TERMO DE REFERÊNCIA

Aquisição de licenciamento adicional para Solução para Análise de Vulnerabilidades, com garantia, suporte e atualização.

PROCESSO ADMINISTRATIVO PA-PRO-2023/00933

1. DO OBJETO

Aquisição de licenciamento adicional para solução de análise de vulnerabilidades com implantação, garantia e suporte pelo período de 60 meses.

2. DA FUNDAMENTAÇÃO

2.1.Da motivação

Temos acompanhado nos últimos anos um aumento exponencial no que diz respeito aos incidentes de ataques cibernéticos e, consequentemente, tornando os principais sistemas de entidades governamentais indisponíveis. Os crimes cibernéticos tornaram-se um dos maiores riscos para a credibilidade das corporações, seja de domínio público ou domínio privado, causando prejuízos econômicos devastadores.

Todo o cenário supracitado nos mostra que, diante do aumento dos ataques cibernéticos e de suas particularidades sob o prisma da complexidade para o restabelecimento dos serviços afetados, as organizações devem possuir controles, políticas, procedimentos, ferramentas e, principalmente, soluções que possam mitigar e responder efetivamente aos incidentes e ataques diversos, que visam o roubo de dados ou tão somente tornar o acesso às informações de determinada instituição inacessíveis.

Ter o conhecimento e estrutura de como agir antes, durante e após determinado incidente, torna-se cada vez mais crucial para o negócio, visto que a capacidade de uma organização em responder de forma célere e precisa é fundamental para limitar os impactos do ataque, recuperar suas informações e reestabelecer a infraestrutura no menor tempo possível.

Em 2021 e 2022, o Tribunal de Justiça do Estado do Pará realizou aporte financeiro expressivo, objetivando adquirir soluções de segurança da informação que pudessem construir um ecossistema de camadas de proteção. Assim, tomando como base os incidentes identificados em outras entidades governamentais, contratou-se plataformas de proteção de servidores, *endpoints*, soluções de proteção de acesso privilegiado, *firewall* de aplicação web, dentre outros.

Com vistas a ampliar as camadas de segurança deste Egrégio Tribunal, é imperativo a aquisição de solução para análise de vulnerabilidades, que visam identificar, por meio de ensaios estatísticos ou dinâmicos, a identificação de vulnerabilidades de falhas conhecidas nos sistemas desenvolvidos por esta Corte ou que sejam contratados para atividade específica, que podem ser originados por erro de configuração, falha humana ou programação com falhas.

Através do contrato 082/2022, gerado através do PA-PRO-2022/01776, foi adquirido uma solução de gerenciamento de vulnerabilidades que contempla licenciamento para analisar 1500 *endpoints*, 300 containers e 225 aplicações web, além de 60 meses de suporte técnico e 5 vagas para treinamento da solução. A expansão do licenciamento da referida solução visa garantir um maior campo de proteção, tanto para a infraestrutura, quanto para o ambiente de aplicações, mantendo o sigilo, disponibilidade e integridade das informações.

A aquisição adicional das licenças para a solução de gerenciamento de vulnerabilidades contratada através do contrato 082/2022, gerado através do PA-PRO-2022/01776, atende aos seguintes resultados direcionadores, cumprindo os seguintes objetivos:

- Identificação de falhas complexas, permitindo que as equipes multidisciplinares mantenham os níveis de segurança da infraestrutura tecnológica;
- Melhoria na confiabilidade e na integridade das informações, evitando vazamento de informações que possam abalar a credibilidade da instituição;
- Otimização no controle de segurança, proporcionando um excelente recurso durante a análise de vulnerabilidades do ambiente;
- Prover indicadores para mitigação de riscos;
- Efetividade na identificação de vulnerabilidades de segurança;
- Potencializar a otimização e performance das aplicações e sistemas, evitando ataques de negação de serviço;
- Reduzir significativamente a incidência de problemas com *ransomwares*, sistemas desatualizados e senhas fracas;
- Proteger os diversos elementos corporativos de ataques cibernéticos, frustrando prejuízos financeiros e da imagem da instituição;
- Ampliar a conformidade com a LGPD, asseverando as boas práticas na gestão de vulnerabilidades.

2.2. Dos objetivos a serem alcançados por meio da contratação

2.2.1. Dotar o Poder Judiciário do Pará de infraestrutura tecnológica capaz de fornecer segurança e proteção lógica aos equipamentos de processamento e armazenamento de dados situados no Data Center e nas demais estações e ativos de trabalho que compõem a rede de computadores do Tribunal.

2.2.2. Permitir o funcionamento contínuo dos serviços de tecnologia da informação, imprescindíveis ao cumprimento da função institucional, evitando indisponibilidade, reduções no desempenho, paradas não programadas ou perdas de informações.

2.2.3. Promover o aumento da credibilidade dos colaboradores e jurisdicionados do quanto à utilização dos recursos de tecnologia da informação e comunicação, qualificados como solução estável e confiável.

2.2.4. Permitir a gravação, registro, monitoramento, análise comportamental, controle e auditoria das ações realizadas pelos

usuários, administradores, servidores e ativos de tecnologia com acessos privilegiados, a fim de promover e melhorar a produtividade, governança, segurança, auditoria e conformidade das mudanças realizadas no ambiente tecnológico do TJPA

2.2.5. Proteção de sessões estabelecidas na administração de ativos que utilizam credenciais privilegiadas.

2.2.6. Monitoramento de comportamentos suspeitos na utilização de credenciais privilegiadas e não-privilegiadas.

2.2.7. Qualificação e valorização dos servidores que realizarem o treinamento.

2.3. Dos benefícios diretos e indiretos resultantes da contratação

2.3.1. Maior proteção dos diversos componentes do ambiente computacional do TJPA.

2.3.2. Monitoramento proativo e contínuo das vulnerabilidades existentes no parque computacional do Tribunal.

2.3.3. Visão gerencial dos riscos existentes no parque, possibilitando o envolvimento da alta gestão no conhecimento desses riscos.

2.3.4. Medição da maturidade do Tribunal em termos de segurança, possibilitando, inclusive, comparações com outros órgãos e empresas que utilizam a mesma solução.

2.3.5. Tornar a infraestrutura de TI do TJPA mais robusta.

2.3.6. Reduzir o risco de vazamento de informações do TJPA, abrangendo magistrados, servidores, terceirizados e usuários dos serviços do Tribunal.

2.3.7. Garantir a continuidade dos serviços oferecidos a sociedade pelo TJPA.

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

A contratação está alinhada ao **Plano de Gestão 2023-2025 do TJPA**.

- **Macrodesafio 12**: Fortalecimento da Estratégia Nacional de TIC e Proteção de Dados;

Da mesma forma, a contratação está alinhada com o Planejamento Estratégico 2021-2026.

- **Macrodesafio 12**: Fortalecimento da Estratégia Nacional de TIC e Proteção de Dados;

A contratação também foi prevista no **Plano de Contratações 2023** no item SEINF31A23.

Esta aquisição também está alinhada com a **Resolução 370/2021** do Conselho Nacional de Justiça (CNJ), que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (**ENTIC-JUD**) para o sexênio 2021-2026:

- **Seção III**, que trata dos riscos, da segurança da informação e da proteção de dados.
- **Art. 38** - Cada órgão deverá elaborar e aplicar práticas e processos de segurança da informação e proteção de dados a serem adotadas na instituição, conforme disposto na Lei nº 13.709/2018 que dispõe sobre a Proteção de Dados Pessoais.

2.5.Da referência aos Estudos Preliminares

Os estudos preliminares foram protocolados no sistema SigaDoc através do PA-PRO-2023/00993.

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

Esta contratação se destina, fundamentalmente, a ampliar a automatização do processo de gerenciamento de vulnerabilidades existentes em servidores físicos, virtuais e estações de trabalho, possibilitando o aumento da detecção, monitoramento e correção dessas vulnerabilidades em um número maior de ativos do TJPA.

E ainda ampliar a atuação conjunta entre as coordenadorias atuantes na SECINFO, com o objetivo de conscientização sobre o papel de cada coordenadoria no processo de gerenciamento de vulnerabilidades e mitigação dos riscos causados pelas mesmas.

Entende-se que as demandas previstas e projetadas pela Secretaria de Informática do TJPA a serem atendidas pela contratação da solução de gerenciamento de vulnerabilidades *(Vulnerability Management)*, serão cobertas em sua plenitude, durante o período de vigência de 60 meses, através do contrato estabelecido entre o CONTRATANTE e a CONTRATADA. Abaixo estão elas listadas:

Item	Descrição	QTD
1	Solução de Gerenciamento de vulnerabilidades para **Aplicações Web (FQDNs Externos)**, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	723
2	Solução de Gerenciamento de vulnerabilidades para **Aplicações Web (FQDNs Internos)**, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e	991

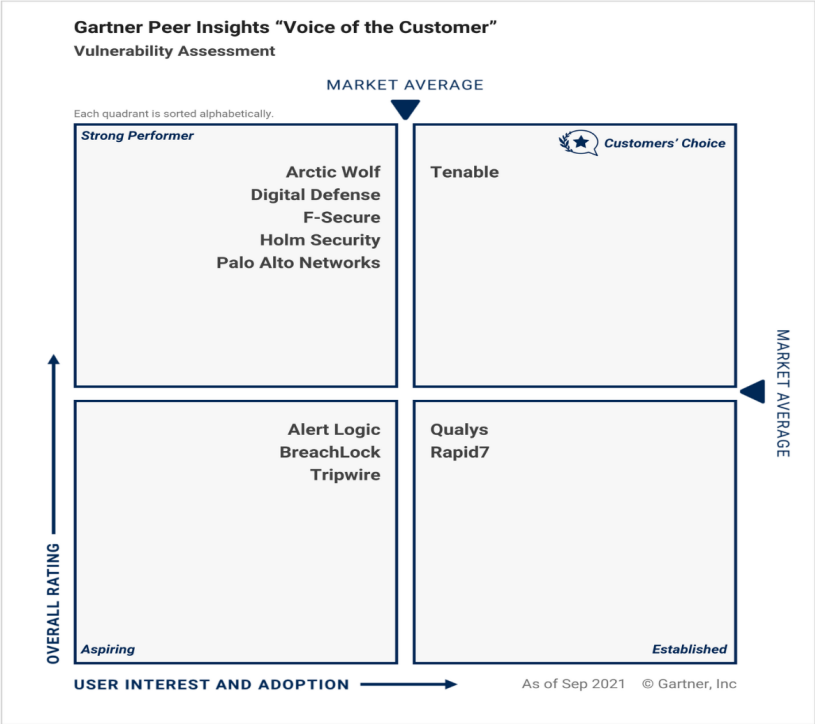
	também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	
3	Solução de Gerenciamento de vulnerabilidades para **Imagens de aplicações em Container**, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	2880
4	Solução de Gerenciamento de vulnerabilidades para **Endpoints**, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	2406

2.7.Da análise de mercado de TIC

Como solução mercadológica que venha a atender as necessidades deste Tribunal não se vislumbra outra que não seja a **Contratação de empresa especializada** no fornecimento de solução de gerenciamento de vulnerabilidades (*Vulnerability Management*), com possibilidade de avaliação de vulnerabilidades não corrigidas em diversas classes de ativos, incluindo aplicações Web, infraestrutura em nuvem e Conteiners, com a finalidade de aumentar o monitoramento proativo de vulnerabilidades decorrentes da falta de atualização da infraestrutura utilizada no âmbito do Tribunal e impedir que essas vulnerabilidades sejam usadas por potenciais atacantes, prevenindo danos decorrentes de ataques cibernéticos que possam ser realizados contra o tribunal. Cumpre destacar que, atualmente, o Poder Judiciário estadual não possui ferramenta específica de proteção supramencionada e, conforme detalhamento do potencial da solução, busca a contratação da plataforma que apresentar melhor custo-benefício, em qualidade e preço a ser pago.

Sendo uma solução comum de mercado, existem diversos fabricantes que podem oferecer soluções de gerenciamento de vulnerabilidades, com diferentes graus de qualidade e diversos preços a serem pagos. Sendo inviável avaliar todas as opções disponíveis, recorreu-se ao Gartner, que é empresa amplamente respeitada e prestigiada no campo da Tecnologia da Informação, servido como referência na área, para delimitar as melhores opções a serem consideradas em processos de aquisição.

Figura 1 - Gartner Peer Insights para soluções de gerenciamento de vulnerabilidades, de setembro de 2021.



O Gartner realiza a mensuração da qualidade e relevância de soluções de TI através de um gráfico que ficou conhecido como "**Quadrante**", o qual reflete os estudos publicados anualmente sobre categorias de produtos e serviços, ou as opiniões emitidas pelos clientes que utilizaram determinada solução. Como o TJPA preza pela qualidade das soluções contratadas para compor sua infraestrutura tecnológica, as soluções consideradas foram as que se estavam mais bem posicionadas no quadrante "***Customer Choice***" (Escolha do Cliente) da avaliação mais recente, publicada em setembro de 2021. Os fabricantes mais bem localizados neste quadrante foram avaliados com as melhores opiniões a respeito da sua solução oferecida.

Ao que podemos verificar no quadrante do Gartner, o fabricante que está melhor posicionado é a **Tenable**, tendo inclusive este Tribunal já escolhido essa solução em uma contratação anterior.

Dado que o objeto da contratação é um elemento essencial para a construção de um ecossistema de segurança da informação no âmbito do TJPA, tendo sido observado a sua contribuição na garantia da segurança da informação no âmbito da administração pública municipal, estadual e federal, com diversos órgãos dos mais variados tamanhos e com a mais diversas funções o possuindo em sua infraestrutura de TI.

As contratações mencionadas abaixo, guardadas as peculiaridades de cada órgão, são similares ao objeto que o TJPA pretende adquirir:

1. Destaca-se a solução contratada pelo **Tribunal Regional do Trabalho da 8ª Região (TRT8)** que, através da **Ata de Registro de Preço (ARP) nº 005/2022** gerada **no Pregão Eletrônico 04/2022**, registrou preços para o objeto:

   "aquisição de solução que auxilie na prevenção e limitação da extensão de ataques cibernéticos, através do gerenciamento de vulnerabilidades, baseada em risco, dos ativos de Tecnologia da Informação, com análise contínua e adaptável, a fim de manter a confidencialidade, a disponibilidade e a integridade das informações".

2. A solução contratada pelo **Ministério Público do Distrito Federal e Territórios (MPDFT)** através da **Ata de Registro de Preço nº 026/2020**, gerada **no Pregão Eletrônico 62/2020**, registrou preços para o objeto:

   "eventual aquisição de Licenças Perpétuas de Solução de Gestão de Vulnerabilidades e serviços associados, conforme especificações constantes do Edital".

3. O **Tribunal Regional Eleitoral da Paraíba (TRE-PB)**, através das **Atas de Registro de Preço nº 100/2020 e 101/2020**, gerada **no Pregão Eletrônico 37/2020**, registrou preços para o objeto:

   "aquisição de solução unificada de gestão de vulnerabilidades em ativos de tecnologia da informação e aplicações web, compreendendo aquisição de serviços de software e suporte técnico".

2.8.Da natureza do objeto

O objeto a ser contratado possui características comuns e usuais encontradas atualmente no mercado de Tecnologia de Informação, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos neste Termo de Referência.

Além disso, trata-se de prestação de serviço continuado, uma vez que sua interrupção pode comprometer a continuidade das atividades do TJPA a partir da implementação, uma vez que a solução implementa segurança através da mediação no uso de credenciais privilegiadas e a interrupção da solução implica em interrupção no acesso aos recursos gerenciados pelas referidas credenciais

2.9.Do parcelamento do objeto

2.9.1. Conforme § 1º, do Art. 23, da Lei Nº 8.666/93, os serviços deverão ser divididos em tantas parcelas quantas se comprovarem técnica e economicamente viáveis, procedendo-se à licitação com vistas ao melhor aproveitamento dos recursos disponíveis no mercado e à ampliação da competitividade sem perda da economia de escala.

2.9.2. O disposto, no entanto, não se aplica na presente demanda, sendo necessário o agrupamento em Lote, tendo em vista a garantia da uniformidade na prestação dos serviços, uma vez que os itens agrupados possuem a mesma natureza e guardam relação entre

si, afastando possíveis prejuízos à competitividade, ao mesmo tempo em que exerce maior atratividade perante os licitantes. Ademais, considerando o número de itens, a organização em lote evita que inúmeros contratos sejam celebrados com diferentes fornecedores, situação que, tecnicamente, afeta diretamente a rotina da Administração, prejudicando a eficiência administrativa, que passa pela otimização do gerenciamento de seus contratos de fornecimento, uma vez que lidar com um único fornecedor diminui o custo administrativo de gerenciamento de todo o processo de contratação.

2.9.3. É importante salientar que o aumento da eficiência administrativa do setor público passa pela otimização do gerenciamento de seus contratos, e essa eficiência administrativa também é de estatura constitucional e deve ser buscada pela administração pública. Busca-se ainda, com o agrupamento, obtenção de preços mais vantajosos à Administração, em razão da economia de escala, eficiência e racionalização de custos.

2.9.4. Dessa forma a presente contratação será realizada por meio de lote único com 05 (cinco) itens.

2.10. Da seleção do fornecedor

Prejudicado. Considerando que foi constatado que a adesão a Ata de Registro de Preços n° 005/2022, do Tribunal Regional do Trabalho – 8ª Região, é mais vantajosa economicamente que licitar, não haverá seleção de fornecedor, sendo a empresa contratada a detentora daquela ARP.

2.10.1. Da forma e do critério de seleção

Prejudicado. Considerando que foi constatado que a adesão a Ata de Registro de Preços n° 005/2022, do Tribunal Regional do Trabalho – 8ª Região, é mais vantajosa economicamente que licitar, não haverá necessidade de fixação de forma e critério de seleção, uma vez que a a empresa contratada será a detentora daquela ARP.

2.10.2. Da modalidade e do tipo de licitação

Prejudicado. Considerando que foi constatado que a adesão a Ata de Registro de Preços n° 005/2022, do Tribunal Regional do Trabalho – 8ª Região, é mais vantajosa economicamente que licitar, não haverá necessidade de fixação de modalidade e tipo de licitação, pois irá ocorrer adesão a ARP.

2.10.3. Dos critérios técnicos de habilitação obrigatórios

Prejudicado. Considerando que foi constatado que a adesão a Ata de Registro de Preços n° 005/2022, do Tribunal Regional do Trabalho – 8ª Região, é mais vantajosa economicamente que licitar, não haverá necessidade de fixação de critérios técnicos de habilitação, uma vez que estes requisitos foram analisados pelo órgão gestor da ARP.

2.11. Do impacto ambiental

Pelo fato da solução a ser adquirida ser totalmente baseada em software, não haverá impactos ambientais relevantes a serem considerados em sua implantação.

2.12. Da conformidade técnica e legal

Serão de propriedade do TJPA todos os produtos gerados pela empresa CONTRATADA relacionados a presente contratação, incluindo estudos, relatórios, especificações, descrições técnicas, protótipos, dados, esquemas, planilhas, plantas, desenhos, diagramas, páginas na Intranet e documentação, em papel ou em qualquer forma ou mídia, em conformidade com o artigo 111 da Lei 8.666/93, com a Lei 9.609/98, que dispõe sobre propriedade intelectual de programa de computador, e com a Lei 9.610/98, que dispõe sobre direito autoral, sendo vedada qualquer comercialização desses por parte da CONTRATADA.

2.13. Das obrigações

2.13.1. Das obrigações do CONTRATANTE

2.13.1.1. Permitir ao pessoal técnico da CONTRATADA, desde que identificado e incluído na relação de técnicos autorizados, o acesso às unidades para a execução das atividades, respeitadas as normas de segurança vigentes nas suas dependências.

2.13.1.2. Notificar a CONTRATADA quanto a defeitos ou irregularidades verificados na execução das atividades objeto deste Termo de referência, bem como quanto a qualquer ocorrência relativa ao comportamento de seus técnicos, quando em atendimento, que venha a ser considerado prejudicial ou inconveniente para o Tribunal.

2.13.1.3. Indicar os locais onde deverão ser instalados os equipamentos, caso necessários, e proporcionar à CONTRATADA as facilidades e instruções necessárias para a realização do serviço de instalação.

2.13.1.4. Verificar a regularidade da situação fiscal e dos recolhimentos sociais trabalhistas da CONTRATADA conforme determina a lei, antes de efetuar o pagamento devido.

2.13.1.5. Promover a fiscalização do contrato, sob os aspectos quantitativo e qualitativo, por intermédio de profissional designado, anotando em registro próprio as falhas detectadas e exigindo as medidas corretivas necessárias, bem como acompanhar o desenvolvimento do contrato, conferir os serviços executados e atestar os documentos fiscais pertinentes, quando comprovada a execução total, fiel e correta dos serviços, podendo ainda sustar, recusar, mandar fazer ou desfazer qualquer procedimento que não esteja de acordo com os termos contratuais.

2.13.1.6. Comunicar tempestivamente à CONTRATADA as possíveis irregularidades detectadas na execução das atividades.

2.13.1.7. Confeccionar Termo de Recebimento Definitivo para os itens do LOTE.

2.13.1.8. Observar para que durante a vigência do contrato sejam cumpridas as obrigações assumidas pela CONTRATADA, bem como sejam mantidas todas as condições de qualificação exigidas no processo de contratação.

2.13.2. Das obrigações da CONTRATADA

2.13.2.1. Compete à CONTRATADA, a execução das atividades na forma estipulada no presente Termo de Referência.

2.13.2.2. É permitida a subcontratação dos serviços constantes nesse processo até o limite de 50% (cinquenta por cento) do valor total.

2.13.2.3. A subcontratação depende de autorização prévia da CONTRATANTE, a quem incumbe avaliar se a subcontratada cumpre os requisitos de qualificação técnica, além da regularidade fiscal e trabalhista, necessários à execução do objeto.

2.13.2.4. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral da CONTRATADA pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades da subcontratada, bem como responder perante a CONTRATANTE pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

2.13.2.5. O Tribunal homologará as atividades correspondentes a cada solicitação a partir da sua entrega pela CONTRATADA.

2.13.2.6. A CONTRATADA deverá indenizar o Tribunal nos casos de danos, prejuízos, avarias ou subtração de seus bens ou valores, bem como por acesso e uso indevido de informações sigilosas ou de uso restrito, quando tais atos forem praticados por quem tenha sido alocado à execução do objeto do contrato, desde que devidamente identificado.

2.13.2.7. A CONTRATADA será a única e exclusiva responsável pela execução das atividades, reservando-se ao Tribunal o direito de exercer a mais ampla e completa fiscalização dessas atividades.

2.13.2.8. A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, do Tribunal, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.

2.13.2.9. A CONTRATADA deverá responsabilizar-se integralmente pela execução das atividades contratadas, nos termos da legislação vigente, de modo que os mesmos sejam realizados com esmero, sob sua inteira e exclusiva responsabilidade, obedecendo às normas e rotinas do Tribunal, em especial as que digam respeito à segurança, à confiabilidade e à integridade.

2.13.2.10. A CONTRATADA deverá assinar termo de responsabilidade e sigilo, comprometendo-se a não comentar nenhum assunto tratado nas dependências do Tribunal ou a serviço deste, salvo se expressamente autorizado por representante legal do Tribunal.

2.13.2.11. No termo de responsabilidade e sigilo assinado, a CONTRATADA declara estar ciente de que a estrutura computacional disponibilizada pelo Tribunal não poderá ser utilizada para fins particulares, e que a navegação em sítios da Internet e as correspondências em meio eletrônico utilizando o endereço do Tribunal ou acessado a partir dos seus equipamentos poderão ser auditadas.

2.13.2.12. A CONTRATADA responsabilizar-se-á pelo comportamento dos seus empregados e por quaisquer danos que estes ou seus prepostos venham porventura ocasionar ao Tribunal, ou a terceiros, durante a execução dos serviços, podendo o órgão descontar o valor correspondente ao dano dos pagamentos devidos.

2.13.2.13. A CONTRATADA deverá manter durante a vigência contratual, todas as condições que ensejarem a sua contratação.

2.13.2.14. A CONTRATADA deverá manter seus empregados, durante o horário de prestação do serviço, quando nas dependências do Tribunal, devidamente identificados mediante uso permanente de crachá.

2.13.2.15. A CONTRATADA deverá cumprir e fazer cumprir por seus empregados as normas e regulamentos disciplinares do Tribunal, bem como quaisquer determinações emanadas das autoridades competentes.

2.13.2.16. A CONTRATADA deverá providenciar a imediata correção das deficiências apontadas pelo Tribunal quanto à execução das atividades previstas.

2.13.2.17. A CONTRATADA não deverá se valer do contrato a ser celebrado para assumir obrigações perante terceiros, dando-o como garantia, nem utilizar os direitos de crédito, a serem auferidos em função das atividades prestadas, em quaisquer operações de desconto bancário, sem prévia autorização do Tribunal.

2.13.2.18. A CONTRATADA deverá comunicar, de forma detalhada, toda e qualquer ocorrência de acidentes verificada no curso da execução contratual.

2.13.2.19. A CONTRATADA deverá ter monitoração da qualidade das atividades executadas. Os registros gerados, depois de atendidos e dados por concluídos, sofrerão avaliação do próprio usuário quanto à conclusão do atendimento e sua satisfação.

2.13.2.20. Caso os usuários não se sintam satisfeitos com a execução do suporte, os registros originais serão imediatamente reabertos.

2.13.2.21. Os registros deverão conter todas as informações necessárias para a consecução do atendimento pela CONTRATADA, bem como suficientes para atender as necessidades do cliente.

A CONTRATADA deverá diligenciar no sentido de que os seus técnicos, ou prepostos, portem, obrigatoriamente, a respectiva identidade funcional, quando do atendimento ao Tribunal.

A CONTRATADA deverá encaminhar expediente ao Tribunal, informando os nomes dos técnicos que estão autorizados a executar as atividades contratadas.
A CONTRATADA deverá apresentar atestado(s) de capacidade técnica expedido por pessoa jurídica de direito público ou privado, onde comprove ter desenvolvido atividades pertinentes e compatíveis aos constantes com o objeto deste edital.
A CONTRATADA deverá apresentar documentação técnica dos serviços executados, nas datas aprazadas, visando homologação da mesma pela CONTRATANTE.
A CONTRATADA deverá pagar todos os impostos e taxas devidas sobre as atividades prestadas ao Tribunal, bem como as contribuições à previdência social, encargos trabalhistas, prêmios de seguro e acidentes de trabalho, emolumentos, quaisquer insumos e outras despesas diretas e indiretas que se façam necessárias à execução dos serviços contratados. A não comprovação do pagamento desobriga o CONTRATANTE do pagamento da fatura até a regularização.

3. ESPECIFICAÇÃO TÉCNICA DETALHADA

3.1.Dos papeis a serem desempenhados

Em atenção à legislação vigente, especialmente no que diz respeito a Resolução nº 182/2013 do CNJ e as Portarias nº 684/2020 e 685/2020, resume-se papeis e responsabilidades relacionados à contratação e fiscalização:

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	Funcionário 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.

Equipe de apoio da contratação (quando se tratar de licitação)		
INTEGRANTE DEMANDANTE Nome: **Erick Johny Maciel Bol** Matrícula: 105937 Telefone: 3289-7181 E-mail: erick.bol@tjpa.jus.br	**INTEGRANTE TÉCNICO** Nome**: Thiago do Rosário de Castro** Matrícula: 174394 Telefone: 3289-7189 E-mail: thiago.rosario@tjpa.jus.br	**INTEGRANTE ADMINISTRATIVO** Nome: **Luciano Santa Brigida das Neves** Matrícula: 147460 Telefone: 3205-3571 E-mail: luciano.neves@tjpa.jus.br

Equipe de gestão e fiscalização da contratação

Gestor do Contrato	Fiscal Demandante	FISCAL TÉCNICO	FISCAL ADMINISTRATIVO
Nome: **MARCUS VINICIUS BARBOSA E SILVA** Matrícula: 116971 Telefone: E-mail: erick.bol@tjpa.jus.br	Nome: **ERICK JOHNY MACIEL BOL** Matrícula: 105937 Telefone: E-mail: erick.bol@tjpa.jus.br	Nome**: Thiago do Rosário de Castro** Matrícula: 174394 Telefone: 3289-7189 E-mail: thiago.rosario@tjpa.jus.br	Nome: Matrícula: Telefone: E-mail:

A CONTRATANTE, deverá indicar um servidor da Coordenadoria de Suporte Técnico (CST) para acompanhar a implantação, onde também, eventualmente e formalmente, delegará competências conforme as necessidades do projeto.

A CONTRATADA, deverá indicar um responsável técnico encarregado de dar suporte ao esclarecimento das exigências técnicas contratuais.

Para fins de contrato, a empresa contratada deverá designar seu "PREPOSTO", ao qual serão transmitidas as instruções, orientações e normas para execução das obrigações contratuais.

Cabe ao PREPOSTO e ao RESPONSÁVEL TÉCNICO:

a) Coordenar, orientar e supervisionar toda a equipe técnica da CONTRATADA alocada para o cumprimento das obrigações contratuais, cabendo-lhe ainda, a delegação e distribuição das tarefas entre as equipes, garantindo o cumprimento dos níveis de serviço estabelecidos.

b) Responder prontamente a todos os questionamentos e solicitações do TJPA, informando-os das necessidades de intervenção, inclusive, se necessário, aquelas que sejam efetuadas através de terceiros.

c) Propor ao TJPA mudanças nas rotinas e procedimentos técnicos, quando julgar pertinente, visando a otimização de custos, a racionalização e melhoria de processos.

d) Participar, quando solicitado pelo Tribunal, de reuniões relativas às atividades sob sua gestão, fornecendo informações e relatórios, apresentando sugestões, e propondo soluções que julgue pertinentes e necessárias.

e) Acompanhar os resultados globais das atividades sob sua gestão, fornecendo subsídios e informações à Secretaria de Informática do TJPA, visando o tratamento das prioridades e do planejamento global.

f) Ser o ponto de contato entre o TJPA e a CONTRATADA, no que se refere as atividades executadas, posicionando os servidores da Secretaria de Informática quanto ao cumprimento das metas estabelecidas.

3.2.Da dinâmica de execução do contrato

3.3.Etapas

3.4.Dos prazos

3.4.1. Prazos de entrega dos bens/execução dos serviços

O prazo de entrega dos bens adquiridos e de serviços prestados deverá ser executado de acordo com os prazos máximos definidos no cronograma abaixo:

#	EVENTO	RESPONSÁVEL	PRAZO
1	Assinatura do Contrato.	CONTRATANTE e CONTRATADA	Até 5 (cinco) dias após a convocação pelo CONTRATANTE.
2	Entrega de todos os componentes da Solução.	CONTRATADA	Até 30 (trinta) dias após o evento 1.
3	Conferência dos componentes da solução.	CONTRATANTE	Até 05 (cinco) dias após o evento 2.
4	Entrega da versão inicial do Plano de Implantação.	CONTRATADA	Até 10 (dez) dias após o evento 1.
5	Aceite do Plano de Implantação.	CONTRATANTE	Até 05 (cinco) dias após o evento 4.
6	Entrega da versão final do Plano de Implantação.	CONTRATADA	Até 2 (dois) dias úteis após o evento 5.
7	Implantação da Solução – Primeira Etapa*.	CONTRATADA	Até 10 (dez) dias úteis após o evento 6.
8	Emissão do Termo de Aceitação Provisória 1 (TAP1).	CONTRATADA	Até 5 (cinco) dias após o evento 7.
9	Implantação da Solução – Segunda Etapa*.	CONTRATADA	Até 10 (dez) dias úteis após o evento 7.
10	Emissão do Termo de Aceitação Provisória 2 (TAP2).	CONTRATADA	Até 5 (cinco) dias após os eventos 9.
11	Implantação da Solução – Terceira Etapa*.	CONTRATADA	Até 10 (dez) dias úteis após o evento 9.
12	Emissão do Termo de Aceitação Definitiva (TAD) da Implantação.	CONTRATADA	Até 5 (cinco) dias úteis após o evento 11.
13	Operação Assistida.	CONTRATADA	Até 30 (trinta) dias úteis de operação assistida após emissão do Termo de Aceitação Definitiva (TAD).

3.4.2. Prazo de vigência do contrato

O prazo de vigência do contrato assinado será de 60 (sessenta) meses, a partir da data da assinatura.

3.4.3. Logística de implantação

Por tratar-se de software, não haverá necessidade de entrega de equipamentos, cabendo apenas o processo de implantação, configuração e

sintonia da solução contratada a qual será realizada segundo agendamento prévio com o fiscal técnico do contrato.

3.4.4. Cronograma

Não haverá nenhum cronograma específico a ser cumprido pela CONTRATADA, mas somente a exigência de cumprimento dos prazos citados no item 3.4.1.

3.5.Dos instrumentos formais de solicitação

As comunicações formais ocorrerão, preferencialmente, por e-mail, especialmente no que tange à formalização de pedidos, prazos e intercâmbio de documentação, sem prejuízo da utilização de recursos telefônicos quando da prestação da garantia e dos seus serviços atrelados de suporte técnico ou quando couber a agilização do contato para a consecução de atividade específica, ficando estas discricionariamente a cargo da CONTRATANTE.

3.6.Garantia e Nível de Serviço

3.6.1. Garantia do produto/serviço

De acordo com o item 3.6.3 dos estudos preliminares, o prazo de garantia do software, suporte e licenciamento que serão adquiridos deverá ser de 60 (sessenta) meses.

3.6.2. Garantia contratual

A garantia contratual é dispensável, tendo em vista que a garantia técnica do fabricante é de 60 meses.

3.6.3. Nível de Serviço

A tabela abaixo descreve os prazos de atendimento que deverão ser cumpridos pela CONTRATADA, de acordo com a severidade de cada chamado aberto:

Tabela de Solução dos chamados			
Severidade	**Descrição**	**Tempo para primeiro contato após abertura do chamado**	**Tempo de resolução do chamado**
Urgente	Serviço crítico parado em produção.	30 minutos	Até 01 (uma) hora
Alta	Erros e problemas que estão impactando no ambiente de produção.	60 minutos	Até 04 (quatro) hora
Média	Problemas ou erros contornáveis que afetam o ambiente em produção, mas não possuem alto impacto.	90 minutos	Até 06 (seis) horas
Baixa	Problemas ou erros contornáveis que não impactam	120 minutos	Até 08 (oito) horas

	significativamente no ambiente em produção.		
Informações	Consulta Técnica, dúvidas em geral, monitoramento.	150 minutos	Até 24 (vinte e quatro) horas

O prazo de atendimento deve começar a ser contabilizado a partir do momento de efetivação da abertura do suporte, através de telefone ou e-mail;

A CONTRATADA deve apresentar relatório de visita para cada solicitação de suporte on-site, contendo a data e hora da solicitação de suporte técnico, o início e o término do atendimento, identificação do problema, providências adotadas e demais informações pertinentes;

O relatório de visita deverá ser assinado pelo técnico responsável pela abertura do chamado e o fiscal do CONTRATANTE responsável pelo contrato;

O nível de severidade será informado no momento da abertura de cada chamado pelo técnico responsável do CONTRATANTE;

Todas as solicitações de suporte técnico devem ser registradas pela CONTRATADA para acompanhar e controlar a execução dos chamados;

O descumprimento dos prazos de atendimento implicará na aplicação de glosas conforme tabela abaixo:

Tabela de aplicação de Glosas		
Severidade	**Fórmula de cálculo da glosa**	**Limite da glosa**
Urgente	HS x 0,5% * VFM	20% da VFM
Alta	HS x 0,4% * VFM	15% da VFM
Média	HS x 0,3% * VFM	10% da VFM
Baixa	HS x 0,2% * VFM	10% da VFM
Informações	HS x 0,1% * VFM	10% da VFM
HS = Horas totais que extrapolaram o limite de resolução dos chamados, no caso de hora quebrada, será apurado o percentual da hora descumprida.		
VFM = Valor da Fatura Mensal para pagamento do serviço de suporte.		
Em caso de descumprimento contumaz pela CONTRATADA nos prazos para atendimento do suporte técnico a fiscalização poderá adotar a aplicação de sanções: advertências, multas, suspensão temporária de participação em licitação e impedimento de contratar com a Administração e declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, na forma da lei 8.666, de 1993.		

3.7.Da forma de comunicação e acompanhamento da execução do contrato

A CONTRATADA deverá fornecer previamente os contatos de e-mail e telefone dos envolvidos na execução do objeto da contratação. Estes serão os principais canais de comunicação a serem utilizados durante a execução do contrato, devendo a comunicação ser realizada preferencialmente por e-mails, para geração de registros documentais. Pela CONTRATANTE, os

componentes da Equipe de Gestão e Fiscalização da Contratação se encarregarão da comunicação com a CONTRATADA no tocante à execução do contrato.

3.8.Do recebimento

3.8.1. Do recebimento provisório e definitivo

3.8.1.1. **Para os equipamentos**, caso a solução tenha necessidade de appliances:

3.8.1.1.1. **Recebimento Provisório** do objeto será dado pelo Fiscal do Contrato, em até 10 (dez) dias após a entrega dos equipamentos, compreendendo dentre outras, as seguintes verificações:

- Os materiais deverão estar em suas respectivas embalagens originais, se cabível, com a indicação da marca/modelo na embalagem e/ou no próprio material, bem como das demais características que possibilitem a correta identificação do material;
- Condições da embalagem e/ou do material;
- Quantidade entregue;
- Apresentação do documento fiscal, com identificação do fornecedor e do comprador (Tribunal), descrição do material entregue, quantidade, preços unitário e total.

3.8.1.1.2. O **Recebimento Definitivo** do objeto será dado pelo Fiscal de Contrato, após a emissão da Nota Fiscal, em até 30 (trinta) dias após a entrega dos equipamentos, satisfeitas as condições abaixo:

- Correspondência de marca/modelo do material com os indicados na nota de empenho ou proposta da fornecedora;
- Compatibilidade do material entregue com as especificações exigidas neste Termo de Referência e constantes da proposta da empresa fornecedora;
- Realização de testes, quando previstos no Termo de Referência ou caso a unidade recebedora entenda necessário;
- Conformidade do documento fiscal quanto à identificação do comprador (Tribunal), descrição do material entregue, quantidade, preços unitário e total.
- Para o aceite, os equipamentos e seus componentes serão submetidos, a critério da CONTRATANTE, a testes de

desempenho e/ou demonstrações de funcionamento, que verificarão funções e parâmetros especificados neste Termo de Referência.

3.8.1.2. Para os serviços de instalação de software, configuração e transferência de conhecimento:

3.8.1.2.1. O **Recebimento Provisório** do objeto será dado pelo Fiscal do Contrato, em até 10 (dez) dias após a execução dos serviços, compreendendo dentre outras, a apresentação do relatório técnico com a descrição dos serviços executados;

3.8.1.2.2. O **Recebimento Definitivo** do objeto será dado pelo Fiscal de Contrato, após a emissão da Nota Fiscal, em até 30 (trinta) dias após a execução dos serviços, satisfeitas as condições abaixo:

- Compatibilidade dos serviços executados com as especificações exigidas neste Termo de Referência e constantes da proposta da empresa fornecedora;
- Em caso de serviços de instalação e configuração, a entrega da solução em pleno funcionamento, conforme avaliado pela equipe técnica do Tribunal;
- Em caso de treinamento, apresentar os certificados de conclusão do curso emitidos para os participantes;
- Conformidade do documento fiscal quanto à identificação do comprador (Tribunal), descrição do serviço entregue, quantidade, preços unitário e total.

3.9.Da forma de pagamento

A CONTRATADA deverá apresentar a Nota Fiscal/Fatura contendo nº da Nota de Empenho, em 02 (duas) vias, emitidas e entregues ao setor responsável pela fiscalização, para fins de ateste, liquidação e pagamento.

O pagamento dos equipamentos, caso a solução tenha necessidade de *appliances*, será realizado em parcela única, após o recebimento pelo Fiscal do Contrato.

O pagamento dos softwares que compõem a solução será feito após a entrega das licenças ao órgão licitante e o recebimento pelo Fiscal do Contrato.

O pagamento dos serviços de instalação e configuração, assim como dos serviços especializados em segurança da informação será realizado em parcela única, após o recebimento definitivo do objeto pelo Fiscal do Contrato, satisfeitas as condições do item "DA FORMA DE RECEBIMENTO".

Os valores para essa contratação foram relacionados no Plano de Orçamentário do Tribunal de Justiça do Estado do Pará, referente à Secretaria de Informática, vigente para o exercício de 2023, e no Plano de Contratações de Soluções de TIC para o referido exercício.

3.10. Da transferência de conhecimento

3.10.1. A CONTRATADA deverá entregar ao Tribunal toda e qualquer documentação gerada em meio magnético e/ou físico em função da prestação de serviços.

3.10.2. As informações geradas pela CONTRATADA estarão disponíveis em ferramentas e em documentos conforme a definições e padrões utilizados pelo Tribunal.

3.10.3. Deverá haver transferência de conhecimento da CONTRATADA para o Tribunal em relação às tecnologias utilizadas na prestação de serviços para melhor eficiência, eficácia, efetividade e economicidade com sua adoção.

3.10.4. Será de inteira responsabilidade da CONTRATADA, sem ônus adicional para o Tribunal, garantir o repasse bem-sucedido de todas as informações necessárias para a continuidade dos serviços pelo órgão ou empresa por este designada.

3.10.5. O apoio na fase de implantação, pela transferência técnica, no uso das soluções implantadas pela CONTRATADA, deverá ser viabilizada, sem ônus adicionais para o Tribunal, e baseado em documentos funcionais, técnicos e/ou manuais específicos da solução desenvolvida. O cronograma e horários dos eventos deverão ser previamente aprovados pelo órgão.

3.11. Dos direitos de propriedade intelectual e autoral

Após a completa implantação da solução adquirida e atestado que a solução está em conformidade com todos os itens do contrato firmado, tanto em termo de qualidade, quando em quantidade, será emitido um TRD (Termo de Recebimento Definitivo) da solução, caracterizando a transferência definitiva da solução e de todos os componentes necessários para o seu total funcionamento, para o Tribunal.

Eventuais softwares que são necessários ao funcionamento da solução são de propriedade do fabricante e deverão ser fornecidos em conjunto com o respectivo *hardware*, sendo que os direitos de propriedade intelectual pertencem ao fabricante da solução, de acordo com a Lei 9609/98, que dispõe sobre a proteção da propriedade intelectual de programa de computador.

3.12. Da qualificação técnica dos profissionais

A Contratada deverá possuir, após a assinatura do contrato, pelo menos 1 (um) profissional com certificação técnica oficial do fabricante, compatível com o objeto deste processo, capaz de prestar o suporte técnico aos produtos em garantia e escalar o chamado ao fabricante, conforme a necessidade.

3.13. Das sanções

Com fundamento no artigo 7º da Lei nº 10.520/2002 e, subsidiariamente, nos artigos 86 e 87 da Lei 8.666/1993, a Contratada ficará sujeita, assegurada prévia e ampla defesa, às seguintes penalidades:

3.13.1 Advertência

- A Contratada será notificada formalmente pelo CONTRATANTE em caso de descumprimento de obrigação contratual e terá que apresentar as devidas justificativas em um prazo de até 5 (cinco) dias úteis após o recebimento da notificação; e
- Caso não haja manifestação dentro desse prazo ou o TJPA entenda serem improcedentes as justificativas apresentadas, a Contratada será advertida.

3.13.2 Multa

- 0,5% por dia, sobre o valor constante no CONTRATO no caso de atraso injustificado na entrega dos serviços, limitada a incidência a 20 (vinte) dias corridos;
- No caso de atraso injustificado na entrega dos serviços por prazo superior a 20 (vinte) dias corridos, com a aceitação pela Administração, será aplicada a multa de 10% sobre o valor da Ordem de Fornecimento.
- Em caso de atraso injustificado na entrega dos equipamentos, será cobrada multa no valor de 1% do valor total do contrato, por dia de atraso, até o limite de 30 (trinta) dias de atraso.
- Decorrido o prazo de 30 (trinta) dias de atraso injustificado na entrega e/ou na solução de chamado de atendimento, será caracterizada a inexecução parcial do contrato. Com a aceitação pela Administração, será aplicada a multa de 10% sobre o valor do contrato.
- Decorrido o prazo de 45 (quarenta e cinco) dias de atraso injustificado na entrega e/ou na solução de chamado de atendimento, será caracterizada a inexecução total do contrato.

O cometimento reiterado de atrasos injustificados dos prazos previstos para entrega/solução dos serviços poderá resultar no cancelamento do registro de preços com a CONTRATADA.

As penalidades acima mencionadas serão aplicadas sem prejuízo das demais penalidades previstas em lei.

As multas e outras sanções administrativas só poderão ser relevadas motivadamente por conveniência administrativa, mediante ato devidamente justificado, expedido pela autoridade competente do CONTRATANTE.

Será garantido o direito à prévia e ampla defesa, sem prejuízo das responsabilidades civil e criminal, ressalvados os casos devidamente justificados e acatados pelo Tribunal.

4. Da confidencialidade de informações

4.1. Os conhecimentos, dados e informações de propriedade do CONTRATANTE, tanto tecnológicos, como administrativos, tais como: produtos, sistemas, técnicas, estratégias, métodos de operação e todos e quaisquer outros, repassados por força do objeto do contrato, constituem informação privilegiada e possuem caráter de confidencialidade.

4.2. Estas informações poderão ser utilizadas, só e exclusivamente, no cumprimento da execução das cláusulas e condições estabelecidas no contrato, sendo expressamente vedado à CONTRATADA:

4.2.1. Utilizá-las para fins não previstos no instrumento contratual;

4.2.2. Repassá-las a terceiros e/ou empregados não vinculados diretamente à execução do objeto contratado.

5. DOS REQUISITOS TÉCNICOS ESPECÍFICOS

5.1. Requisitos Gerais

5.1.1. O licenciamento da plataforma deverá ser por ativo, sendo este um dos abaixo:

5.1.1.1 Ativos em rede;
5.1.1.2 Servidores e Estações de trabalho ou Notebooks;
5.1.1.3. Servidores em Cloud;
5.1.1.4. Contêineres;
5.1.1.5. Aplicações Web e API;

5.1.2. O licenciamento poderá ser flexível, ou seja, não limitado por módulo.

5.1.3. O gerenciamento da plataforma deverá ser centralizado e único para todos os módulos descritos neste documento;

5.1.4. A solução deve fornecer alta disponibilidade, com cluster ativo – ativo, no site principal e site backup, com redundância da base de dados entre os sites.

5.2. Plataforma de Gestão de Vulnerabilidade em Ativos de Rede e Nuvem.

5.2.1. Características Gerais:

5.2.1.1. A solução deve ser licenciada para realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance) e indícios e padrões de códigos maliciosos conhecidos (malware);

5.2.1.2. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;

5.2.1.3. Deve possibilitar, por meio da console, no mínimo 4 (quatro) métodos de escaneamento:

5.2.1.3.1. Scan ativo;

5.2.1.3.2. Scan com uso de agentes;

5.2.1.3.3. Scan passivo;

5.2.1.3.4. Scanner em nuvem;

5.2.1.4 Deve ser capaz de identificar no mínimo 50.000 CVEs (Common Vulnerabilities and Exposures);

5.2.1.5 A solução deve ter a capacidade de adicionar etiquetas (tags) aos ativos de maneira automática, manual e possibilitar o uso de regras com parâmetros específicos para aplicação das mesmas;

5.2.1.6 . Deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv3 score;

5.2.1.7 . A solução deve calcular a criticidade e priorização de vulnerabilidades com base nos dados dos ativos, de preferência utilizando algoritmos de inteligência artificial (machine learning);

5.2.1.8. A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades;

5.2.1.9. A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente;

5.2.1.10. Deve possuir um sistema de busca de informações de um determinado ativo com, no mínimo, as seguintes características:

5.2.1.10.1. Por sistema operacional;

5.2.1.10.2. Por um determinado software instalado;

5.2.1.10.3. Por Ativos impactados.

5.2.1.11. Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente;

5.2.1.12. Possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual;

5.2.1.13. Deve possuir API abrangente para automação de processos e integração com aplicações terceiras, permitindo, no mínimo, a extração de dados para carga no SIEM;

5.2.1.14. Deve ser capaz de fazer a correlação diária de ameaças ativas contra as vulnerabilidades existentes na infraestrutura;

5.2.1.15. A solução poderá permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;

5.2.1.16. A solução deve possuir conectores para a seguintes plataformas:

5.2.1.16.1. Amazon Web Service (AWS);

5.2.1.16.2. Microsoft Azure;

5.2.1.16.3. Google Cloud Platform;

5.2.1.16.4. Oracle Cloud.

5.2.1.17. A solução deve ser capaz de produzir relatórios, no mínimo, nos seguintes formatos: PDF, CSV e HTML;
5.2.1.18. A solução deve ser capaz de identificar novos hosts no ambiente sem a necessidade de scan;
5.2.1.19. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
5.2.1.20. A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real;
5.2.1.21. Deve ser possível determinar quais portas estão abertas em determinado ativo;
5.2.1.22. Deve ser capaz de guardar no mínimo os seguintes atributos de um ativo:
5.2.1.22.1. Endereço IPv4 e IPv6;
5.2.1.22.2. Sistema Operacional;
5.2.1.22.3. Nome NetBIOS:
5.2.1.22.4. FQDN;
5.2.1.23. A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para, no mínimo:
5.2.1.23.1. Bancos de dados;
5.2.1.23.2. Hypervisors;
5.2.1.23.3. Dispositivos móveis;
5.2.1.23.4. Dispositivos de rede;
5.2.1.23.5. Endpoints;
5.2.1.23.6. Aplicações;
5.2.1.24. Deve realizar em tempo real a identificação de informações sensíveis no tráfego de rede do ambiente;
5.2.1.25. A solução deve ser capaz de identificar a comunicação de malwares na rede de forma passiva;
5.2.1.26. Deve ser capaz de, em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede;
5.2.1.27. A solução deve ser capaz de, em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede sem a necessidade de um agente;
5.2.1.28. Permitir identificar vulnerabilidades associadas a servidores de Banco de Dados no tráfego de rede em tempo real sem a necessidade de um agente;
5.2.1.29. A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBM QRadar, Microfocus ArcSight e Splunk;
5.2.1.30. A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços;
5.2.1.31. A solução deve ser capaz de realizar varreduras (scans) de vulnerabilidades para o número de ativos contratados;
5.2.1.32. A solução deve ser licenciada para uso de agentes instalados em estações de trabalho e servidores, para varredura diretamente no sistema operacional, no número total de ativos contratados.
5.2.1.33. A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como Hypervisors VMWare e Dispositivos de Rede;

5.2.1.34. A solução deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;
5.2.1.35. A solução deve fornecer agentes prontos para instalação em sistemas operacionais distintos, para monitoramento de configurações e vulnerabilidades;
5.2.1.36. A solução deve incluir possibilidade de gerenciamento de varreduras: execução, agendamento, exceções, frequências, horários e periodicidade.
5.2.1.37. A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;
5.2.1.38. A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;
5.2.1.39. A solução deverá apresentar o status da vulnerabilidade, demonstrando na interface de gerenciamento se a mesma é Nova, Persistente, Corrigida ou Reincidente no ativo
5.2.1.40. Deverá ser possível modificar a severidade das vulnerabilidades, de um único ativo ou múltiplos ativos;
5.2.1.41. A solução deve suportar o uso de Tags nos ativos, sendo estas aplicados de forma manual ou automática;
5.2.1.42. Deverá ser possível configurar quais usuários, ou grupos de usuários, podem editar as Tags;
5.2.1.43. A solução deverá usar as Tags como filtros, podendo ser utilizadas na lista de vulnerabilidades, onde o objetivo é ver todas as vulnerabilidades existentes nos ativos que possuem determinada Tag;
5.2.1.44. Ser possível fazer análise dos ativos através de Tags, como exemplo todos os Ativos que possuem a Tag Linux;

5.2.2. Controle de Usuários

5.2.2.1. A solução deve suportar RBAC (Role Based Access Control) com no mínimo 3 tipos de usuários pré-definidos;
5.2.2.2. Deve possuir no mínimo um perfil administrador e um perfil somente leitura;
5.2.2.3. Somente servidores da Contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;
5.2.2.4. A solução deve permitir a realização de autenticação com duplo fator através de protocolo RADIUS ou outros meios de comunicação;
5.2.2.5. A solução deve permitir, no mínimo, os seguintes métodos de autenticação: Usuário e senha, LDAP e Radius;
5.2.2.6. A solução deve possibilitar a criação de Grupos de Usuários;
5.2.2.7. Deve permitir configurar quais usuários, ou grupos de usuários, tem permissão de visualizar determinados ativos da organização e suas vulnerabilidades, e quais tem permissão de executar análises de vulnerabilidades nesses ativos;
5.2.2.8. Deve possibilitar configurar permissões, por usuário e grupo de usuário, específicas para cada política de análise de vulnerabilidades;

5.2.3. Relatórios e Dashboards

5.2.3.1. A solução deve suportar o envio automático de relatórios para destinatários específicos;
5.2.3.2. Deve ser possível definir a frequência na geração dos relatórios para, no mínimo: Diário, Mensal e Semanal;
5.2.3.3. A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou excluir painéis de acordo com a necessidade;
5.2.3.4. Deve possuir ao menos 5 modelos de dashboards já criados, podendo ser customizados;
5.2.3.5. Deve ser possível exportar os dados em HTML, PDF ou CSV;
5.2.3.6. Deve ser possível exportar os gráficos dos dashboards, através da console de gerenciamento, em PDF, PNG ou JPG;
5.2.3.7. Deve ser possível criar um novo Dashboard e definir este como padrão de visualização do usuário, ou seja, o primeiro Dashboard a aparecer na console no acesso;
5.2.3.8. Deve ser possível configurar um filtro permanente no Dashboards para apresentar informações de todos os ativos, ou somente ativos específicos do ambiente;
5.2.3.9. A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:
5.2.3.9.1. Hosts verificados sem credenciais;
5.2.3.9.2. Top 100 Vulnerabilidades mais críticas;
5.2.3.9.3. Top 10 Hosts infectados por Malwares;
5.2.3.9.4. Hosts exploráveis por Malwares;
5.2.3.9.5. Total de vulnerabilidades que podem ser exploradas pelo Metasploit;
5.2.3.9.6. Vulnerabilidades críticas e exploráveis;
5.2.3.9.7. Máquinas com vulnerabilidades que podem ser exploradas.

5.2.4. Conformidade

5.2.4.1. A solução deve ser totalmente licenciada para realizar scans de auditoria e compliance;
5.2.4.2. A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;
5.2.4.3. A solução deve ser licenciada para realizar scans de conformidade e compliance de forma ilimitada;
5.2.4.4. Toda a solução deve ser licenciada de modo a realizar scans de conformidade para os seguintes padrões: CIS, SCAP e OVAL;
5.2.4.5. A solução deverá possuir modelos prontos de padrões de configuração, no mínimo para: CIS, DISA e MSCT (Microsoft Security Compliance Toolkit)
5.2.4.6. Deve suportar a verificação de compliance para, no mínimo:
5.2.4.6.1. Bluecoat ProxySG;
5.2.4.6.2. Brocade Fabric OS;
5.2.4.6.3. Checkpoint;
5.2.4.6.4. Cisco IOS;
5.2.4.6.5. Citrix Xenserver;
5.2.4.6.6. Fireeye;

5.2.4.6.7. Fortinet FortiOS;
5.2.4.6.8. IBM iSeries;
5.2.4.6.9. Netapp Data ONTAP;
5.2.4.6.10. Palo Alto Firewall;
5.2.4.6.11. Red Hat Enterprise Virtualization;
5.2.4.6.12. Unix;
5.2.4.6.13. Windows;
5.2.4.6.14. VMware.

5.2.4.7. A solução deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;

5.2.4.8. O score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade;

5.2.4.9. Deve ser capaz de calcular a criticidade dos ativos da organização;

5.2.4.10. Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;

5.2.4.11. A solução deve gerar uma pontuação para cada um dos ativos, onde é levada em conta as vulnerabilidades presentes naquele ativo, assim como a classificação do ativo na rede (peso do ativo).

5.2.4.12. A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos.

5.2.4.13. A solução deve permitir um acompanhamento histórico do nível de exposição da organização;

5.2.4.14. Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução.

5.2.4.15. A solução deve possuir um gráfico indicativo do percentual de ativos com soluções de proteção de endpoint instaladas, bem como o nome e a versão da solução.

5.2.4.16. A solução deve permitir a segregação lógica entre áreas distintas da empresa a fim de obter a pontuação referente à exposição cibernética por área.

5.2.4.17. A solução deve permitir a segregação lógica entre aplicações distintas da empresa a fim de obter a pontuação referente à exposição cibernética por aplicação.

5.3.Plataforma de Gestão de Vulnerabilidades em Aplicações Web.

5.3.1. Características Gerais:

5.3.1.1. A solução de gestão de vulnerabilidades deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;

5.3.1.2. A solução deverá ser capaz de executar varreduras em sistemas web através de seus endereços FQDN (DNS);

5.3.1.3. Deve possuir modelos (templates) prontos de varreduras e também ser possível a criação de modelos customizados;

5.3.1.4. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:
5.3.1.4.1. Cookies, Headers, Formulários e Links;
5.3.1.4.2. Nomes e valores de parâmetros da aplicação;
5.3.1.4.3. Elementos JSON e XML;
5.3.1.4.4. Elementos DOM.
5.3.1.5. Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;
5.3.1.6. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;
5.3.1.7. Deve ser capaz de instituir no mínimo os seguintes limites:
5.3.1.7.1. Número máximo de URLs para crawl e navegação;
5.3.1.7.2. Número máximo de diretórios para varreduras;
5.3.1.7.3. Número máximo de profundidade dos elementos DOM;
5.3.1.7.4. Tamanho máximo de respostas;
5.3.1.7.5. Limite de requisições de redirecionamentos;
5.3.1.7.6. Tempo máximo para a varredura;
5.3.1.7.7. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;
5.3.1.7.8. Número máximo de requisições HTTP por segundo.
5.3.1.8. A solução deve ser capaz de detectar congestionamento de rede e limitar os seguintes aspectos da varredura:
5.3.1.8.1. Limite em segundos para timeout de requisições de rede;
5.3.1.8.2. Número máximo de timeouts antes que a varredura seja abortada.
5.3.1.9. Deve ser capaz de agendar a varredura e determinar sua frequência entre: única, diária, semanal e mensal;
5.3.1.10. Deve ser capaz de enviar notificações através de E-mail e, caso possível, outras formas;
5.3.1.11. Deverá avaliar sistemas web utilizando frameworks como AJAX, HTML5 e SPA;
5.3.1.12. Deverá possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma personalizada a ser enviada durante os testes;
5.3.1.13. Deverá ser compatível com avaliação de RESTful APIs;
5.3.1.14. Deverá suportar no mínimo os seguintes esquemas de autenticação:
5.3.1.14.1. Autenticação básica (digest);
5.3.1.14.2. NTLM;
5.3.1.14.3. Form de login;
5.3.1.14.4. Autenticação de Cookies;
5.3.1.14.5. Autenticação através de Selenium.
5.3.1.15. Deve ser capaz de importar scripts de autenticação selenium previamente configurados pelo usuário;
5.3.1.16. Deve ser capaz de customizar parâmetros Selenium como delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos;
5.3.1.17. Deve ser capaz de exibir os resultados das varreduras em dashboard dedicados para este tipo de análise;
5.3.1.18. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;

5.3.1.19. Para cada vulnerabilidade encontrada, devem ser exibidas as evidências da mesma em seus detalhes;
5.3.1.20. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc), deve evidenciar nos detalhes do evento encontrado:
5.3.1.20.1. Payload injetado;
5.3.1.20.2 Evidência em forma de resposta da aplicação;
5.3.1.20.3 Detalhes da requisição HTTP;
5.3.1.20.4 Detalhes da resposta HTTP.
5.3.1.21. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;
5.3.1.22. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;
5.3.1.23. A solução deve possuir suporte a varreduras de componentes para, no mínimo:
5.3.1.23.1. Wordpress;
5.3.1.23.2. AngularJS;
5.3.1.23.3. Apache;
5.3.1.23.4. Apache Tomcat;
5.3.1.23.5. Backbone.js;
5.3.1.23.6. ASP.NET;
5.3.1.23.7. Bootstrap;
5.3.1.23.8. Drupal;
5.3.1.23.9. Joomla!;
5.3.1.23.10. jQuery;
5.3.1.23.11. Magento;
5.3.1.23.12. Nginx;
5.3.1.23.13. PHP; e
5.3.1.23.14. AJAX.
5.3.1.24. A solução deverá possuir controle de permissão de usuários, com no mínimo ,3 níveis, sendo: Administrador, Operador de Scan e Somente Leitura;
5.3.1.25. Deverá possuir a capacidade de manter privado os resultados de um scan, ou seja, não aparecendo o resultado no dashboard da solução;
5.3.1.26. A solução poderá possuir scanners pré-configurados em nuvem, para realização de scans externos;
5.3.1.27. A solução deve possuir, também, sensores (scanner) on-premisses;
5.3.1.28. Deverá ser possível exportar os gráficos do dashboard em PDF, PNG ou JPEG, nativamente pelo console de gerência.
5.3.1.29. A solução deve suportar listas de exclusão globais;
5.3.1.30. Deve possuir um dicionário já criado com as principais páginas comuns e páginas de backup existentes.
5.3.1.31. Deve apresentar a nota do CVSSv3 nas vulnerabilidades encontradas;
5.3.1.32. A solução deverá gerar relatórios das vulnerabilidades, no mínimo em PDF, HTML e CSV.

5.4.Plataforma de Gestão de Vulnerabilidade em Contêineres

5.4.1. Características Gerais

5.4.1.1. A solução deverá ser licenciada contabilizando o número de imagens únicas, não sendo contabilizadas novas versões de uma mesma imagem;

5.4.1.2. A solução de gestão de vulnerabilidades deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações em Containers Docker como parte dos ativos a serem inspecionados;

5.4.1.3. A solução deve ser capaz de analisar imagens em Container utilizadas pelo TJPA, preparadas pelos desenvolvedores, em busca de vulnerabilidades identificadas e malwares residentes no sistema de arquivos;

5.4.1.4. A documentação de API da solução deverá ter acesso público através de website ou documentação do próprio fabricante;

5.4.1.5. A console de administração deverá possuir controle de acesso no mínimo permitindo usuários com capacidade de somente visualizar as informações, e usuários com capacidade para efetuar análise das imagens;

5.4.1.6. A solução deve inventariar o sistema operacional de cada imagem analisada e suas vulnerabilidades encontradas;

5.4.1.7. A solução deve ser capaz de identificar containers que não foram analisados antes de sua implementação em produção;

5.4.1.8. A solução deve analisar as camadas (layers) de um container;

5.4.1.9. A solução deve ser capaz de identificar containers que tiveram mudanças de arquivos entre a análise e a sua implementação em produção;

5.4.1.10. A solução deve ser capaz de identificar as devidas tags das imagens avaliadas;

5.4.1.11. A solução deve informar os CVEs para cada vulnerabilidade encontrada nos pacotes e bibliotecas residentes na imagem;

5.4.1.12. A solução deve ter a capacidade de testar automaticamente todas as imagens armazenadas, ou previamente testadas, sempre que uma nova vulnerabilidade for publicada e atualizada no banco de dados de vulnerabilidade da solução, sem qualquer tipo intervenção manual;

5.4.1.13. Deve ser capaz de inventariar os pacotes e bibliotecas e suas respectivas versões;

5.4.1.14. A solução deve possuir conectores e permitir importação de imagens, no mínimo, dos seguintes repositórios:

5.4.1.14.1. Docker HUB;

5.4.1.14.2. GitLab Container Registry;

5.4.1.14.3. Harbor;

5.4.1.14.4. Oracle Container Registry.

5.4.1.15. A solução deve fornecer scanner em formato Docker para implementação local e análise de imagens sem a necessidade de envio destas para repositório remoto, fora do ambiente da CONTRATANTE;

5.4.1.16. A solução ser capaz de configurar políticas usando como condições: CVSS Score, CVEs específicos e Malware identificado;

5.4.1.17. A solução deve permitir a criação de políticas específicas por repositório;
5.1.4.18. A solução deve prover integração com, no mínimo, as seguintes plataformas de integração contínua: GitLab, Jenkins, Argo CD, Travis CI e Kubernetes;
5.1.4.19. A solução deverá ser capaz de analisar vulnerabilidades também na infraestrutura, onde as imagens de container são executadas, tanto do sistema operacional quanto das aplicações que nele estão instaladas. Esta capacidade poderá ser:
5.4.1.19.1 Nativa da solução, desde que exista uma extensa compatibilidade de sistemas operacionais e aplicações relacionadas a container, algumas já explicitadas em itens anteriores, e já licenciada para uso;
5.4.1.19.2 Executada através de integração com terceiros, desde que toda a solução esteja licenciada para a CONTRATANTE.

6. PROPOSTA DE MODELOS A SEREM UTILIZADOS

O preço proposto para este fornecimento deve englobar os valores relativos a impostos, fretes, seguros, salários, encargos e demais despesas necessárias ao fornecimento completo do objeto.

As propostas comerciais deverão ser válidas, no mínimo, por 60 (sessenta) dias.

Deverá constar, obrigatoriamente, na proposta:

O preço unitário do item ofertado, considerando todos os componentes de hardware e software necessários à execução do serviço;

A descrição detalhada dos itens propostos, atendendo aos quantitativos e às especificações mínimas descritas neste Termo de Referência e em seus anexos, indicando os números de identificação dos serviços ofertados.

O fabricante poderá ser convocado a validar a compatibilidade dos itens e as declarações apresentadas, de modo a validar as condições de garantia existentes.

A proposta comercial, necessariamente, deverá atender a descrição dos itens propostos, conforme descrito neste Termo de Referência.

Todas as características técnicas obrigatórias deverão ser do fabricante e comprovadas por meio de folders, catálogos, manuais, impressão de páginas na Internet do fabricante ou testes realizados pelo CONTRATANTE, os quais deverão ser entregues juntamente com a proposta, em folhas numeradas e sequenciais.

7. INFORMAÇÕES COMPLEMENTARES

Não há

Belém, 16 de março de 2023

(ASSINATURA DOS MEMBROS DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO)