso, funcionalidades mais acessadas, porta de entrada para os serviços, atividades executadas, dentre outras. É também através desse serviço que desvios no comportamento padrão, tanto de comportamento, quanto de tempo de resposta e volume de acesso são acompanhados e analisados.
  - Análise e acompanhamento dos índices de sucesso das aplicações, contemplando as atividades de análise, estudo, configuração e acompanhamento de indicadores que medem a eficiência negocial das aplicações. Além disso, contempla as atividades de avaliar

eventos que possam causar impactos aos índices de sucesso, apontando estratégias que visem a melhoria destes índices.

- Simulação de uso e avaliação da qualidade das aplicações, contemplando as atividades para permitir a simulação de uso e avaliação de qualidade de uma aplicação. A simulação deve ocorrer através de acessos de usuários virtuais simulando o uso da aplicação, bem como a análise do comportamento e qualidade da aplicação quando submetido a um volume de acessos simulados. Engloba as atividades de análise e definição do escopo de ações a serem avaliadas, a criação e configuração de scripts de simulação, a execução (a partir da Internet) dos acessos simulados, a coleta e análise dos indicadores de comportamento e qualidade do serviço digital. O volume de acesos simulados para esta atividade deve ser suficiente para simular um total de até 3.000 usuários virtuais simultâneos. Para a execução desta atividade, a contratada deverá disponibilizar, na Internet, toda a infraestrutura para simulação do uso das aplicações e não poderá haver custos adicionais para o TJPA.
- Elaboração de relatórios técnicos e negociais, contemplando as atividades de estudo, análise, avaliação e elaboração de relatórios técnicos referentes à avaliação técnica de aplicações, tanto quanto as questões avaliação da arquitetura de software, qualidade da construção, soluções técnicas, avaliação de banco de dados e armazenamento. Compreende o estudo técnico de soluções que possam agregar e melhorar as aplicações ofertados pelo TJPA. Contempla também a geração de relatórios com visões gerenciais e negociais a respeito das aplicações do TJPA, possibilitando uma análise e definição de melhores estratégias a respeito da implementação e disponibilização das aplicações aos usuários dos serviços.
- Apoio na definição e na implementação de ações de melhoria das aplicações, contemplando as atividades de apoio à definição e implementação de ações de melhoria das aplicações do TJPA. Entende-se como apoio à definição e implementação a proposição e apoio à implementação de configurações, codificação, ajustes de componentes de solução técnica, ajustes de arquitetura, melhorias de banco de dados, ajustes na infraestrutura, configurações de segurança, ajustes de usabilidade das aplicações, dentre outras, relacionadas às aplicações do TJPA. Estas atividades podem, ou não, estar relacionadas aos apontamentos realizados pelos relatórios de análise elaborados pelas outras atividades deste catálogo.
- Apoio na implementação e configuração de componentes tecnológicos, contemplando as atividades de instalação, configuração e *tunning* de soluções tecnológicas que sustentam as aplicações que podem ir desde a sistemas operacionais, soluções de virtualização, gerenciadores de contêineres, banco de dados, servidores de aplicação, servidores web, balanceadores de carga, ativos de rede, enfim, todo e qualquer arcabouço tecnológico que possa influenciar na qualidade, performance e segurança das aplicações e experiência dos usuários. Estas atividades podem, ou não, estar relacionadas aos apontamentos realizados pelos relatórios de análise elaborados pelas outras atividades deste catálogo.

4.3. Abaixo, seguem os requisitos tecnológicos e de implantação:

- A solução deverá ser implantada em nuvem própria ou de terceiros;

- O TJPA não irá disponibilizar infraestrutura para implantação da solução;
- A solução não poderá consumir mais do que 3% de CPU dos servidores monitorados;
- Para a implantação da solução, não será permitida a edição de código-fonte das aplicações para realizar instrumentação manual;
- A solução deverá ser compatível com o seguinte ambiente computacional e tecnologias do TJPA:

Recurso	Tecnologia	Características	Qtde
Servidores	Linux / Windows	RHEL 7 e 8 / Win 2016	42
Banco de dados	Postgresql	Versão11.11	3
Aplicações	Java/ Jboss/ PHP	Versões 6,7 e 8	3

4.4. Abaixo, seguem os requisitos temporais:

- Os serviços especializados deverão ser executados em horário comercial, de segunda-feira a sexta-feira, das 08hrs às 12hrs e das 13hrs às 17hrs. Eventualmente e, de comum acordo entre o TJPA e a contratada, este horário poderá ser revisto, porém sem redução da quantidade de horas diárias;
- As ferramentas de software disponibilizadas pela contratada deverão funcionar coletando e analisando informações em um regime de 24x7, ou seja, 24 horas por dia, 07 dias por semana;
- O Suporte técnico, manutenção e garantia deverão ser disponibilizados pela contratada durante toda a vigência contratual;
- A contratada deverá, num prazo máximo de 30 dias corridos após devidamente autorizado pelo TJPA, disponibilizar todas as ferramentas de softwares necessárias à execução do contrato. Ainda durante esse período, deverá instalar, configurar e integrar todos os módulos/ferramentas juntamente com o ambiente do TJPA;
- Após emissão de Ordem de Serviço, a contratada deverá disponibilizar, num prazo máximo de 05 dias úteis equipe técnica de consultores para execução dos serviços especializados;
- No prazo de 30 dias antes do encerramento do contrato, a contratada deverá realizar disponibilizar relatório de transição com o objetivo de realizar o repasse do projeto para garantir a continuidade dos serviços. Em caso de renovação, essa atividade não será necessária;
- Os serviços deverão ser executados remotamente ou, caso solicitado pelo TJPA, presencialmente nas dependências do TJPA, em Belém/PA.

4.5. Abaixo, seguem os requisitos de segurança:

- As ferramentas de software utilizadas pela contratada deverão garantir as questões de segurança da informação;
- As ferramentas deverão dispor de mecanismos de autenticação e controle de níveis de acesso, possibilitando que seja autorizado acesso apenas para consulta aos dados;
- Para a implantação e operacionalização das ferramentas, deverão ser garantidas as questões de sigilo de senhas e dados sensíveis, não sendo permitido que estas informações fiquem disponíveis sem proteção para serem consultadas e visualizadas nas ferramentas. As ferramentas devem permitir a configuração de dados sensíveis para que estes não sejam exibidos de forma aberta aos usuários e consultores;
- As ferramentas de software utilizadas pela contratada deverão garantir o sigilo aos dados pessoais, estando aderente aos requisitos definidos da LGPD - Lei Geral de Proteção de dados nº 13.709/18, nos artigos 6º a 46º, 48º e 50º;

- As ferramentas de software utilizadas pela contratada, caso necessitem de instalações de módulos coletores nos servidores e infraestrutura do TJPA, devem garantir que não sejam geradas vulnerabilidades ao ambiente do TJPA;
- A contratada, bem como os consultores que atuaram no projeto, devem assinar termo de sigilo e confidencialidade. Estes termos ter por objetivo garantir as questões de segurança da informação.

5. PROPOSTA DE MODELOS A SEREM UTILIZADOS

5.1. Os modelos utilizados nessa contratação consistem em:

5.1.1. Anexo A – Modelo de Proposta.

5.1.2. Anexo B – Modelo de Termo de Vistoria ou renúncia.

6. INFORMAÇÕES COMPLEMENTARES

6.1. **Visita técnica**

6.1.1. A empresa interessada em participar do processo licitatório poderá realizar vistoria técnica nas instalações físicas do TJJA, a fim de tomar ciência das condições locais e dos custos decorrentes do cumprimento das obrigações contratuais, no Av. Almirante Barroso n 3089 - Bairro: Souza - CEP: 66613-710 - Belém - PA, a ser agendada pelos e-mails arilson.silva@tjpa.jus.br ou paulo.lourinho@tjpa.jus.br ou ainda pelos telefones (91) 98366-9678 ou, (91) 98161-3141 nos horários das 8h às 17h.

6.1.2. A vistoria técnica tem por objetivo apresentar aos licitantes as reais condições em que serão executados os serviços, com destaque para as disponibilidades e limitações das instalações, do ambiente computacional físico e lógico, da infraestrutura, conectividade, fluxos e processos de trabalho etc., sobre as quais a inobservância poderá acarretar sérias distorções operacionais ou na formação do preço.

6.1.3. Assim, a vistoria técnica assegura a isonomia no domínio de informações relevantes para a construção de uma proposta comercial, assegurada a convicção sobre o preço ofertado e, consequentemente, como medida garantidora da redução de riscos da contratação e da futura gestão contratual.

6.1.4. Caso a LICITANTE não julgar necessária a realização da visita técnica, deverá apresentar declaração de desistência, que deverá ser devidamente assinada e anexada juntamente com a documentação de habilitação, abdicando do direito de se cientificar das condições locais, assumindo total responsabilidade pelas instalações e configurações da solução e a garantia do seu perfeito funcionamento, não sendo isenta do cumprimento das cláusulas contratuais, e devendo manter os custos apresentados na proposta.

6.1.5. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até dois dias úteis anteriores ao dia do certame, devendo o licitante ou seu representante estar devidamente identificado.

6.1.6. Após a realização da visita técnica, as empresas deverão entregar a declaração de vistoria conforme MODELO DE VISTORIA OU RENÚNCIA por meio da qual manifestarão o pleno conhecimento às condições.

6.1.7. Em nenhuma hipótese a LICITANTE poderá alegar desconhecimento, incompreensão, dúvidas ou esquecimento de qualquer detalhe relativo ao objeto, responsabilizando-se por quaisquer ônus decorrentes desses fatos;

Belém, 23 de junho de 2021.

ANEXO A – MODELO DE PROPOSTA DE PREÇO

PREGÃO XX/2021

OBJETO: Registro de preço para eventual contratação de serviços de solução de avaliação de performance, qualidade e segurança de aplicações, bem como serviços técnicos especializados de operação e análise, conforme especificações e quantidades detalhadas neste termo de referência.

EMPRESA: XXXXXXXXXXXXX						
MARCA/PRODUTO SOFTWARE: XXXXXXXXXXXXX						
Item	**Descrição**	**métrica**	**Qtde**	**Valor unit***	**Valor total anual**	**Valor 24 meses**
1	Módulo de monitoramento e análise de desempenho de aplicações	Pacote para 4 cores ou Pacote para 16 GB RAM	49			
2	Módulo de monitoramento e análise dos acessos a aplicação	Pacotes de um milhão de acessos por ano	2			
3	Módulo de monitoramento e análise da segurança das aplicações	Por aplicação	3			
4	Serviços técnicos especializados	Homem x hora	3.840			
				TOTAL		

*** Para os módulos de monitoramento e análise de desempenho, acessos e segurança, o valor unitário refere-se ao valor de uma licença do módulo pelo período de 12 meses. Para os serviços técnicos especializados o valor unitário refere-se ao valor da hora de serviço técnico em "Homem X hora".**

Preço total por extenso para 24 meses: XXXXXXXXXXXXX

Prazo de validade: (não inferior a 60 (sessenta) dias corridos, a contar da data de sua apresentação)

Composição dos preços: Nos preços propostos acima estão inclusas todas as despesas, frete, tributos e demais encargos de qualquer natureza incidentes sobre o objeto deste Pregão.

Esta empresa declara estar ciente de que a apresentação da presente proposta implica na plena aceitação das condições estabelecidas no Edital e seus Anexos.

(Local e data)

Nome da empresa

PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DO PARÁ
SECRETARIA DE INFORMÁTICA

(Assinatura do Representante Legal e NOME COMPLETO)

ANEXO B – MODELO DE TERMO DE VISTORIA OU RENÚNCIA

Declaro que:

( ) Vistoriei minuciosamente os locais para a prestação dos serviços constantes do objeto do Edital de Licitação nº __ /2021, e tomei conhecimento das reais condições de execução dos serviços, bem como coletei informações de todos os dados e elementos necessários à perfeita elaboração da proposta comercial e que será mantido o sigilo de todas as informações de que tomei conhecimento em razão da vistoria.

( ) Optei pela não realização de vistoria assumindo inteiramente a responsabilidade ou consequências por essa omissão, mantendo as garantias que vincularem a proposta ao presente processo licitatório, em nome da empresa que represento.

Dados da empresa:

Razão Social:
CNPJ/MF:
Endereço:
Tel/Fax:
e-mail:
CEP:
Cidade:
UF:

Dados do Representante Legal da Empresa:
Nome:
CPF:

(Local e data)

Nome da empresa

(Assinatura do Representante Legal e NOME COMPLETO)

ANEXO C – ITENS A SEREM DEMOSTRADOS NA PROVA DE BANCADA

1. Os itens dos requisitos abaixo deverão ser demostrados na prova de bancada:

Item	Descrição	Atende (Sim ou Não)
	Módulo de monitoramento e análise de desempenho de aplicações	
1	O Módulo permite controle de acesso e permissões?	
2	O Módulo é compatível com o ambiente computacional do TJPA?	
3	O Módulo é capaz de coletar, analisar e gerar informações das aplicações do TJPA?	
4	O Módulo possui funcionalidade e ferramental que possibilite a análise de logs de dados? Esta funcionalidade permite a criação de regras de padrão para pesquisa, bem como que ações a sejam executadas (como por exemplo gerar um alerta) no caso de encontrar uma quantidade determinada de ocorrências no log analisado?	
5	O Módulo disponibiliza ferramenta de análise das informações considerando a temporalidade considerando as análises e visualização das informações conforme abaixo? • Período de tempo (data/hora/minuto inicial e data/hora/minuto final) • Comparação entre dois períodos de tempo (antes e depois) • Granularidade de informações de 2 minutos ou mais.	
6	O Módulo realiza, de forma automática sem a alteração manual de código-fonte e arquivos de configuração, o mapeamento dos componentes (e relacionamentos entre) que sustentam as aplicações? Este mapeamento considera, ao menos, os serviços, processos, infraestrutura (servidores) e seus relacionamentos?	
7	O Módulo permite que sejam definidos critérios de sucesso para uma aplicação de forma que, a partir desta definição o Módulo possa acompanhar as plataformas de serviço do TJPA, registrando a taxa de sucesso dos usuários das aplicações?	
8	O Módulo permite a configuração de mais de um critério de sucesso para uma mesma aplicação?	
9	O Módulo possibilita que seja feita a análise das taxas de sucesso ao longo do tempo, permitindo assim que seja analisado a melhora ou não dos objetivos das aplicações?	
10	O Módulo coleta e meder a taxa de abandono das aplicações? (Entende-se por taxa de abandono de aplicações o percentual de acessos de usuários que acessaram a aplicação e saíram sem realizar uma transação negocial propriamente dita)	

PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DO PARÁ
SECRETARIA DE INFORMÁTICA

11	O Módulo consegue avaliar o nível de qualidade das aplicações, possibilitando a análise temporal dessa qualidade? É possível realizar esta avaliação considerando as regiões geográficas?	
12	O Módulo permite a criação de áreas geográficas baseadas em IPs ou range de IPs, possibilitando a coleta, agrupamento e análise das informações de acesso dos usuários por área criada?	
13	O Módulo identifica, de forma automática para uma aplicação em específico, quais serviços estão relacionados a ele, além de identificar o tempo médio de execução, o volume de falhas e requisições?	
14	O Módulo coleta e analisa a forma de acesso às aplicações, identificando as atividades de entrada (primeira atividade ao acessar as aplicações) e as atividades de saída (última ação executada antes de deixar a aplicação), além de identificar, volume e o tempo médio de duração.	
15	O Módulo disponibiliza, para as aplicações que for compatível, funcionalidade que permita a avaliação proativa das aplicações do TJPA? (Entende-se por proativa a análise independente do uso pelos usuários finais) Para esta análise, O Módulo disponibiliza os itens abaixo? • Ferramenta para definição do acesso à aplicação que será avaliado, bem como a gravação de script de simulação; • Ferramenta que permita que seja contemplado no script de gravação ações reais dos usuários, simulando, de fato, o acesso que o usuário faz ao acessar a aplicação; • Ferramenta que permita a simulação do acesso à aplicação, conforme definição e script gravado, sendo executado a partir da Internet? (fora das dependências do TJPA); • Agendamento que permita executar estas simulações a cada 5 minutos (no mínimo) e de ao menos 3 origens distintas; • Ferramenta para coletar os dados de tempo de cada atividade simulada, exibindo estes dados ao longo do tempo.	
16	Visando a avaliação da qualidade das aplicações, o Módulo deverá disponibilizar funcionalidade para identificar e analisar as falhas das aplicações. Assim sendo, o Módulo disponibiliza os seguintes requisitos relativos à avaliação de qualidade? • Avalia, de forma automática, os níveis de qualidade das aplicações de forma que, quando algum serviço for impactado, o Módulo gera alerta automático, apontando o problema, o impacto (inclusive negocial), usuários afetados (inclusive individualmente) e a origem do mesmo? • Com o objetivo de evitar que sejam gerados vários alertas referentes a um mesmo problema, O Módulo tem a inteligência de correlacionar sub-eventos a um evento pai, gerando um único alerta? • Disponibiliza ferramenta para análise da evolução da falha, possibilitando a sua reprodução e correlacionamento dos componentes de tecnologia impactados pela falha?	

	• Com o objetivo de possibilitar uma análise multidisciplinar de uma falha, O Módulo disponibiliza mecanismo para a análise de todas as informações coletadas na janela de tempo da falha?	
17	O Módulo permite a análise detalhada da qualidade dos componentes tecnológicos que suportam as aplicações, como por exemplo, serviços, servidores (hosts), banco de dados e rede? Para esta análise de qualidade, o Módulo disponibiliza as seguintes informações? • Nível de utilização do recurso ou aplicação; • Tempo de resposta do recurso ou aplicação; • Volume de falhas; • Estas são disponibilizadas de forma individual para cada recurso ou serviço?	
18	Ainda em relação à análise detalhada da qualidade dos componentes tecnológicos, o Módulo disponibiliza mecanismos integrados de avaliação de falhas para cada chamada individual a um serviço, identificando e correlacionando as chamadas a banco de dados e a análise em nível de código-fonte das aplicações do TJPA?	
19	• O Módulo disponibiliza ferramenta para possibilitar a criação de painéis e relatórios, conforme detalhamento abaixo? • Estes painéis e relatórios contém informações e métricas coletadas pelo Módulo e detalhada nestes requisitos? • Existem painéis já configurados e possibilidade de configuração e adequação dos mesmos? • Há a possibilidade de criação de várias visões e o compartilhamento destes painéis?	
20	O Módulo disponibiliza informações a respeito do tempo de resposta, volumetria de acesso e disponibilidade entre as aplicações do TJPA e de componentes ou serviços de terceiros? (Por serviços de terceiros, entende-se serviços, acessados pelas aplicações do TJPA, que não fazem parte da infraestrutura gerenciada pelo TJPA.)	
21	Para a geração de relatórios e painéis, o Módulo permite que os mesmos sejam gerados avaliando intervalos de tempo, correlacionando e agregando informações sem que para isto utilize de programação de software? (ou seja, deve disponibilizar mecanismos onde usuários com treinamento do Módulo possam gerar e customizar seus próprios painéis e relatórios.)	

22	O Módulo é hospedado em nuvem, própria ou de terceiros?	
23	Há a necessidade de instalação de componentes para realizar a coleta das informações nos servidores do TJPA? (tal necessidade é permitida desde que respeitadas as questões de segurança e recursos já detalhados neste elemento técnico)	
24	O Módulo de software utilizado garante as questões de segurança da informação?	
25	O Módulo dispõe de mecanismos de autenticação e controle de níveis de acesso, possibilitando que seja autorizado acesso apenas para consulta aos dados?	
26	Para a implantação e coleta de dados do Módulo, são garantidas as questões de sigilo de senhas e dados sensíveis? (Não deve ser permitido que estas informações fiquem disponíveis sem proteção para serem consultadas e visualizadas no Módulo) O Módulo permite a configuração de dados sensíveis para que estes não sejam exibidos de forma aberta aos usuários e consultores?	
27	O Módulo de software garante o sigilo aos dados pessoais, estando aderente aos requisitos definidos da LGPD - Lei Geral de Proteção de dados nº 13.709/18, nos artigos 6º a 46º, 48º e 50º?	
28	O Módulo de software garante que não sejam geradas vulnerabilidades de criticidade elevada ao ambiente do TJPA? (questão pertinente caso necessitem de instalações de módulos coletores nos servidores e infraestrutura do TJPA).	
29	A instalação de módulos coletores, ocorre de forma automática? (sem a necessidade de alterações manuais em arquivos fontes e arquivos de configuração da aplicação)	
30	É possível a desativação e ativação de monitoramento de host a partir da console central, sem a necessidade de alteração manual de arquivos de configuração ou restart de aplicações?	
Módulo de monitoramento e análise dos acessos a aplicação		

31	O Módulo deverá coletar e identificar o perfil dos usuários das aplicações do TJPA. Os seguintes parâmetros devem ser considerados para identificação do perfil dos usuários das aplicações: • Usuários regressos; • Localização física do usuário (UF); • Tipo de dispositivo para acesso; • Tipo de navegador utilizado para acesso; • Tipo de sistema operacional utilizado; • Operadoras utilizadas; • Número de ações do usuário durante o uso; • Tempo médio que os usuários permaneceram acessando o serviço digital; • Quantidade média de ações dos usuários durante o uso; • A sazonalidade diária no uso dos serviços digitais;	
32	O Módulo deverá, para as aplicações do TJPA que requerem autenticação, identificar o usuário4 que o está acessando.	
33	O Módulo, para as aplicações nas tecnologias possíveis, deverá gravar, para até 50% dos usuários, o acesso às aplicações, possibilitando a sua reprodução. Para isso, mantendo as questões de sigilo às informações, deverá permitir que as informações digitadas pelos usuários possam ser mascaradas.	
34	O Módulo deverá classificar automaticamente a qualidade dos acessos dos usuários às aplicações do TJPA. Deverá fazer isso para cada acesso de usuário. A qualidade deverá ser classifica considerando ao menos 03 níveis (Ruim, bom e excelente).	
32	Para cada acesso a uma aplicação, o Módulo deverá realizar uma análise detalhada do mesmo, identificando a região de origem, a qualidade do acesso, o tipo de navegador, a versão do sistema operacional, o IP de origem e o comportamento temporal das ações e funcionalidades acessadas no serviço digital.	
35	O Módulo deverá verificar o comportamento de uso das aplicações, verificando o volume de usuários que utilizam a aplicação, bem como o tempo médio que os usuários permaneceram utilizando a aplicação.	
36	O Módulo deverá possibilitar a coleta e análise de todas as interações (acessos, ações, cliques) do usuário com as aplicações	
37	O Módulo deverá permitir a comparação do desempenho das aplicações pela perspectiva do usuário.	
38	O Módulo deverá detectar de forma automática, transações chaves para o negócio do TJPA que estejam apresentando problemas ou baixo desempenho.	

39	O Módulo deverá apresentar, no mínimo, as seguintes métricas em relação às ações dos usuários: • Quantidade de Bytes baixados; • Tempo médio de interatividade do usuário com o serviço digital; • Tempo no servidor; • Tempo no browser do usuário; • Tempo de tráfego de rede.	
40	O Módulo deve permitir a análise das ações de usuários mais lentas e mais rápidas.	
41	O Módulo deve coletar e analisar o tempo exato de carregamento da página até que a mesma esteja completamente pronta para utilização do usuário, separando essa métrica ainda por: localidade, tipo de dispositivo, localização, sistema operacional ou tipo de navegador;	
42	Buscando identificar o uso que os usuários fazem das aplicações do TJPA, o Módulo deverá prover as seguintes informações a respeito das aplicações, inclusive durante o tempo: • Volume de atividades/ações; • Tempo de atendimento (deverá permitir analisar a média e os 10% mais lento); • Volume de falhas dos serviços (falhas http e JavaScript); • Volume de uso de recursos externos ao serviço digital; • Tempo médio de resposta dos recursos externos ao serviço digital.	
<u>Módulo de monitoramento e análise da segurança das aplicações</u>		
43	O Módulo deverá realizar teste dinâmico de segurança em aplicação web (DAST - *dynamic application security testing*), identificando falhas de segurança e vulnerabilidades contidas dentro do desenvolvimento da aplicação.	
44	O Módulo deve permitir a definição de uma política de segurança da aplicação, permitindo personalizações abaixo: ○ Aderência nos padrões de segurança abaixo: ▪ OWASP; ▪ SANS TOP 25; ▪ PCI; ▪ CERT; ○ Lista de ID do CWE que a aplicação analisada não deve conter; ○ Lista de severidades de falhas que a aplicação analisada não deve conter; ○ Lista de categorias de falhas que a aplicação analisada não deve conter; ○ Pontuação (score) mínima que a aplicação deve ter como resultado da verificação, tendo como base o CVSS (Common Vulnerability Scoring System).	

45	Aplicações devem conter um perfil/cadastro dentro do módulo, permitindo: • Definir um nome de identificação; • Definir descrição da aplicação e seu propósito; • Atrelar uma política de segurança do aplicativo (conforme requisitos definidos neste documento), onde a aplicação é avaliada perante os resultados não aderentes a sua política de segurança. • Definir quais times de desenvolvimento terão visibilidade da aplicação e seus resultados. • Hist análises DAST executadas, contendo seus resultados, bem como análise em execução.	

46	O motor (engine) de análise DAST deve realizar os testes de segurança, visando a identificação de falhas de segurança na aplicação web, atendendo os itens abaixo: ○ Origem das conexões do motor de análise deve utilizar blocos de IP previamente determinados. ○ Deve realizar análise em aplicações web disponíveis através dos protocolos HTTP e HTTPS. ○ A exclusão de determinadas URL (endereço web) deve ser permitida visando em evitar os testes de segurança em certas partes do aplicativo web. ○ A localidade da aplicação deve ser indicada através de sua URL, contendo o protocolo (HTTP ou HTTPS), a porta TCP onde o serviço está disponível e o caminho do recurso, conforme a sintaxe definida pela RFC 1738. ○ O motor da análise deve ser capaz de navegar pela aplicação web de forma automatizada, enumerando os links, páginas, cookies, parâmetros HTTP e demais componentes da aplicação web. O resultado deste procedimento deve ser alvo do teste de segurança realizado pelo motor da análise. ○ Com base na URL fornecida, o motor de análise deve ser orientado a quanto aos limites da aplicação web, evitando que o teste seja executado em outras aplicações. Deve conter ao menos os seguintes recursos: ○ Com base na URL informada, indicar se a navegação e testes de segurança podem ser executados: ▪ Apenas no diretório final da URL. ▪ No diretório final da URL e seus subdiretórios. ▪ Remover limitação, permitindo o motor de análise a navegar em qualquer diretório. ○ O motor de análise deverá realizar autenticação na aplicação web que está sendo analisada, suportando as seguintes formas de autenticação: ▪ Não autenticado. ▪ Autenticação básica do HTTP. ▪ Autenticação baseada em certificados de cliente em formato PKCS12. ○ Identificar automaticamente formulários de autenticação e realizar a autenticação com base em usuário e senha previamente definidos. ○ Importação de um roteiro de autenticação com base no Selenium IDE, onde o motor de análise repetirá o procedimento de autenticação, preenchendo formulários de autenticação e alterando opções/elementos da página de autenticação. ○ Importação de roteiros de navegação personalizados devem ser suportados pela solução, onde, a partir da navegação manual pela aplicação web, seja gerado o roteiro de navegação personalizado e este seja usado pelo motor de análise para repetir as ações na aplicação web. ○ Durante as requisições HTTP/HTTPS, o motor da análise deve indicar o campo "User-Agent" do protocolo HTTP	

	(como descrito na RFC 2616). Este campo deve conter dados de navegadores comuns (Firefox, Chrome, Safari e Microsoft Edge), bem como suportar que seja informado um valor personalizado. ○ Não deve existir um número máximo de links a serem testados e analisados pelo motor DAST, no entanto isto deve ser configurável, permitindo definir uma determinada quantidade de links máximos ou manter ilimitado. ○ Durante a execução da análise, o motor DAST deve utilizar-se da tecnologia de multithreading, onde o teste é executado por mais que uma instância de processamento de forma simultânea e paralela. ○ Visando em evitar testes desnecessários, deve ser possível informar tecnologias utilizadas pela aplicação web (como banco de dados e sistema operacional), removendo assim testes para tecnologias não utilizadas, as seguintes tecnologias devem ser suportadas Oracle, SQL Server, PgSQL MySQL, Linux e Windows. ○ Antes de realizar a execução da análise DAST, o motor deve realizar uma verificação prévia, visando em garantir os seguintes aspectos: ▪ Servidor está acessível pelo motor da análise através da URL informada. ▪ Dados de autenticação na aplicação web estão funcionando. ▪ Motor de análise pode navegar pela aplicação. ○ Tarefa de análise DAST deve poder ser executada de imediato, bem como deve ser possível agendar um determinado dia e horário para iniciar.	

47	Relatório das falhas de segurança identificadas pela análise DAST deve conter: ○ Listagem das URL contempladas pela análise. ○ Sumário executivo listando as falhas de segurança identificadas, informando o número de identificações realizadas e agrupadas por suas severidades, seguindo o padrão CVSS (Common Vulnerability Scoring System). ○ Exportação do relatório em formato PDF. ○ Exportação do relatório em formato PDF seguindo os padrões do PCI. ○ Exportação dos dados que compõem o relatório em formato XML. ○ Relatório de aderência perante a política de segurança atrelada ao perfil da aplicação. ○ Estimativa de tempo de desenvolvimento para correção da falha de segurança. ○ Estimativa de linhas de código que necessitam ser alteradas para correção da falha de segurança. ○ Descritivo das falhas de segurança contendo a contextualização da mesma. ○ Recomendações para realização a correção das falhas de segurança identificadas.	
48	Metodologia de classificação e pontuação dos aplicativos e falhas deve estar aderente aos padrões abaixo: • NIST FIPS Pub. 199 • Common Weakness Enumeration (CWE) • Common Vulnerability Scoring System (CVSS)	
49	Falhas de segurança identificadas devem conter uma categorização atrelada a sua severidade e baseado com o CVSS (Common Vulnerability Scoring System), incluindo no mínimo as categorizações abaixo: • Muito alto; • Alto; • Médio; • Baixo; • Muito baixo; • Informativo.	
50	A solução deve conter as falhas definidas pelo CWE (Common Weakness Enumeration), tendo as atualizações em pelo menos 90 dias.	
51	Identificação de falhas de segurança tendo cobertura das categorias abaixo: • Problemas de autenticação; • Problemas de autorização; • Injeção de código; • Injeção de comandos ou parâmetros; • Gerenciamento de credenciais; • Injeção de CRLF (Carriage Return e Line Feed); • Cross-Site Scripting (XSS);	

	• Problemas criptográficos; • Configuração de implantação; • Directory traversal; • Vazamento de informações; • Falta de validação da entrada de dados; • Injeção de comandos no sistema operacional; • Configurações do servidor; • Fixação de sessões; • Injeção de SQL;	

52	Identificação de falhas de segurança tendo cobertura dos itens abaixo conforme o Common Weakness Enumeration (CWE): • CWE 287 - Improper Authentication • CWE 352 - Cross-Site Request Forgery (CSRF) • CWE 693 - Clickjacking/Content Security Policy insecure unsafe-inline directive used/Content Security Policy insecure unsafe-eval directive used • CWE 285 - Improper Authorization • CWE 98 - Improper Control of Filename for Include/Require Statement in PHP Program (PHP File Inclusion) • CWE 830 - Inclusion of Web Functionality from an Untrusted Source • CWE 78 - Improper Neutralization of Special Elements used in an OS Command (OS Command Injection) • CWE 259 - Use of Hard-coded Password • CWE 522 - Insufficiently Protected Credentials • CWE 113 - Improper Neutralization of CRLF Sequences in HTTP Headers (HTTP Response Splitting) • CWE 79 - Improper Neutralization of Input During Web Page Generation (Cross-site Scripting) • CWE 80 - Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) • CWE 83 - Improper Neutralization of Script in Attributes in a Web Page • CWE 296 - Improper Following of Chain of Trust for Certificate Validation • CWE 297 - Improper Validation of Host-specific Certificate Data • CWE 298 - Improper Validation of Certificate Expiration • CWE 321 - Use of Hard-coded Cryptographic Key • CWE 326 - Inadequate Encryption Strength • CWE 327 - Use of a Broken or Risky Cryptographic Algorithm • CWE 614 - Sensitive Cookie in HTTPS Session Without Secure Attribute • CWE 402 - Transmission of Private Resources into a New Sphere (Resource Leak) • CWE 668 - Exposure of Resource to Wrong Sphere • CWE 22 - Improper Limitation of a Pathname to a Restricted Directory (Path Traversal) • CWE 200 - Information Exposure • CWE 209 - Information Exposure Through an Error Message • CWE 215 - Information Exposure Through Debug Information • CWE 526 - Information Exposure Through Environmental Variables • CWE 530 - Exposure of Backup File to an Unauthorized Control Sphere • CWE 538 - File and Directory Information Exposure • CWE 548 - Information Exposure Through Directory Listing • CWE 434 - Unrestricted Upload of File with Dangerous Type • CWE 601 - URL Redirection to Untrusted Site (Open Redirect) • CWE 78 - Improper Neutralization of Special Elements used in an OS Command (OS Command Injection) • CWE 16 - Configuration • CWE 642 - External Control of Critical State Data • CWE 757 - Selection of Less-Secure Algorithm During Negotiation (Algorithm Downgrade) • CWE 384 - Session Fixation	

	• CWE89 - Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)	

53	Caso a solução necessite de um servidor local para processamento e execução das tarefas de verificação DAST: • Deve ser fornecido junto com o as licenças, incluindo o hardware (servidor com fonte redundante, 2 interfaces de rede gigabit, para rack de 19", ocupando no máximo 1U), sistema operacional e demais custos envolvidos para permitir que o servidor local esteja em operação. • Deve ser capaz de executar tarefas de análise DAST em todas as aplicações simultaneamente.	
54	Caso a solução utilize serviço em nuvem, a mesma deve conter: • Comunicação segura através de TLS 1.2 ou mais recente, validando a procedência do certificado e recusando comunicação não confiável. • Possuir seguir e ser aprovada em auditoria quanto a SOC 2, SOC 3 e SSAE 16 tipo II SOC 1. • Governança da Segurança da Informação. • Avaliação e Tratamento de Riscos. • Política de segurança. • Organização da Segurança da Informação. • Gestão de ativos. • Segurança de Recursos Humanos. • Segurança Física e Ambiental. • Gestão de Comunicações e Operações. • Controle de acesso.	
55	Deve permitir integração em esteiras de desenvolvimento, permitindo a automatização do processo de iniciar análise DAST, possuindo integração com Jenkins, bem como ferramenta de linha de comando.	
56	Deve possuir integração com plataformas de controle de defeitos (bug tracking), suportando: • Jira; • Jira Cloud; • Visual Studio Team Services; • Team Foundation Server (TFS); • BugZilla.	
57	Visando em personalizações e integrações, a solução deve possuir API para execução de operações automatizadas na solução/plataforma, permitindo: • Criar, editar e deletar aplicações; • Criação e envio de tarefas de verificação DAST; • Criação, edição e deleção de times de desenvolvimento; • Listagem dos resultados das verificações DAST;	
58	Desenvolvedores devem ter acesso as falhas de segurança identificadas, contendo a contextualização da falha, local onde a falha foi identificada (URL, parâmetros e resposta do servidor), bem como as recomendações de correção.	