PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DO PARÁ
Coordenadoria de Infraestrutura Tecnologica

Termo de Referência de TIC

Processo SEI	0024137-90.2026.8.14.0900
Código PAC	SETIC102A26

1. DO OBJETO

1.1. Definição do Objeto

1.1.1. O objeto da contratação consiste no registro de preços para contratação de solução integrada de segurança cibernética, contemplando proteção de endpoints, gestão de exposição a riscos, detecção e resposta estendida — XDR, inspeção e análise de tráfego de rede, appliance dedicado, créditos de serviços XDR, serviços gerenciados de segurança, suporte, monitoramento, garantia e resposta a incidentes, conforme condições, quantidades e exigências estabelecidas neste Termo de Referência.

1.2. Descrição detalhada do Objeto

1.2.1. A solução deverá prover capacidade integrada de prevenção, detecção, análise, contenção, monitoramento e resposta a ameaças cibernéticas, com o objetivo de ampliar a segurança, a visibilidade, a rastreabilidade e a resiliência operacional do ambiente tecnológico do Tribunal de Justiça do Estado do Pará.

1.2.2. A solução deverá contemplar, no mínimo, os seguintes componentes:

1.2.2.1. **Proteção essencial de endpoints**, destinada à proteção ampla dos dispositivos finais do ambiente institucional, incluindo estações de trabalho, notebooks e demais ativos computacionais abrangidos pela solução.

1.2.2.2. **Proteção avançada de endpoints com recursos de EDR/XDR**, destinada aos ativos de maior criticidade, incluindo servidores, estações de usuários privilegiados e demais ativos estratégicos ou sensíveis, com capacidade de detecção, investigação, resposta remota e contenção de ameaças.

1.2.2.3. **Gestão de exposição a riscos cibernéticos**, destinada à identificação, avaliação, priorização e acompanhamento de vulnerabilidades, exposições, configurações inseguras e demais condições que possam ampliar a superfície de ataque do ambiente tecnológico do TJPA.

1.2.2.4. **Plataforma de detecção e análise de tráfego de rede**, com integração à arquitetura de resposta estendida, destinada ao monitoramento centralizado do tráfego de rede, à identificação de comportamentos anômalos e à geração de evidências técnicas para apoio à resposta a incidentes.

1.2.2.5. **Appliance dedicado de detecção e análise de rede**, destinado ao processamento e monitoramento de tráfego, compatível com a necessidade de inspeção do ambiente institucional e com os requisitos de desempenho definidos para a solução.

1.2.2.6. **Créditos de serviços XDR ou de plataforma de segurança**, destinados ao consumo de funcionalidades sob demanda, processamento adicional de eventos, análise de arquivos em ambiente seguro, uso de recursos avançados da plataforma e demais funcionalidades associadas à operação da solução.

1.2.2.7. **Serviços gerenciados de segurança**, incluindo suporte, monitoramento contínuo, triagem de alertas, análise de eventos, comunicação de incidentes, orientação técnica, apoio à contenção e resposta a incidentes de segurança da informação durante o período contratado.

1.2.3. A solução deverá operar de forma integrada e centralizada, permitindo administração unificada, aplicação de políticas de segurança, correlação de eventos de múltiplas fontes, geração de relatórios, registro de evidências, rastreabilidade das ações executadas e acompanhamento pela equipe técnica do TJPA.

1.2.4. A contratação deverá incluir todos os recursos necessários ao pleno funcionamento da solução durante a vigência contratual, abrangendo licenças ou subscrições, appliance, suporte técnico, garantia, atualizações, correções, manutenção, serviços especializados, documentação técnica, transferência de conhecimento e demais atividades necessárias à implantação, sustentação e operação da solução.

1.2.5. Segue o quantitativo detalhado para a composição do objeto:

GRUPO ÚNICO

Item	Descrição	Catmat/ Catser	Unidade	Quantidade	Valor Unitário	Valor Total
01	TrendAi Endpoint Security Essentials	27502	Licença	8.000	R$ 490,87	R$ 3.926.960,0
02	TrendAi Endpoint Security Pro	27502	Licença	1.000	R$ 2.398,00	R$ 2.398.000,(
03	TrendAi Cyber Risk Exposure Management Core	27502	Licença	9.000	R$ 161,37	R$ 1.452.330,0
04	TrendAi Deep Discovery Inspector Series 9000 - 10Gb software only com XDR	27502	Licença	01	R$ 5.994.083,33	R$ 5.994.083,3
05	TrendAi Deep Discovery 9000 Hardware	462071	Equipamento	01	R$ 922.154,32	R$ 922.154,32
06	Créditos Trend AI Flex Vision One	27502	Créditos	200.000	R$ 6,28	R$ 1.256.000,0
07	Serviços gerenciados de segurança para suporte e monitoramento, contendo ações corretivas, preventivas e de resposta a incidentes, contendo ações corretivas, preventivas e de resposta a incidentes	26980	Mês	24	R$ 41.696,67	R$ 1.000.720,0
VALOR TOTAL DA CONTRATAÇÃO						**R$ 16.950.247**

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. Motivação

A contratação é motivada pela necessidade de evolução da maturidade de segurança cibernética do Tribunal de Justiça do Estado do Pará, considerando a criticidade dos sistemas judiciais e administrativos, a crescente digitalização dos serviços institucionais e a necessidade de assegurar a disponibilidade, a integridade e a confidencialidade das informações tratadas no ambiente tecnológico do TJPA.

O ambiente institucional do TJPA está exposto a ameaças cibernéticas cada vez mais sofisticadas, incluindo ataques de ransomware, exploração de vulnerabilidades críticas, uso de credenciais comprometidas, movimentação lateral em redes corporativas, exfiltração de dados e execução de códigos maliciosos com técnicas evasivas. Tal cenário exige mecanismos integrados de prevenção, detecção, análise, contenção, monitoramento e resposta a incidentes.

A solução atualmente utilizada para proteção de endpoints e segurança de ativos decorre do Contrato nº 036/2021, cuja vigência se encerra em 22 de julho de 2026, sem possibilidade de nova prorrogação, conforme registrado no Estudo Técnico Preliminar. A solução existente, embora adequada ao contexto tecnológico de sua contratação, encontra-se defasada diante da evolução das ameaças cibernéticas, por não contemplar, de forma integrada, capacidades avançadas de detecção e resposta estendida, correlação automatizada de eventos, visibilidade sobre múltiplas camadas e apoio especializado à resposta a incidentes.

A ausência de contratação tempestiva poderá comprometer a continuidade da proteção dos ativos computacionais do TJPA, ampliar a exposição da infraestrutura tecnológica a incidentes de segurança e elevar o risco de indisponibilidade dos serviços judiciais e administrativos.

A contratação deverá permitir ao TJPA evoluir de modelo predominantemente centrado em proteção tradicional de endpoints para arquitetura integrada de segurança cibernética, com proteção de ativos, detecção e resposta estendida, inspeção de tráfego de rede, gestão de exposição a riscos, monitoramento contínuo e resposta a incidentes.

A demanda está diretamente vinculada à necessidade de garantir a continuidade dos sistemas, a segurança das informações e a proteção dos serviços críticos do Poder Judiciário do Estado do Pará, reduzindo riscos de downtime, otimizando a atuação da equipe técnica, apoiando a conformidade com a LGPD e ampliando a capacidade de contenção e resposta imediata a incidentes.

2.2. Alinhamento com o Plano Anual de Contratações e ao Plano Diretor de TIC

CÓDIGO DO PAC		SETIC102A26
ID	**AÇÃO DO PDTIC**	**META DO PDTIC ASSOCIADA**
N14	Contratar serviço de gestão e correlação de eventos de segurança para resposta a incidentes de Segurança da Informação.	Aprimorar a Segurança da Informação e a Gestão de Dados.
ID	**OBJETIVO NO PLANEJAMENTO ESTRATÉGICO**	**MACRODESAFIO**
OEPE02	Aprimorar o Domínio de Serviços de TIC.	Aprimorar a segurança da informação e a Gestão de Dados.

2.3. Objetivos

2.3.1. A contratação possui como objetivo geral fortalecer a capacidade institucional do TJPA de prevenir, detectar, analisar, conter, monitorar e responder a ameaças cibernéticas, assegurando maior proteção aos ativos de TIC, continuidade dos serviços jurisdicionais e resiliência operacional do ambiente tecnológico.

2.3.2. Constituem objetivos específicos da contratação:

2.3.2.1. Proteger os endpoints, servidores e demais ativos computacionais abrangidos pela solução contra códigos maliciosos, ransomware, ameaças persistentes, comportamentos suspeitos e execuções não autorizadas.

2.3.2.2. Ampliar a visibilidade da equipe técnica sobre o ambiente tecnológico institucional, por meio de gerenciamento centralizado, correlação de eventos, registro de evidências e geração de relatórios técnicos.

2.3.2.3. Implementar capacidades de detecção e resposta estendida, permitindo investigação, contenção, isolamento e resposta coordenada a incidentes de segurança da informação.

2.3.2.4. Identificar, avaliar e priorizar exposições, vulnerabilidades e configurações inseguras presentes no ambiente tecnológico do TJPA, possibilitando atuação preventiva orientada a riscos.

2.3.2.5. Monitorar e analisar o tráfego de rede institucional, especialmente nos pontos críticos do ambiente, com capacidade compatível com a infraestrutura do Tribunal.

2.3.2.6. Disponibilizar serviços gerenciados de segurança, suporte técnico, monitoramento contínuo e resposta a incidentes durante a vigência contratual.

2.3.2.7. Reduzir o tempo médio de detecção e o tempo médio de resposta a incidentes de segurança, minimizando impactos sobre os serviços judiciais e administrativos.

2.3.2.8. Garantir rastreabilidade das ações executadas, preservação de evidências, apoio à auditoria e conformidade com requisitos legais, regulatórios e institucionais aplicáveis à segurança da informação e à proteção de dados pessoais.

2.4. Referência aos Estudos Técnicos Preliminares

2.4.1. Este Termo de Referência foi elaborado considerando o Documento de Oficialização da Demanda (DOD) encaminhado pelo Gabinete da Secretaria de Tecnologia da Informação e Comunicação e os Estudos Técnicos Preliminares constantes do Processo Administrativo Eletrônico n° 0024137-90.2026.8.14.0900.

2.5. Análise de Mercado de TIC

2.5.1. Considerando as necessidades e os requisitos da demanda, foram avaliadas no Estudo Técnico Preliminar as seguintes alternativas de solução de TIC:

2.5.1.1. Solução 1: plataforma integrada de segurança cibernética com proteção, detecção, gestão de

exposição a riscos e serviços gerenciados.

2.5.1.2. Solução 2: plataforma de proteção de endpoints com EDR ou XDR e suporte especializado.

2.5.1.3. **Solução 3: desenvolvimento próprio ou customização interna de solução de segurança cibernética**.

2.5.2. O ETP registrou consulta ao Catálogo de Software Público Brasileiro, por meio da qual foi constatada a inexistência de soluções públicas capazes de atender ao escopo pretendido, especialmente quanto às funcionalidades de endpoint, XDR, segurança cibernética e detecção e resposta.

2.5.3. A Solução 1 foi considerada a alternativa mais adequada, por consolidar capacidades preventivas, detectivas e responsivas em arquitetura unificada, permitindo maior visibilidade do ambiente, correlação de eventos de segurança, resposta coordenada a incidentes, acompanhamento da superfície de exposição a riscos e suporte especializado à operação contínua.

2.5.4. A Solução 2 foi considerada inviável como alternativa autônoma para atendimento integral da demanda, em razão do atendimento parcial de requisitos críticos, especialmente quanto à inspeção e análise de tráfego de rede, à gestão integrada de exposição a riscos, à visibilidade abrangente do ambiente institucional e à correlação de eventos provenientes de múltiplas fontes.

2.5.5. A Solução 3 foi considerada inviável em razão do baixo índice de compatibilidade, da complexidade técnica, da incompatibilidade temporal com a necessidade institucional e da ausência de capacidade imediata comprovada para atender aos requisitos críticos de correlação de múltiplas fontes, inspeção de tráfego de rede, gestão de exposição a riscos, disponibilidade, desempenho e resposta efetiva a ameaças modernas.

2.5.6. A solução escolhida deverá ser especificada por requisitos funcionais, tecnológicos, operacionais e de segurança, de forma a preservar a competitividade, evitar direcionamento indevido e assegurar que a proposta vencedora atenda integralmente às necessidades institucionais descritas no ETP.

2.6. Benefícios e Resultados

2.6.1. A contratação deverá produzir os seguintes benefícios e resultados esperados:

2.6.1.1. Fortalecimento da segurança da informação institucional, com redução da probabilidade e do impacto de incidentes cibernéticos.

2.6.1.2. Aumento da disponibilidade e da confiabilidade dos sistemas judiciais e administrativos, assegurando a continuidade da prestação jurisdicional.

2.6.1.3. Modernização da arquitetura de segurança, com adoção de abordagem integrada baseada em XDR, inspeção de tráfego de rede e análise orientada a riscos.

2.6.1.4. Melhoria da governança de segurança da informação, com geração de evidências, relatórios, registros e trilhas de auditoria.

2.6.1.5. Otimização dos recursos humanos de TIC, reduzindo a carga operacional da equipe interna e permitindo maior foco em atividades estratégicas.

2.6.1.6. Maior eficiência na resposta a incidentes, com redução do tempo de detecção e do tempo de resposta.

2.6.1.7. Aderência às melhores práticas e diretrizes de segurança cibernética aplicáveis ao setor público e ao Poder Judiciário.

2.6.2. Os benefícios esperados constam do ETP e incluem fortalecimento da segurança da informação, aumento da disponibilidade dos sistemas, modernização da arquitetura de segurança, melhoria da governança, otimização da equipe interna e maior eficiência na resposta a incidentes.

2.7. Relação entre a Demanda Prevista e a Contratada

Item	Descrição	Métrica	Quantidade
1	TrendAi Endpoint Security Essentials	Endpoint	8.000
2	TrendAi Endpoint Security Pro	Endpoint	1.000
3	TrendAi Cyber Risk Exposure Management Core	Ativo	9.000
4	TrendAi Deep Discovery Inspector Series 9000 - 10Gb software only com XDR	Licença	01
5	TrendAi Deep Discovery 9000 Hardware	Equipamento	01
6	Créditos Trend AI Flex Vision One	Créditos	200.000
7	Serviços gerenciados de segurança para suporte e monitoramento, contendo ações corretivas, preventivas e de resposta a incidentes, contendo ações corretivas, preventivas e de resposta a incidentes	Mês	24

2.7.1. A demanda prevista e a contratada foram estimadas a partir da seguinte metodologia:

2.7.1.1. Os quantitativos da solução foram definidos com base no ambiente tecnológico atualmente existente no Tribunal de Justiça do Estado do Pará, considerando a expansão institucional prevista, a criticidade dos ativos de TIC e as melhores práticas de segurança cibernética adotadas pelo mercado.

Para os itens 1 e 2, referentes à proteção de endpoints (EPP/EDR/XDR), estimou-se um universo aproximado de 6.500 ativos, contemplando os equipamentos atualmente em operação, inclusive os 2.000 novos notebooks recentemente adquiridos em decorrência da ampliação do quadro funcional. Com vistas a assegurar cobertura integral do parque computacional, foi previsto o quantitativo de 8.000 licenças de proteção essencial para endpoints. Adicionalmente, foram previstas 1.000 licenças de proteção avançada, com recursos de EDR/XDR, destinadas aos ativos de maior criticidade, tais como servidores, estações de trabalho de usuários privilegiados e demais ativos estratégicos ou sensíveis. A adoção dessa estratégia observa prática consolidada de mercado, que recomenda a aplicação de mecanismos avançados de detecção e resposta prioritariamente nos ativos que apresentam maior risco operacional e de segurança.

O quantitativo do item 3, referente à solução de gestão de exposição a riscos, foi definido considerando a totalidade dos ativos inventariados e projetados para o ambiente institucional, estimados em aproximadamente 9.000 ativos, de modo a assegurar cobertura integral da superfície de ataque do ambiente tecnológico do TJPA.

Para os itens 4 e 5, relativos à solução de Network Detection and Response (NDR) e ao respectivo appliance dedicado, foi previsto um único conjunto composto por uma licença de software e um appliance específico para processamento e monitoramento do tráfego de rede. O dimensionamento considerou a necessidade de monitoramento centralizado do tráfego do datacenter principal do Tribunal, incluindo enlaces de alta capacidade de até 10 Gbps, sendo suficiente para a cobertura inicial do ambiente e passível de expansão futura conforme a evolução das necessidades institucionais.

No que se refere ao item 6, correspondente aos créditos de consumo da plataforma de segurança, o quantitativo foi estabelecido de acordo com o modelo operacional da solução, contemplando atividades como análise de arquivos em ambiente sandbox, processamento adicional de eventos de segurança e utilização de funcionalidades disponibilizadas sob demanda pela plataforma XDR.

Por sua vez, para o item 7, relativo aos Serviços Gerenciados de Segurança (Managed Security Services – MSS), foi definido período de prestação de 24 meses, considerando a necessidade de operação contínua dos serviços de monitoramento e resposta a incidentes em regime 24 horas por dia, sete dias por semana, bem como a compatibilidade com a vigência usualmente adotada para contratações de serviços de TIC e a necessidade de garantir a sustentação adequada da solução durante seu ciclo inicial de operação.

Os quantitativos definidos buscam assegurar cobertura adequada do ambiente tecnológico atual e futuro do TJPA, observando sua expansão institucional, a criticidade dos ativos envolvidos e uma abordagem moderna de segurança cibernética baseada em gestão de riscos, priorizando a aplicação de recursos avançados nos ativos estratégicos e garantindo monitoramento contínuo, visibilidade operacional e capacidade efetiva de resposta a incidentes de segurança.

2.8. Impacto Ambiental

2.8.1. A contratação apresenta impacto ambiental reduzido, considerando que a solução será composta

majoritariamente por licenças, subscrições, serviços especializados e componentes de operação em ambiente de TIC já existente.

2.8.2. O impacto ambiental direto está associado ao fornecimento e à operação do appliance dedicado de detecção e análise de tráfego de rede, ao consumo energético ordinário do equipamento e à eventual necessidade de substituição, recolhimento ou descarte de componentes eletrônicos durante ou ao final da vigência contratual.

2.8.3. A implantação deverá priorizar execução remota sempre que tecnicamente possível, reduzindo deslocamentos, consumo de recursos e impactos ambientais indiretos.

2.8.4. O ETP registra que não foi identificada necessidade de adequação ambiental específica para recepção da solução, sendo os impactos ambientais reduzidos e limitados à utilização ordinária de equipamentos tecnológicos e recursos computacionais já existentes no ambiente institucional.

2.9. Impacto Social e Cultural

2.9.1. A contratação produzirá impacto social positivo ao contribuir para a continuidade, confiabilidade e segurança dos serviços digitais prestados pelo Poder Judiciário do Estado do Pará, reduzindo riscos de indisponibilidade de sistemas judiciais e administrativos utilizados por magistrados, servidores, advogados, membros do Ministério Público, Defensoria Pública, partes e demais usuários dos serviços jurisdicionais.

2.9.2. A contratação também fortalecerá a cultura institucional de segurança da informação, ao ampliar a capacidade de monitoramento, registro, resposta, governança, auditoria e tratamento de incidentes no ambiente tecnológico do TJPA.

2.9.3. A execução contratual deverá observar práticas de não discriminação, proteção de dados pessoais, confidencialidade, sigilo das informações institucionais e respeito às normas internas do TJPA.

2.10. Critérios de Sustentabilidade

2.10.1. A contratada deverá observar, durante toda a execução contratual, critérios de sustentabilidade compatíveis com a natureza da solução, especialmente quanto ao uso eficiente de recursos tecnológicos, redução de deslocamentos, utilização de documentação eletrônica e descarte ambientalmente adequado de equipamentos ou componentes eletrônicos, quando aplicável.

2.10.2. O appliance fornecido deverá observar requisitos de eficiência energética, segurança elétrica e conformidade com normas técnicas aplicáveis ao equipamento.

2.10.3. A contratada deverá providenciar, quando cabível, a destinação ambientalmente adequada de equipamentos, peças, componentes eletrônicos, pilhas, baterias ou materiais substituídos no curso da execução contratual, observadas as normas aplicáveis à logística reversa e ao descarte de resíduos eletroeletrônicos.

2.10.4. A execução dos serviços deverá priorizar meios digitais para abertura de chamados, envio de relatórios, comunicação formal, documentação técnica, evidências de execução e acompanhamento contratual.

2.10.5. A Instrução Normativa nº 01/2023 do TJPA prevê a descrição de possíveis impactos ambientais e respectivas medidas mitigadoras, incluindo requisitos de baixo consumo de energia e logística reversa para desfazimento e reciclagem de bens e refugos, quando aplicável.

2.11. Conformidade Legal

2.11.1. A contratação deverá observar a legislação e os normativos aplicáveis às contratações públicas de soluções de tecnologia da informação e comunicação, especialmente a Lei nº 14.133/2021, a Resolução CNJ nº 468/2022, a Instrução Normativa nº 01/2023 do TJPA, a Instrução Normativa nº 02/2024-GP do TJPA e demais normas internas aplicáveis ao planejamento, seleção do fornecedor, execução, gestão e fiscalização contratual.

2.11.2. A solução deverá observar a Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais, no que couber, especialmente quanto à confidencialidade, segurança, rastreabilidade, tratamento adequado de dados pessoais e comunicação de incidentes de segurança que possam envolver dados pessoais.

2.11.3. A contratação deverá observar as políticas e normas de segurança da informação adotadas pelo TJPA,

bem como as diretrizes de segurança cibernética aplicáveis ao Poder Judiciário.

2.11.4. A solução não tem por finalidade a interoperabilidade entre sistemas judiciais, a assinatura digital ou a gestão de processos e documentos eletrônicos, razão pela qual o Modelo Nacional de Interoperabilidade — MNI, a Infraestrutura de Chaves Públicas Brasileira — ICP-Brasil e o MoReq-Jus não se aplicam diretamente ao objeto. Ainda assim, a solução deverá permitir integração técnica com o ambiente de TIC do TJPA, comunicação segura entre seus componentes, exportação de logs, armazenamento de registros, rastreabilidade de eventos e apoio à auditoria técnica.

2.11.5. Os procedimentos de segurança da informação e o processamento das informações deverão estar em conformidade com as políticas, normas, controles e procedimentos internos adotados pelo TJPA, sem prejuízo da observância das obrigações de sigilo, confidencialidade, proteção de dados, continuidade operacional e rastreabilidade previstas neste Termo de Referência e no futuro instrumento contratual.

3. DA LICITAÇÃO

3.1. Natureza do Objeto da Contratação

3.1.1. O objeto caracteriza-se como solução integrada de bens e serviços de Tecnologia da Informação e Comunicação, composta por licenciamento ou subscrição de software especializado de segurança cibernética, fornecimento de appliance dedicado, suporte técnico, manutenção, monitoramento contínuo e resposta a incidentes.

3.1.2. A contratação possui natureza continuada quanto aos serviços de suporte, manutenção, monitoramento, sustentação e resposta a incidentes, sem dedicação exclusiva de mão de obra, e natureza de fornecimento quanto às licenças, subscrições, créditos de plataforma e appliance dedicado.

3.1.3. A solução poderá ser licitada como bem e serviço comum de TIC, uma vez que seus padrões de desempenho, qualidade, compatibilidade, suporte, garantia, níveis de serviço e critérios de aceite podem ser objetivamente definidos no edital, no Termo de Referência e em seus anexos.

3.1.4. O Estudo Técnico Preliminar classifica a contratação como solução integrada de bens e serviços de TIC, composta por licenciamento ou subscrição de software, componentes tecnológicos necessários à operação e serviços continuados de suporte, manutenção, monitoramento e resposta a incidentes.

3.2. Parcelamento e Adjudicação

3.2.1. O objeto não será parcelado, devendo ser adjudicado de forma global, em grupo único.

3.2.1.1. A contratação em grupo único decorre da natureza integrada, complementar e interdependente da solução, cujos componentes tecnológicos e serviços especializados devem atuar de forma coordenada para prover proteção de endpoints, detecção e resposta estendida, inspeção e análise de tráfego de rede, gestão de exposição a riscos, monitoramento contínuo, suporte técnico e resposta a incidentes.

A divisão do objeto em itens ou grupos independentes comprometeria a unidade funcional da solução, fragmentaria a responsabilidade técnica sobre a proteção do ambiente institucional e ampliaria os riscos de incompatibilidade entre componentes, falhas de integração, sobreposição de responsabilidades, lacunas de monitoramento e dificuldade de correlação de eventos de segurança.

A adjudicação global preserva a responsabilidade integral da contratada pela entrega, implantação, configuração, integração, operação, suporte, monitoramento, manutenção, sustentação e evolução operacional da solução de segurança cibernética.

O ETP registra que os resultados esperados dependem da atuação coordenada e integrada de todos os componentes tecnológicos e serviços associados, razão pela qual a contratação foi caracterizada como solução única e indivisível sob o ponto de vista técnico e operacional, com adjudicação global em grupo único.

3.3. Modalidade e Tipo de Licitação

3.3.1. A contratação será realizada por meio de licitação, na modalidade Pregão, em sua forma eletrônica,

mediante Sistema de Registro de Preços, com critério de julgamento pelo menor preço global do lote único.

3.3.2. A adoção do Sistema de Registro de Preços é adequada à natureza da solução, considerando a necessidade de registrar quantitativos estimados, permitir contratação conforme a efetiva necessidade administrativa e preservar flexibilidade para atendimento do ambiente tecnológico do TJPA durante a vigência da ata.

3.3.3. O critério de julgamento pelo menor preço global do lote único é compatível com a necessidade de contratação integrada da solução, desde que a proposta vencedora atenda integralmente às especificações técnicas, aos requisitos de segurança, aos níveis de serviço, aos critérios de aceite e às demais condições estabelecidas neste Termo de Referência.

3.3.4. O modo de disputa adotado será o aberto, com apresentação de lances públicos e sucessivos pelos licitantes, observadas as regras do sistema eletrônico utilizado pelo TJPA.

3.3.4.1. A adoção do modo de disputa aberto justifica-se pela natureza comum do objeto, pela possibilidade de definição objetiva dos requisitos técnicos mínimos e pela expectativa de obtenção de maior competitividade e economicidade mediante disputa sucessiva de preços entre licitantes aptos a fornecer a solução integrada.

3.3.4.2. O modo de disputa aberto é compatível com o critério de julgamento pelo menor preço global do lote único, pois permite a redução progressiva dos valores ofertados sem afastar a exigência de atendimento integral às especificações técnicas, aos níveis de serviço, aos critérios de aceite e às demais condições previstas neste Termo de Referência e no edital.

3.4. Forma e Critérios de Seleção do Fornecedor

3.4.1. Será selecionada a proposta que apresentar o menor preço global para o lote único, desde que atenda integralmente às exigências técnicas, operacionais, comerciais, de segurança, habilitação, suporte, garantia, manutenção, monitoramento e resposta a incidentes estabelecidas neste Termo de Referência.

3.4.2. A proposta deverá contemplar todos os itens do lote único, não sendo admitida proposta parcial, supressão de item, alteração unilateral de quantitativos ou oferta que comprometa a integração da solução.

3.4.3. A análise de aceitabilidade da proposta deverá considerar, no mínimo:

3.4.3.1. compatibilidade da solução ofertada com os requisitos técnicos estabelecidos;

3.4.3.2. atendimento integral aos quantitativos previstos;

3.4.3.3. comprovação da capacidade de fornecimento, implantação, suporte, manutenção, monitoramento e resposta a incidentes;

3.4.3.4. atendimento aos níveis mínimos de serviço exigidos;

3.4.3.5. compatibilidade dos preços unitários e global com o orçamento estimado;

3.4.3.6. apresentação de documentação técnica suficiente para demonstrar aderência da solução aos requisitos do objeto;

3.4.3.7. comprovação de autorização para comercialização, implantação e suporte da solução ofertada, quando a licitante não for fabricante ou detentora da tecnologia.

3.4.4. A proposta que apresentar o menor preço global, mas não comprovar atendimento integral aos requisitos técnicos e operacionais da contratação, deverá ser recusada, sem prejuízo da realização de diligência para esclarecimento de informações, desde que não haja alteração substancial da proposta.

3.4.5. Não será admitida a participação de empresas reunidas em consórcio.

3.4.5.1. A vedação à participação de consórcios justifica-se pela natureza integrada da solução, que exige responsabilidade técnica, operacional e contratual única sobre o fornecimento, implantação, configuração,

integração, suporte, monitoramento contínuo, manutenção e resposta a incidentes de segurança cibernética. A execução do objeto por empresas consorciadas poderia gerar fragmentação de responsabilidades, dificuldade de apuração de falhas, sobreposição de competências, divergência na condução técnica dos serviços e risco à rastreabilidade das ações executadas no ambiente tecnológico do TJPA.

A solução pretendida encontra-se disponível no mercado por fornecedores aptos a entregar integralmente os componentes tecnológicos e os serviços associados, não sendo necessária a reunião de empresas para viabilizar a participação no certame ou ampliar a competitividade. A vedação ao consórcio preserva a eficiência da gestão contratual, a segurança da informação, a cadeia de responsabilização, a confidencialidade das informações tratadas e o cumprimento dos níveis de serviço estabelecidos para a proteção do ambiente institucional.

3.4.6. Não será admitida a participação de cooperativas.

3.4.6.1. A vedação à participação de cooperativas decorre da incompatibilidade entre o objeto da contratação e o regime cooperativo, considerando que a execução envolve atividades críticas de segurança cibernética, monitoramento contínuo, suporte especializado, resposta a incidentes, controle de acesso, tratamento de informações sensíveis e cumprimento de níveis de serviço com responsabilização direta da contratada.

A contratação exige estrutura operacional permanente, equipe técnica qualificada, atuação coordenada, supervisão contínua, disponibilidade para atendimento a incidentes e capacidade de resposta tempestiva, características que demandam organização empresarial compatível com a assunção integral dos riscos e obrigações contratuais. A participação de cooperativas poderia comprometer a responsabilização objetiva pela execução do objeto, a continuidade operacional dos serviços, a gestão dos acessos ao ambiente tecnológico do TJPA, a rastreabilidade das ações executadas e o cumprimento dos níveis de serviço exigidos. A vedação não possui caráter restritivo indevido, pois decorre das características técnicas, operacionais e de segurança do objeto, preservando a adequada execução contratual, a confidencialidade das informações institucionais e a proteção dos ativos de TIC do Tribunal.

3.5. Da subcontratação

3.5.1. Não será admitida a subcontratação do objeto principal, compreendendo o licenciamento ou subscrição da plataforma, o fornecimento do appliance dedicado, a implantação da solução, a operação dos serviços gerenciados de segurança, o suporte técnico, o monitoramento contínuo e a resposta a incidentes.

3.5.1.1. A vedação à subcontratação decorre da natureza crítica do objeto, que envolve acesso a informações sensíveis, infraestrutura de rede, servidores, estações, registros de segurança, evidências técnicas e dados institucionais do TJPA. A execução por terceiros não avaliados no procedimento licitatório poderia comprometer a rastreabilidade das ações executadas, a cadeia de custódia das evidências, o controle de acesso, a confidencialidade das informações, a responsabilização técnica e o cumprimento dos níveis de serviço.

3.5.2. A contratada deverá executar o objeto sob sua responsabilidade direta, com equipe qualificada e compatível com a solução ofertada, respondendo integralmente perante o TJPA pelo cumprimento das obrigações contratuais, técnicas, legais, operacionais e de segurança da informação.

3.5.3. Não se caracteriza como subcontratação a aquisição de licenças, subscrições, appliance, peças, componentes, insumos ou suporte técnico de terceiro nível prestado diretamente pelo fabricante, distribuidor autorizado ou detentor da tecnologia, desde que a contratada permaneça responsável pela gestão, implantação, suporte, monitoramento, operação dos serviços gerenciados e atendimento ao TJPA.

3.6. Da Indicação de Marca

3.6.1. Fica admitida, para a presente contratação, a indicação da marca/fabricante Trend Micro, em razão da necessidade de padronização tecnológica, compatibilidade com o ambiente atualmente implantado, continuidade operacional, preservação dos investimentos já realizados e mitigação dos riscos técnicos associados à substituição integral da solução de segurança cibernética em uso no TJPA.

3.6.1.1. A indicação da marca/fabricante decorre de justificativa técnica registrada no Estudo Técnico Preliminar, segundo a qual o TJPA já utiliza solução de segurança de endpoints baseada em tecnologia do referido fabricante, com licenças adquiridas, componentes operacionais integrados à rotina institucional, políticas de segurança configuradas, histórico operacional, registros de eventos, regras de monitoramento, procedimentos de resposta e conhecimento técnico acumulado pela equipe interna.

A manutenção do mesmo ecossistema tecnológico deverá permitir a evolução da solução atualmente implantada para arquitetura mais abrangente e integrada, contemplando capacidades avançadas de proteção de endpoints, detecção e resposta estendida, inspeção e análise de tráfego de rede, gestão de exposição a riscos, serviços gerenciados de segurança, monitoramento contínuo e resposta a incidentes.

A substituição integral por solução de fabricante distinto implicaria custos diretos e indiretos relevantes, incluindo desinstalação e substituição de agentes, implantação de nova console de gerenciamento, reconfiguração de políticas de segurança, reconstrução de regras de detecção e resposta, reintegração com serviços corporativos, revalidação de compatibilidade com estações, servidores e ambiente de rede, nova parametrização de alertas, recriação de relatórios, capacitação da equipe interna e eventual necessidade de operação paralela durante período de transição.

A substituição por solução de fabricante distinto também poderia gerar riscos operacionais sensíveis ao ambiente de segurança cibernética, tais como janelas de menor visibilidade, sobreposição temporária de agentes, conflitos de configuração, aumento de falsos positivos ou falsos negativos, perda de histórico operacional, degradação temporária da capacidade de resposta a incidentes e aumento do esforço de acompanhamento pela equipe interna do TJPA.

A indicação da marca/fabricante não se fundamenta em preferência subjetiva, mas em critérios técnicos, operacionais e econômicos relacionados à continuidade da proteção cibernética, à interoperabilidade dos componentes, à preservação da maturidade operacional já alcançada, à redução dos riscos de transição e ao aproveitamento da base técnica atualmente existente.

3.6.2. A indicação da marca/fabricante não restringe a participação no certame ao fabricante da solução, sendo admitida a participação de licitantes, revendedores, integradores, distribuidores ou parceiros autorizados que comprovem capacidade para comercializar, implantar, configurar, prestar suporte, manter, monitorar e operar a solução, conforme exigências deste Termo de Referência e do edital.

3.6.3. A contratada deverá assegurar a regularidade do licenciamento, a continuidade das atualizações, o acesso aos canais oficiais de suporte, a garantia dos componentes contratados, a manutenção da solução durante a vigência contratual e a prestação dos serviços associados, permanecendo integralmente responsável perante o TJPA pela execução do objeto.

3.6.4. A indicação da marca/fabricante deverá ser interpretada de forma restrita às condições técnicas que justificam a padronização e a continuidade tecnológica, não afastando a obrigação de atendimento integral aos requisitos funcionais, técnicos, operacionais, de segurança, suporte, garantia, monitoramento e resposta a incidentes definidos neste Termo de Referência.

3.6.5. A contratação deverá preservar a autonomia tecnológica do TJPA durante a execução e no encerramento contratual, mediante exigência de documentação técnica, transferência de conhecimento, registro das configurações relevantes, exportação de logs, relatórios e evidências, rastreabilidade das ações executadas, governança de acessos e plano de transição contratual, quando aplicável.

3.7. Critérios de Habilitação

Habilitação jurídica

3.7.1. A habilitação jurídica limita-se à comprovação de existência jurídica da pessoa e, quando cabível, de autorização para o exercício da atividade a ser contratada, nos termos do art. 66 da Lei Federal n° 14.133/2021.

3.7.2. As licitantes deverão comprovar a habilitação econômico-financeira, restrita à apresentação da seguinte documentação, nos termos do art. 69 da Lei Federal n° 14.133/2021, conforme abaixo:

a) Inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ);

b) Inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicílio ou sede da Licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) Regularidade perante a Fazenda federal, estadual e/ou municipal do domicílio ou sede da Licitante, ou outra equivalente, na forma da lei;

d) Regularidade relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;

e) Prova de regularidade perante a Justiça do Trabalho; e

f) Apresentar declaração de cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal.

Habilitação técnica

3.7.3. A licitante deverá apresentar um ou mais atestados de capacidade técnica, emitidos por pessoa jurídica de direito público ou privado, que comprovem a prestação satisfatória de serviços compatíveis em características, complexidade tecnológica e criticidade operacional com o objeto da contratação.

3.7.3.1. Os atestados deverão demonstrar que a licitante prestou serviços relacionados ao fornecimento, implantação, suporte, sustentação, monitoramento ou operação de solução de segurança cibernética compatível com o objeto desta contratação.

3.7.4. Para fins de comprovação de compatibilidade técnica, serão considerados pertinentes os atestados que demonstrem experiência em uma ou mais das seguintes capacidades: proteção de endpoints, EDR, XDR, monitoramento de segurança, resposta a incidentes, gestão de exposição a riscos, inspeção de tráfego de rede, operação de SOC ou serviços gerenciados de segurança.

3.7.5. Para fins de comprovação quantitativa mínima, a licitante deverá demonstrar experiência na implementação, sustentação, suporte ou operação de ambiente com, no mínimo, 2.700 endpoints protegidos simultaneamente, correspondente a 30% do universo de 9.000 ativos abrangidos pela contratação.

3.7.6. Será admitido o somatório de atestados para comprovação do quantitativo mínimo exigido, desde que os documentos apresentados demonstrem, em conjunto, a prestação de serviços compatíveis com o objeto e evidenciem execução satisfatória no período de referência indicado no item 3.7.3.1.

3.7.7. Os atestados deverão conter, no mínimo, identificação da pessoa jurídica emitente, identificação da licitante, descrição dos serviços prestados, período de execução, quantitativo de ativos ou endpoints atendidos, escopo executado e declaração de execução satisfatória.

3.7.8. A licitante deverá declarar que possui ou possuirá, no momento da contratação e durante a execução contratual, equipe técnica qualificada para implantação, configuração, suporte, monitoramento, sustentação e resposta a incidentes relacionados à solução ofertada.

3.7.9. Quando a licitante não for fabricante ou detentora da tecnologia ofertada, deverá apresentar documento emitido pelo fabricante, distribuidor autorizado ou representante oficial, comprovando que está autorizada a comercializar, implantar e prestar suporte à solução ofertada no território nacional.

3.7.10. Declaração do fabricante acompanhada

Habilitação financeira

3.7.11. Certidão negativa de falência expedida pelo distribuidor da sede da pessoa jurídica, dentro do prazo de validade previsto na própria certidão, ou, na omissão desta, expedida há no máximo 90 (noventa) dias anteriores à data de abertura do certame;

3.7.12. Balanço patrimonial e demonstrações contábeis dos 02 (dois) últimos exercícios social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 03 (três) meses da data de apresentação da proposta;

3.7.13. A comprovação da situação financeira da empresa será constatada mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um) resultantes da aplicação das fórmulas:

LG = Ativo Circulante + realizável a longo prazo

Passivo circulante + passivo não circulante

SG = Ativo total

Passivo circulante + passivo não circulante

LC = Ativo Circulante

Passivo circulante

3.7.14. As empresas que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar capital mínimo ou patrimônio líquido de no mínimo 10% (dez por cento) do valor total estimado da contratação ou do item pertinente.

4. DA EXECUÇÃO E GESTÃO DO CONTRATO

4.1. Papéis desempenhados na contratação

4.1.1. A execução contratual será acompanhada e fiscalizada por equipe formalmente designada pelo TJPA, composta por gestor do contrato, fiscal requisitante, fiscal técnico e fiscal administrativo, sem prejuízo da indicação de suplentes e da possibilidade de substituição formal dos agentes durante a vigência contratual.

4.1.2. A equipe de gestão e fiscalização deverá acompanhar a execução do objeto, avaliar o atendimento dos requisitos técnicos, verificar o cumprimento dos prazos, níveis de serviço, obrigações contratuais, condições de pagamento, garantias e demais exigências estabelecidas neste Termo de Referência, no edital e no instrumento contratual.

	Gestor do Contrato	**Fiscal Requisitante**	**Fiscal Técnico**	**Fiscal Administrativo**
Nome	Arilson Galdino da Silva	---	Daniel Azevedo Ferreira	---
Matrícula	183318	---	116394	---
E-mail	arilson.silva@tjpa.jus.br	---	daniel.ferreira@tjpa.jus.br	---
Caso necessário, indique que funções serão absorvidas pelo Gestor do Contrato.		SIM	NÃO	SIM

SUPLENTES				
	Gestor do Contrato	**Fiscal Requisitante**	**Fiscal Técnico**	**Fiscal Administrativo**
Há Indicação?	NÃO	NÃO	NÃO	NÃO
Nome	---	---	---	---
Matrícula	---	---	---	---
E-mail	---	---	---	---

4.1.3. A contratada deverá indicar formalmente preposto responsável pela interlocução com o TJPA, coordenação da implantação, acompanhamento dos serviços gerenciados de segurança, tratamento de incidentes, atendimento de demandas técnicas e recebimento de comunicações formais.

4.2. Formas de comunicação e acompanhamento da execução do contrato

4.2.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas, as disposições deste Termo de Referência, o edital, o instrumento contratual e a Lei nº 14.133/2021.

4.2.2. As comunicações entre o TJPA e a contratada deverão ocorrer, preferencialmente, por meio do sistema institucional de gestão contratual definido pelo TJPA.

4.2.3. Na indisponibilidade do sistema institucional, as comunicações formais poderão ocorrer por e-mail, ofício, chamado eletrônico, sistema web da contratada ou outro meio formalmente aceito pela fiscalização, desde que permita rastreabilidade, identificação dos responsáveis, data, horário, conteúdo da solicitação e histórico de atendimento.

4.2.4. A contratada deverá fornecer previamente os contatos de e-mail, telefone e demais canais de atendimento de seu preposto e da equipe responsável pelo suporte técnico, monitoramento e resposta a incidentes.

4.2.5. Caso a contratada não responda à mensagem de correio eletrônico no prazo de 2 dias úteis, será considerada a ciência automática ao final desse período, sem prejuízo de eventual apuração de descumprimento contratual, quando aplicável.

4.2.6. Para incidentes críticos de segurança, os canais de comunicação deverão permanecer disponíveis em regime 24x7, contemplando abertura, registro, acompanhamento, escalonamento e encerramento de ocorrências.

4.3. Principais marcos e eventos da Execução do contrato

4.3.1. A tabela abaixo foi elaborada com os principais marcos e eventos relevantes que ocorrerão durante a execução do contrato:

Etapa	Descrição	Prazo de Conclusão	Atores Envolvidos	Comprovante de Entrega	Meio de Comprovação
1	Assinatura do contrato e/ou emissão da Nota de Empenho	Conforme fluxo administrativo	TJPA e contratada	Contrato, Nota de Empenho ou instrumento equivalente	Sistema institucional/SEI
2	Reunião inicial de alinhamento e apresentação do plano de implantação	Até 5 dias úteis após convocação do TJPA	Gestor, fiscais, preposto e equipe técnica	Ata de reunião e plano preliminar	SEI, e-mail ou sistema de gestão
3	Disponibilização das licenças, subscrições, acessos e chaves de ativação	Até 10 dias corridos após recebimento da ordem de fornecimento ou instrumento equivalente	Contratada e Fiscal Técnico	Comprovante de disponibilização	Portal do fabricante, e-mail ou relatório técnico
4	Entrega do appliance dedicado	Até 30 dias corridos após recebimento da ordem de fornecimento ou instrumento equivalente	Contratada e Fiscal Técnico	Documento de entrega e nota fiscal	Termo de entrega, nota fiscal e conferência física
5	Configuração, integração e implantação da solução	Até 15 dias corridos após disponibilização dos componentes necessários à etapa	Contratada, Fiscal Técnico e equipe técnica do TJPA	Relatório de implantação	Relatório técnico, evidências e registros de configuração
6	Ativação dos serviços gerenciados de segurança, monitoramento e resposta a incidentes	Imediatamente após a conclusão da implantação mínima necessária	Contratada, Fiscal Técnico e preposto	Termo de ativação operacional	Relatório de ativação e evidências da operação
7	Recebimento provisório	Até 4 dias úteis após entrega ou conclusão do marco correspondente	Fiscal Técnico e equipe de fiscalização	Termo de Recebimento Provisório	Lista de verificação e relatório técnico

8	Recebimento definitivo	Até 5 dias úteis após o recebimento provisório, desde que sanadas eventuais pendências	Gestor, fiscais e comissão, quando designada	Termo de Recebimento Definitivo	Lista de verificação, testes e evidências
9	Execução mensal dos serviços gerenciados	Durante a vigência contratual	Contratada e fiscalização	Relatório mensal de serviços	Relatório gerencial, chamados, eventos e indicadores
10	Ateste, liquidação e pagamento	Após recebimento definitivo ou aceite mensal dos serviços	Fiscais, gestor e unidade competente	Nota fiscal atestada	Sistema de gestão, SEI e documentos fiscais

4.4. Dinâmica de execução e requisito de segurança da informação

4.4.1. A execução terá início após a assinatura do contrato, emissão da Nota de Empenho, ordem de fornecimento, ordem de serviço ou instrumento equivalente, conforme o caso.

4.4.2. A contratada deverá apresentar plano de implantação contendo, no mínimo, cronograma, premissas, responsabilidades, etapas de instalação e configuração, plano de comunicação, riscos da implantação, estratégia de reversão, requisitos de acesso, requisitos de integração e critérios de validação técnica.

4.4.3. A implantação deverá ser conduzida de forma planejada, podendo ocorrer por fases, incluindo piloto, expansão controlada, validação técnica e operação assistida, de modo a minimizar impactos sobre os serviços críticos do TJPA.

4.4.4. A contratada deverá disponibilizar licenças, subscrições, acessos, appliance, documentação, suporte técnico, atualizações, serviços gerenciados, monitoramento e resposta a incidentes, conforme prazos e condições previstos neste Termo de Referência.

4.4.5. A solução deverá ser integrada ao ambiente tecnológico do TJPA, observadas as regras de segurança da informação, controle de acesso, segregação de perfis, confidencialidade e demais diretrizes institucionais aplicáveis.

4.4.6. A contratada deverá registrar as atividades executadas, evidências de implantação, configurações relevantes, ocorrências, incidentes, chamados, relatórios, recomendações e ações de resposta adotadas durante a execução contratual.

4.4.7. A contratada deverá emitir declaração do fabricante acompanhada de documentação técnica oficial, comprovando suporte aos padrões STIX 2.0 ou superior e TAXII 2.0 ou superior.

4.4.8. A contratada deve fornecer ficha técnica, documentação oficial do fabricante ou demonstração de relatórios de mapeamento de ameaças, que fazem uso do framework MITRE ATT&CK como base técnica de para classificação de táticas, técnicas e procedimentos (TTPs) de adversários.

4.4.9. Declaração de conformidade emitida pelo fabricante, acompanhada de relatórios de auditoria.

4.4.10. Os serviços SaaS que compõem a solução EDR/XDR deverão possuir certificação ISO/IEC 27001 vigente e relatório SOC 2 Tipo II, emitido por auditor independente. Para componentes de segurança instalados localmente, quando aplicável ao produto e à versão ofertados, será aceita adicionalmente certificação Common Criteria, conforme a série ISO/IEC 15408.

4.4.11. O appliance de inspeção de rede deverá ser fornecido com todos os cabos de alimentação necessários ao funcionamento de suas fontes principal e redundante, contendo plugues destinados à conexão à rede elétrica em conformidade com a ABNT NBR 14136, compatíveis com a tensão e a corrente nominal do equipamento, sem utilização de adaptadores.

4.5. Instrumentos formais de solicitação do objeto

4.5.1. A solicitação de fornecimento, implantação, suporte, monitoramento ou resposta a incidentes poderá ocorrer por meio dos seguintes instrumentos:

4.5.1.1. Nota de Empenho;

4.5.1.2. Ordem de Fornecimento de Bens;

4.5.1.3. Ordem de Serviço;

4.5.1.4. chamado eletrônico;

4.5.1.5. sistema web da contratada;

4.5.1.6. e-mail institucional;

4.5.1.7. telefone ou canal emergencial, para incidentes críticos;

4.5.1.8. sistema de gestão contratual definido pelo TJPA.

4.5.2. Os instrumentos formais deverão conter, quando aplicável, descrição da demanda, item solicitado, quantitativo, prazo de execução, local de entrega ou execução, responsável pelo acompanhamento, critério de aceite e demais informações necessárias à execução.

4.6. Local, Horário e Regime de Execução

4.6.1. As licenças, subscrições, acessos e créditos deverão ser disponibilizados eletronicamente, por meio de portal do fabricante, console da solução, chave de ativação, transferência eletrônica de direitos ou mecanismo equivalente.

4.6.2. O appliance dedicado deverá ser entregue em unidade indicada pelo TJPA, preferencialmente em Belém/PA, em endereço a ser informado pela fiscalização contratual.

4.6.3. A implantação, configuração, suporte e sustentação da solução deverão ocorrer preferencialmente de forma remota, sendo admitida execução presencial quando tecnicamente necessária ou quando determinada pela fiscalização.

4.6.4. As atividades presenciais deverão ocorrer, preferencialmente, em dias úteis, no horário de 8h às 16h, salvo autorização ou solicitação diversa do TJPA.

4.6.5. Os serviços gerenciados de segurança, monitoramento e resposta a incidentes deverão ser prestados em regime 24 horas por dia, 7 dias por semana, durante toda a vigência contratual.

4.6.6. As demandas ordinárias de suporte poderão observar horário comercial, sem prejuízo do atendimento contínuo de incidentes críticos de segurança, que deverá ocorrer em regime ininterrupto.

4.7. Prazo de Vigência do Contrato

4.7.1. O contrato terá vigência de 24 meses, contados da data definida no instrumento contratual.

4.7.2. A vigência contratual poderá ser prorrogada nos termos da Lei nº 14.133/2021, considerando a natureza continuada dos serviços de suporte, manutenção, monitoramento, sustentação e resposta a incidentes de segurança cibernética.

4.7.3. A vigência da ata de registro de preços, quando aplicável, observará o prazo definido na legislação e no edital.

4.8. Requisitos de Sustentabilidade na Execução

4.8.1. A contratada deverá priorizar meios eletrônicos para comunicação, envio de relatórios, documentação

técnica, evidências, abertura de chamados e acompanhamento contratual.

4.8.2. A execução deverá reduzir deslocamentos presenciais sempre que tecnicamente possível, sem prejuízo da qualidade, segurança e tempestividade da implantação e dos serviços.

4.8.3. O appliance fornecido deverá observar normas técnicas aplicáveis, eficiência energética compatível com sua categoria e requisitos de segurança elétrica.

4.8.4. Peças, componentes, equipamentos ou materiais substituídos durante a garantia deverão receber destinação ambientalmente adequada, quando aplicável, observadas as normas de logística reversa e descarte de resíduos eletroeletrônicos.

4.9. Acordo de Níveis de Serviço (ANS)

4.9.1. Os níveis de serviço deverão aferir objetivamente a qualidade da execução, o cumprimento de prazos, a tempestividade do suporte, a resposta a incidentes e a disponibilidade operacional da solução.

4.9.2. A contratada deverá apresentar relatório mensal de serviços contendo, no mínimo, chamados abertos, chamados encerrados, incidentes classificados por criticidade, tempos de resposta, tempos de contenção ou solução, eventos relevantes, recomendações técnicas, descumprimentos de níveis de serviço, glosas aplicáveis e evidências de execução.

Cumprimento do Prazo de Entrega e Implantação	
Finalidade	Medir o cumprimento dos prazos de entrega, disponibilização, implantação e ativação da solução.
Metas a cumprir	IAE menor ou igual a 0.
Instrumento de medição	Ordem de Fornecimento, Ordem de Serviço, Termo de Recebimento Provisório e Termo de Recebimento Definitivo.
Forma de acompanhamento	Comparação entre o prazo previsto e a data efetiva de entrega ou conclusão validada pela fiscalização.
Periodicidade	Por ordem ou marco concluído.
Mecanismo de Cálculo	IAE = TEX – TEST. TEX: tempo efetivo de execução. TEST: tempo estimado para execução.
Início da Vigência	A partir da emissão da ordem correspondente.
Consequência do descumprimento	Aplicação de glosa, multa ou sanção, conforme gravidade, recorrência e previsão contratual.

Criticidade	**Ocorrência Referencial**	**Tempo Máximo de Resposta**	**Tempo Máximo de Contenção, Solução ou Encaminhamento Técnico**	**Glosa por ocorrência não atendida**
Crítica	Interrupção total da solução, falha generalizada de agentes, indisponibilidade da console, incidente de segurança em andamento ou vazamento de dados em curso	30 minutos	4 horas para contenção inicial, mitigação ou restabelecimento operacional mínimo	10% da parcela mensal do serviço afetado
Alta	Indisponibilidade de componente essencial, falha em atualização crítica, degradação relevante da solução ou perda parcial de monitoramento	1 hora	8 horas	7% da parcela mensal do serviço afetado

Média	Falha localizada, erro na geração de relatórios, problema em política específica ou demanda técnica que não gere indisponibilidade crítica	4 horas	24 horas	4% da parcela mensal do serviço afetado
Baixa	Dúvida operacional, solicitação de orientação, agendamento de reunião técnica ou geração ordinária de relatório	8 horas úteis	48 horas úteis	2% da parcela mensal do serviço afetado

4.9.3. O tempo de resposta corresponderá ao intervalo entre o registro da demanda ou incidente e o primeiro atendimento técnico qualificado pela contratada.

4.9.4. O tempo de contenção, solução ou encaminhamento técnico corresponderá ao intervalo necessário para adoção de medida efetiva de mitigação, restabelecimento operacional, correção, orientação técnica ou encaminhamento formal de plano de ação, conforme a natureza da ocorrência.

4.9.5. As glosas decorrentes de descumprimento de níveis de serviço deverão incidir sobre a parcela mensal do serviço afetado, limitadas a 30% da respectiva parcela mensal, sem prejuízo da aplicação de sanções administrativas em caso de reincidência, inexecução parcial, inexecução total ou dano relevante ao TJPA.

4.9.6. Não serão considerados descumprimentos os atrasos comprovadamente decorrentes de indisponibilidade causada pelo TJPA, ausência de autorização necessária, dependência de terceiro sob responsabilidade do TJPA ou caso fortuito e força maior, desde que formalmente demonstrados pela contratada e aceitos pela fiscalização.

4.10. Qualificação Técnica dos Profissionais

4.10.1. A contratada deverá dispor de equipe técnica qualificada e em quantidade compatível com a implantação, configuração, suporte, manutenção, monitoramento, sustentação e resposta a incidentes relacionados à solução.

4.10.2. A equipe deverá possuir experiência ou qualificação compatível com, no mínimo:

4.10.2.1. implantação e administração de soluções de proteção de endpoints;

4.10.2.2. operação de plataformas EDR/XDR;

4.10.2.3. análise e resposta a incidentes de segurança;

4.10.2.4. monitoramento de eventos de segurança em ambiente SOC ou MSS;

4.10.2.5. inspeção e análise de tráfego de rede;

4.10.2.6. gestão de exposição a riscos, vulnerabilidades e configurações inseguras.

4.10.3. A contratada deverá substituir, quando solicitado pelo TJPA, profissional que demonstre incapacidade técnica, conduta inadequada, descumprimento de normas internas ou risco à segurança da informação.

4.10.4. A substituição de profissional não poderá comprometer a continuidade dos serviços, os níveis de serviço ou os prazos contratuais.

4.11. Forma de recebimento provisório/definitivo e qualidade

4.11.1. O recebimento provisório será realizado em até 10 dias úteis após a entrega, disponibilização ou conclusão do marco correspondente, mediante conferência inicial pela fiscalização técnica.

4.11.2. O recebimento definitivo será realizado em até 15 dias úteis após o recebimento provisório, condicionado à validação técnica da entrega, funcionamento, aderência aos requisitos e apresentação das evidências exigidas.

4.11.3. O recebimento definitivo das licenças, subscrições e acessos dependerá da comprovação de ativação, regularidade do licenciamento, vigência contratada, acesso à console, disponibilidade de atualizações e aderência

aos quantitativos contratados.

4.11.4. O recebimento definitivo do appliance dependerá da conferência física, validação do modelo fornecido, funcionamento básico, conectividade, capacidade compatível com os requisitos estabelecidos e garantia aplicável.

4.11.5. O recebimento definitivo da implantação dependerá da comprovação de configuração, integração, comunicação dos agentes ou componentes aplicáveis, ativação dos serviços gerenciados, entrega de documentação técnica e apresentação de evidências de funcionamento.

4.11.6. Caso sejam identificados vícios, falhas, inconsistências, pendências ou não conformidades, a contratada deverá saná-los no prazo de até 5 dias úteis, salvo prazo diverso justificado pela fiscalização em razão da complexidade técnica da correção.

4.11.7. A emissão dos termos de recebimento não afastará a responsabilidade da contratada por vícios ocultos, falhas supervenientes, inconsistências técnicas, descumprimento de garantia ou inexecução de obrigações contratuais.

4.12. Forma de Pagamento

4.12.1. O pagamento será realizado após o recebimento definitivo do objeto ou da parcela correspondente e o ateste da nota fiscal pela fiscalização competente.

4.12.2. Os itens de fornecimento de licenças, subscrições, créditos, appliance e implantação serão pagos conforme o regime definido no edital e no contrato, condicionados ao recebimento definitivo da respectiva parcela.

4.12.3. Os serviços gerenciados de segurança, suporte, monitoramento, manutenção e resposta a incidentes serão pagos mensalmente, após validação do relatório mensal de serviços, verificação do cumprimento dos níveis de serviço e aplicação das glosas eventualmente cabíveis.

4.12.4. O pagamento será realizado por ordem bancária, em conta corrente indicada pela contratada, no prazo máximo de 30 dias, contado do ateste da nota fiscal ou instrumento de cobrança equivalente.

4.12.5. A nota fiscal deverá conter, no mínimo, data de emissão, dados do contrato, período de execução, descrição do item ou serviço, valor devido, eventuais retenções tributárias e demais informações exigidas pela legislação aplicável.

4.12.6. Havendo erro na nota fiscal, pendência documental, não conformidade na execução ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até a regularização, reiniciando-se o prazo após a correção da pendência.

4.12.7. O TJPA poderá deduzir, cautelar ou definitivamente, valores correspondentes a glosas, multas, ressarcimentos ou indenizações devidas pela contratada, assegurados o contraditório e a ampla defesa quando exigidos.

4.12.8. Em caso de atraso de pagamento imputável ao TJPA, os valores devidos serão atualizados conforme regra prevista no contrato.

Da Liquidação e Pagamento

4.12.9. O pagamento será realizado somente após a realização do recebimento definitivo pela equipe de gestão e fiscalização, o qual será formalizado por meio do atesto da nota fiscal de cobrança;

4.12.10. Após o recebimento definitivo, o pagamento será realizado por meio de ordem bancária, creditada na conta corrente da EMPRESA, em no máximo 30 (trinta) dias corridos;

4.12.11. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da lei n. 14.133, de 2021;

4.12.12. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

4.12.12.1. o prazo de validade;

4.12.12.2. a data de emissão;

4.12.12.3. os dados do contrato e do órgão contratante;

4.12.12.4. o período respectivo de execução do contrato;

4.12.12.5. o valor a pagar;

4.12.12.6. eventual destaque do valor de retenções tributárias cabíveis.

4.12.13. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

4.12.14. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021;

4.12.15. A Administração deverá realizar consulta ao SICAF para:

4.12.15.1. verificar a manutenção das condições de habilitação exigidas no edital;

4.12.15.2. identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).

4.12.16. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa.

4.12.17. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

4.12.18. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos;

4.12.19. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa;

4.12.20. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

4.12.21. O TJPA realizará o pagamento no prazo de até 30 (trinta) dias, contado do recebimento definitivo do serviço objeto da ata de registro de preços ou do contrato e da apresentação do documento fiscal correspondente;

4.12.22. No caso de atraso pelo TJPA, os valores devidos ao contratado serão atualizados monetariamente entre o tempo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA de correção monetária;

4.12.23. O TJPA, observados os princípios do contraditório e da ampla defesa, poderá deduzir, cautelar ou definitivamente, do montante a pagar à Fornecedora, os valores correspondentes a multas, ressarcimentos ou indenizações devidas pela Fornecedora, nos termos pactuados;

4.12.24. No caso de atraso de pagamento, desde que a Fornecedora não tenha concorrido de alguma forma para

tanto, serão devidos pelo TJPA encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples;

4.12.25. O valor dos encargos será calculado pela fórmula: EM = I x N x VP, onde: EM = Encargos moratórios devidos; N = Números de dias entre a data prevista para o pagamento e a do efetivo pagamento; I = Índice de compensação financeira = 0,00016438; e VP = Valor da prestação em atraso.

4.12.26. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pela CONTRATADA;

4.12.27. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento;

4.12.28. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável;

4.12.29. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente;

4.12.30. A(s) EMPRESA(S) fornecedora, regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar. O pagamento ficará ainda condicionado, à consulta e constatação de que a empresa permanece como enquadra ao regime do Simples Nacional por ocasião da liquidação da despesa.

4.12.31. A CONTRATADA deverá enviar nota fiscal/fatura para o CONTRATANTE, através do sistema de gestão de contratos indicado pela CONTRATANTE.

4.12.31.1. Caso o sistema de gestão de contratos esteja indisponível, o envio deverá ser feito via endereço de e-mail protocolo.geral@tjpa.jus.br, com a especificação do número e ano do contrato, bem como a indicação da Secretaria de Informática como destinatário.

4.12.32. O envio das notas fiscais/faturas deverá ocorrer, preferencialmente, até o 5° dia subsequente ao recebimento definitivo dos serviços pelo fiscal do contrato e, impreterivelmente, até o 30º dia subsequente a esse recebimento, sob pena de abertura de processo administrativo de aplicação de penalidade.

Da Garantia Contratual

4.12.33. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual de 5% do valor inicial do contrato e condições descritas nas cláusulas do contrato.

4.12.34. Caberá à CONTRATADA optar por uma das seguintes modalidades de garantia, conforme §1º do art. 96:

4.12.34.1. Caução em dinheiro ou em títulos da dívida pública;

4.12.34.2. Seguro-garantia;

4.12.34.3. Fiança bancária;

4.12.34.4. Título de capitalização.

4.12.35. Em caso opção pelo seguro-garantia, a parte adjudicatária terá prazo de um mês, contado da data de homologação da licitação, para sua apresentação, que deve ocorrer antes da assinatura do contrato.

4.12.36. No caso do seguro-garantia, deverá conter explicitamente o prazo de validade que deverá abarcar a vigência do contrato.

4.12.37. A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 10 dias úteis após a assinatura do contrato.

4.12.38. Nas contratações de serviços e fornecimentos contínuos com vigência superior a 1 (um) ano, assim como nas subsequentes prorrogações, será utilizado o valor anual do contrato para definição e aplicação dos percentuais.

4.12.39. A garantia contratual prestada pela contratada deverá ser atualizada sempre que houver atualização do valor do contrato, havendo ou não prorrogação contratual.

4.12.40. Os riscos a serem cobertos seja por qualquer das garantias são:

4.12.40.1. prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas, e

4.12.40.2. multas moratórias e punitivas aplicadas pelo CONTRATANTE à CONTRATADA.

4.12.41. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

4.12.42. A Garantia deverá contemplar, ainda:

4.12.42.1. O risco a ser coberto seja por qualquer das modalidades de garantias; e

4.12.42.2. Prejuízos causados à Administração ou a terceiros, decorrentes de culpa ou dolo durante a execução do Contrato.

4.12.43. A garantia de responsabilidade civil obedecerá às mesmas regras elencadas no item 4.12.35 e seguintes.

4.13. Manutenção e Garantia do objeto

4.13.1. A contratada deverá assegurar o pleno funcionamento da solução durante toda a vigência contratual, abrangendo licenças, subscrições, console, agentes, módulos, appliance, serviços gerenciados, suporte técnico, atualizações, correções e demais componentes contratados.

4.13.2. As licenças e subscrições deverão contemplar direito de uso, atualizações, correções de segurança, melhorias, upgrades compatíveis com o licenciamento contratado e acesso às bases de inteligência de ameaças durante toda a vigência.

4.13.3. O appliance deverá possuir garantia mínima de 36 meses, incluindo suporte técnico, manutenção corretiva, substituição de peças e reparo ou substituição do equipamento em caso de defeito coberto pela garantia.

4.13.4. Os serviços gerenciados deverão garantir monitoramento contínuo, triagem de alertas, análise técnica, orientação, comunicação, escalonamento, contenção e apoio à resposta a incidentes de segurança.

4.13.5. A contratada deverá manter canal de atendimento para registro, acompanhamento, escalonamento e encerramento de chamados técnicos.

4.13.6. Todas as correções, atualizações, substituições, ajustes e manutenções necessárias ao funcionamento regular da solução deverão ser realizadas sem ônus adicional ao TJPA, quando decorrentes das obrigações contratadas.

4.14. Direitos de Propriedade Intelectual e direitos autorais

4.14.1. A contratação não contempla desenvolvimento de software sob encomenda, sendo baseada no fornecimento de licenças ou subscrições de software proprietário, appliance dedicado e serviços especializados associados.

4.14.2. Os direitos de propriedade intelectual da solução permanecerão com o fabricante ou detentor da tecnologia, cabendo ao TJPA o direito de uso das licenças, subscrições, módulos, funcionalidades e serviços contratados durante a vigência.

4.14.3. Os relatórios técnicos, documentos de configuração, planos de implantação, registros de incidentes, evidências, recomendações, procedimentos operacionais, inventários, trilhas de auditoria e demais artefatos produzidos no âmbito da execução contratual serão de propriedade do TJPA.

4.14.4. A contratada não poderá divulgar, compartilhar, reutilizar ou transferir informações, documentos, registros, evidências ou artefatos produzidos no âmbito da execução contratual sem autorização prévia e formal do TJPA.

4.15. Obrigações do Contratante

4.15.1. Verificação das regularidades fiscais, trabalhistas e previdenciárias para fins de pagamento;

4.15.2. Permitir o acesso às dependências do TJPA, aos técnicos do fornecedor responsáveis pela execução dos serviços de garantia quando necessários;

4.15.3. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos da fornecedora;

4.15.4. Comunicar formalmente qualquer anormalidade referente aos serviços de garantia quando necessários;

4.15.5. Responsabilizar-se pelos pagamentos dos bens fornecidos pela fornecedora;

4.15.6. Realizar a instalação dos produtos e o atendimento inicial dos chamados técnicos conforme o manual de instalação fornecido pelo fabricante.

4.15.7. Receber o objeto fornecido pela Contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas.

4.15.8. Comunicar a empresa para que emita a Nota Fiscal com o valor exato dimensionado pela fiscalização com base na Avaliação de Resultado.

4.16. Obrigações da Contratada

4.16.1. A Contratada deve cumprir todas as obrigações constantes deste Termo de Referência, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

4.16.2. Entregar o objeto conforme especificações, prazos e locais constantes neste Termo, bem como regras descritas no edital e seus anexos.

4.16.3. A Contratada deverá fornecer previamente os contatos de e-mail e telefone de seu(s) preposto(s). Estes serão os principais canais de comunicação a serem utilizados durante a execução do contrato, devendo as partes optarem pelo uso preferencial de e-mails, para geração de registros documentais.

4.16.4. Atender as solicitações feitas caso o suporte necessite ser acionado, cumprindo os termos do contrato;

4.16.5. Atender às determinações regulares emitidas pelo fiscal da contratação ou gestor do contrato;

4.16.6. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos;

4.16.7. Manter seus profissionais, quando nas dependências do CONTRATANTE, em perfeitas condições de apresentação e asseio, submetendo-os às normas internas de conduta, segurança e disciplina e à Política de Prevenção e Enfrentamento do Assédio Moral, do Assédio Sexual e da Discriminação, instituída pela Resolução CNJ 351/2020, sem que se configure, com isso, qualquer vínculo empregatício com o órgão.

4.16.8. Substituir, no prazo estabelecido pelo CONTRATANTE, qualquer um de seus empregados que for considerado inconveniente à boa ordem, demonstre incapacidade técnica, perturbe a ação da fiscalização do

CONTRATANTE, não acate as suas determinações ou não observe às normas internas do CONTRATANTE.

4.16.9. Não contratar, durante a vigência da contratação, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do Fiscal ou Gestor da contratação, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

4.16.10. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

4.16.11. Manter durante toda a vigência da contratação, em compatibilidade com as obrigações assumidas, todas as condições exigidas para qualificação, na contratação direta;

4.16.12. Cumprir, durante todo o período de execução da contratação, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação;

4.16.13. A Contratada deve cumprir todas as obrigações constantes no instrumento contratual e sua proposta, assumindo como exclusivamente seus, os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

4.16.14. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Termo de Referência, acompanhado da respectiva Nota Fiscal, na qual constarão as indicações referentes ao número da Nota de Empenho a que se refere, atentando para que a discriminação do produto e a unidade estejam de acordo com a descrição do objeto, a marca, fabricante e prazo de validade.

4.16.15. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os Arts. 12, 13 17 a 27, do Código de Defesa do Consumidor (Lei Nº 8.078, de 1990).

4.16.16. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos.

4.16.17. Além do contido na Lei Nº 14.133/21, são obrigações da Contratada responsabilizar- se pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes, bem como taxas, fretes, seguros, deslocamento de pessoal, prestação de garantia e quaisquer outras que incidam ou venham a incidir na execução do contrato.

4.16.18. Reparar e corrigir, às suas expensas, no total ou em parte, o objeto da contratação, em que se verificarem incorreções resultantes do transporte ou de meios empregados.

4.16.19. Atender prontamente às solicitações do CONTRATANTE acerca de dúvidas quanto a procedimentos de configuração ou atualização das licenças.

4.16.20. Executar o fornecimento por meio de pessoas idôneas, assumindo total responsabilidade por quaisquer danos ou faltas que eles venham a cometer no desempenho das funções, podendo o TJPA exigir a retirada daquela cuja conduta seja julgada inconveniente, obrigando-se, também, a indenizar o TJPA por todos os danos e prejuízos que eventualmente ocasionarem.

4.16.21. Entregar todos os produtos mediante a apresentação da respectiva Nota Fiscal, constando no campo “observações”, o número da NOTA DE EMPENHO a que se refere, atentando para que a discriminação do produto e a unidade estejam de acordo com o Termo de Referência.

4.16.22. Estar em situação regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF.

4.16.23. Manter sigilo, sob pena de responsabilidade, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto da contratação, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações e as regras de negócio, devendo orientar seus empregados nesse sentido.

4.17. Obrigações de Ambas as Partes

4.17.1. As definições e obrigações desta contratação seguirão a Lei 13.709/2018 (LGPD), bem como as

demais normas e leis aplicáveis à proteção de dados, especialmente as editadas pela Autoridade Nacional de Proteção de Dados Pessoais - ANPD.

4.17.2. A CONTRATANTE será considerado o titular dos dados pessoais.

4.17.3. As partes CONTRAENTES serão consideradas agentes de tratamento com os seguintes papéis:

4.17.4. TRIBUNAL DE JUSTIÇA: será a controladora dos dados pessoais.

4.17.5. CONTRATADA: será a operadora dos dados pessoais, sendo seu dever tratá-los respeitando a finalidade da contratação.

4.17.6. É proibido às partes utilizar qualquer informação pessoal fornecida em decorrência da execução do contrato para fins diferentes daqueles previstos no objeto do contrato, sujeitas à responsabilização administrativa, cível e criminal.

4.17.7. As partes comprometem-se a manter sigilo e confidencialidade de todas as informações, especialmente dados pessoais e sensíveis, fornecidos em decorrência da execução do contrato, conforme estabelecido na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), sendo vedada a transferência dessas informações a outras empresas ou pessoas, exceto em casos de obrigações legais ou para cumprir o objeto do contrato.

4.17.8. As partes serão responsáveis administrativa e judicialmente por danos materiais, morais, individuais ou coletivos, causados aos titulares dos dados pessoais fornecidos em decorrência da execução do contrato, por descumprimento da Lei Geral de Proteção de Dados.

4.17.9. Em conformidade com a Lei Geral de Proteção de Dados, o CONTRATANTE, para a execução do serviço objeto deste contrato, terá acesso aos dados pessoais dos representantes da CONTRATADA, tais como CPF, RG, endereço eletrônico, endereço residencial e cópia do documento de identificação.

4.17.10. A CONTRATADA reconhece a existência da Lei Geral de Proteção de Dados e compromete-se a ajustar todos os procedimentos internos conforme o disposto na legislação, visando proteger os dados pessoais fornecidos pelo CONTRATANTE.

4.17.11. A CONTRATADA deverá informar ao CONTRATANTE, dentro de 24 (vinte e quatro) horas, qualquer incidente de acesso não autorizado aos dados pessoais, assim como situações acidentais ou ilícitas de destruição, perda, alteração, divulgação ou qualquer forma de tratamento inadequado ou ilegal, adotando as medidas previstas no artigo 48 da Lei Geral de Proteção de Dados.

4.18. Estimativa de preços

4.18.1. A presente contratação tem por estimativa o valor total R$ 16.950.247,73.

4.19. Adequação orçamentária

Ação orçamentária	8180, 8181, 8182
Fonte de recursos	0118
Elemento de despesa	3.3.90.40
Exercício financeiro	2026, 2027, 2028

4.20. Reajustamento

4.20.1. Em casos de prorrogação do contrato, os preços inicialmente registrados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em *(informar a data da validação da pesquisa de preços)*.

4.20.2. Após o interregno de um ano, e independente de pedido do contratado, os preços dos itens serão reajustados com base no Índice Nacional de Preços ao Consumidor Amplo –IPCA, do saldo renovado quando da prorrogação do Contrato.

4.20.3. O TJPA deverá negociar com a Contratada a possibilidade de não aplicar o reajuste ou aplicá-lo a menor.

Devendo haver manifestação expressa da Contratada acerca da aceitação dos termos da negociação.

4.20.4. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

4.20.5. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o TJPA pagará ao contratado a importância calculada pela última variação conhecida.

4.20.6. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

4.20.7. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

4.20.8. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

4.20.9. O reajuste será realizado por apostilamento.

4.21. Sanções Administrativas

4.21.1. Para definições e aplicações dos subitens tratados neste tópico, o normativo balizador é a Instrução Normativa Nº 003/2024-GP, que regulamenta, no âmbito do TJPA, o processo administrativo sancionatório e a dosimetria na aplicação de penalidades definidas no art. 156 da Lei Federal Nº 14.133/2021.

4.21.2. O licitante ou o contratado será responsabilizado administrativamente pelas seguintes infrações (art. 6º da IN Nº 003/2024-GP):

4.21.2.1. dar causa à inexecução parcial do contrato;

4.21.2.2. dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

4.21.2.3. dar causa à inexecução total do contrato;

4.21.2.4. deixar de entregar a documentação exigida na etapa de seleção do fornecedor ou execução do contrato, mesmo após realização de diligências;

4.21.2.5. não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

4.21.2.6. não celebrar o contrato ou assinar a ata de registro de preços ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

4.21.2.7. ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

4.21.2.8. apresentar declaração ou documentação falsa exigida no certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

4.21.2.9. fraudar a licitação ou praticar ato fraudulento na execução do contrato;

4.21.2.10. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

4.21.2.11. praticar atos ilícitos com vistas a frustrar os objetivos da licitação; e

4.21.2.12. praticar ato lesivo previsto no art. 5º da Lei Nº 12.846/2013.

4.21.3. Aos licitantes ou às empresas que praticarem infrações administrativas previstas no parágrafo anterior deste Termo de Referência, ficarão sujeitos às seguintes sanções administrativas:

4.21.3.1. advertência;

4.21.3.2. multa: moratória e/ou compensatória;

4.21.3.3. impedimento de licitar e contratar com o Estado do Pará pelo prazo máximo de 3 (três) anos;

4.21.3.4. declaração de inidoneidade para licitar ou contratar com a Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.

4.21.4. Na aplicação das sanções serão considerados:

4.21.4.1. a natureza e a gravidade da infração cometida, entendendo-se como qual o fato gerador a ser imputado à hipótese normativa - leve, média, grave ou gravíssima;

4.21.4.2. as peculiaridades do caso concreto, nos termos do art. 5° da Lei 14.133, de 2021, e do art. 22 da LINDB;

4.21.4.3. as circunstâncias agravantes ou atenuantes;

4.21.4.4. os danos que da infração provierem para a Administração Pública; e

4.21.4.5. a implantação ou o aperfeiçoamento de programa de integridade.

4.21.5. Com fundamento no Capítulo II da IN nº 003/2024-GP, a Empresa:

4.21.6. Será sancionada com advertência nas hipóteses de descumprimento das obrigações contratuais que não cause grave dano à Administração, ao funcionamento dos serviços públicos e ao interesse coletivo e que não justifique a imposição de penalidade mais grave.

4.21.7. A sanção de advertência somente será aplicada durante a vigência do contrato.

4.21.8. Ficará impedida de licitar e contratar no âmbito do Estado do Pará pelo prazo de até 3 (três) anos, sem prejuízo da rescisão unilateral do contrato ou instrumento correspondente, quando praticar as seguintes infrações e não se justificar a imposição de penalidade mais grave:

4.21.8.1. dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo (de três meses a dois anos);

4.21.8.2. dar causa à inexecução total do Contrato (de seis meses a três anos);

4.21.8.3. deixar de entregar a documentação exigida na etapa de seleção do fornecedor ou execução do Contrato mesmo após realização de diligências (de dois meses a seis meses);

4.21.8.4. não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado (de dois meses a um ano);

4.21.8.5. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta (de seis meses a um ano);

4.21.8.6. ensejar o retardamento da execução ou da entrega do objeto do contrato sem motivo justificado (de três meses a um ano).

4.21.9. Será declarada inidônea para licitar e contratar quaisquer órgãos do Poder Público, em qualquer nível federativo, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, quando praticar as seguintes infrações, nos termos dos artigos 25 e 26, da IN nº 003/2024-GP:

4.21.9.1. aquelas previstas para a sanção de impedimento de licitar e contratar com a Estado do Pará, que implicarem danos financeiros significativos para o TJPA, impactos severos na eficiência do contrato ou nas rotinas administrativas;

4.21.9.2. apresentar declaração ou documentação falsa exigida no certame ou de prestar declaração falsa durante a licitação ou a execução do contrato;

4.21.9.3. fraudar a licitação ou de praticar ato fraudulento na execução do contrato;

4.21.9.4. comportar-se de modo inidôneo ou de cometer fraude de qualquer natureza

4.21.9.5. praticar atos ilícitos com vistas a frustrar os objetivos da licitação; e

4.21.9.6. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 2013.

4.21.10. A multa poderá ser aplicada cumulativamente com as demais sanções, por qualquer das infrações previstas no art. 155 da Lei n. 14.133/2021, e não poderá ser inferior a 0,5% (cinco décimos por cento) ou superior a 30% (trinta por cento) do valor total do empenho. total do empenho.

4.21.11. A multa compensatória será aplicada para o caso de inexecução parcial ou total do contrato nos seguintes percentuais e condições:

4.21.11.1. De 20% (vinte por cento) do valor da parcela do objeto não entregue, no caso de inexecução parcial do contrato;

4.21.11.1.1. A inexecução parcial do contrato restará configurado, entre outras hipóteses, quando a EMPRESA atrasar em prazo superior a 30 (trinta) dias a entrega do objeto e está, apesar de realizada, não ocorreu em sua totalidade.

4.21.11.2. De 30% (trinta por cento) do valor total do empenho, no caso de inexecução total do contrato.

4.21.11.2.1. A inexecução total do contrato restará configurada, entre outras hipóteses, quando a EMPRESA atrasar a entrega do objeto em prazo superior a 30 (trinta) dias e a sua totalidade não for entregue.

4.21.12. A multa de mora será aplicada quando a CONTRATADA ensejar o retardamento da execução ou da entrega do objeto, sem motivo justificado e aceito pela TJPA, entre outras hipóteses, em 0,5% (cinco décimos por cento) do valor unitário do produto, por dia e produto em atraso.

4.21.13. Além das multas compensatórias por inexecução parcial ou total do contrato e das multas de mora estabelecidas, serão aplicadas multas por descumprimento de obrigação contratual, entre outras hipóteses, no percentual de 1% (um por cento) a 10% (dez por cento) do valor do empenho, quando a EMPRESA entregar o objeto com especificações incompatíveis com as exigidas do contrato ou no edital e anexos da licitação que deu origem à adjudicação.

4.21.14. Fica dispensada, a critério da autoridade competente da unidade demandante, a formalização de solicitação de instauração de processo administrativo de apuração de responsabilidade, quando a soma dos valores atribuídos à empresa for considerada irrisória (art. 20, parágrafo único, incisos I e II, da IN Nº 003/2024-GP).

5. DO SISTEMA DE REGISTRO DE PREÇOS

5.1. Hipótese para a utilização do Sistema de Registro de Preços	
Dadas as características do bem ou serviço, há a necessidade de contratações permanentes ou frequentes.	☐
Por ser mais conveniente a aquisição de bens com previsão de entregas parceladas.	☒
Por ser mais conveniente a contratação de serviços remunerados por unidade de medida ou em regime de tarefa.	☒
Por ser mais conveniente a aquisição de bens ou a contratação de serviços para o atendimento a mais de uma unidade, órgão ou entidade.	☐
Devido à natureza do objeto, não é possível definir previamente o quantitativo a ser demandado pelo TJPA.	☐
5.2. Justificativa técnica para a adoção do Sistema de Registro de Preço	

A adoção do Sistema de Registro de Preços é tecnicamente adequada à presente contratação, considerando que a solução pretendida é composta por licenças, subscrições, appliance, créditos de plataforma, serviços gerenciados de segurança, suporte, monitoramento e resposta a incidentes, com possibilidade de consumo conforme a necessidade institucional durante a vigência da ata.

A contratação envolve solução de segurança cibernética destinada à proteção de ativos de TIC, gestão de exposição a riscos, detecção e resposta estendida, análise de tráfego de rede e operação de serviços especializados de monitoramento, cujo dimensionamento pode ser afetado pela evolução do parque tecnológico, pela ampliação da superfície de ataque, pela criticidade dos ativos protegidos e pelas demandas operacionais da SETIC.

O SRP permite ao TJPA preservar disponibilidade de contratação, registrar preços para os componentes necessários, planejar o consumo de forma controlada e realizar contratações conforme a efetiva demanda, sem impor aquisição imediata de todos os quantitativos registrados.

O uso do SRP também contribui para a eficiência da gestão pública, ao permitir planejamento de médio prazo, padronização da solução, preservação da economicidade, racionalização da instrução processual e maior previsibilidade na continuidade da proteção cibernética institucional.

A solução deverá ser registrada em lote único, em razão da interdependência funcional e operacional dos componentes tecnológicos e dos serviços especializados, preservando a integração, a responsabilidade técnica única e a coerência da arquitetura de segurança cibernética definida no ETP e neste Termo de Referência.

5.3. Da necessidade de formalização de contrato

A formalização de contrato justifica-se pela natureza crítica e continuada do objeto, que envolve licenciamento ou subscrição de software, fornecimento de appliance, serviços gerenciados de segurança, suporte técnico, manutenção, monitoramento contínuo, resposta a incidentes, garantia, níveis de serviço, obrigações de segurança da informação, proteção de dados e confidencialidade.

O contrato decorrente da Ata de Registro de Preços deverá estabelecer, no mínimo, o quantitativo contratado, os itens abrangidos, o prazo de vigência, as condições de execução, os marcos de entrega, os níveis de serviço, a forma de pagamento, as obrigações das partes, as regras de garantia, as sanções aplicáveis e demais condições necessárias à adequada execução e fiscalização.

A emissão de Nota de Empenho, Ordem de Fornecimento ou Ordem de Serviço poderá ser utilizada como instrumento operacional de solicitação, sem afastar a necessidade de contrato formal quando a contratação envolver serviços continuados, obrigações de segurança da informação, suporte, monitoramento ou resposta a incidentes.

5.4. Órgãos participantes à Ata de Registro de Preços

O TJPA atuará como órgão gerenciador da Ata de Registro de Preços.

A Ata de Registro de Preços será destinada ao atendimento das necessidades do Tribunal de Justiça do Estado do Pará, por intermédio da Secretaria de Tecnologia da Informação e Comunicação, conforme quantitativos estimados neste Termo de Referência. Portanto, não haverá órgãos participantes na fase de formação da Ata de Registro de Preços.

5.5. Intenção de Registro de Preço – IRP

A abertura de intenção de registro de preços mostra-se necessária como medida voltada à observância dos princípios da economicidade, eficiência e planejamento, bem como da ampliação da competitividade nas contratações públicas, conforme previsto na Administração Pública e disciplinado pela Lei n° 14.133/2021, sendo um procedimento estratégico fundamental para a eficácia das aquisições públicas.

A utilização do instrumento de IRP viabiliza a identificação de órgãos que apresentem demandas afins, fomentando a execução de compras compartilhadas e proporcionando ganho de escala, com expressiva redução de gastos operacionais e o alcance de propostas mais benéficas para o erário. Ademais, essa medida colabora para a otimização dos procedimentos licitatórios, impedindo a ocorrência de certames repetitivos para produtos ou serviços correspondentes.

Portanto, para o certame em tela, legitima-se a adoção do procedimento de IRP para suprir as necessidades presentes e vindouras desta Secretaria de Tecnologia da Informação e Comunicação, visto que a interrupção das soluções e atividades causaria danos reais às rotinas institucionais e tecnológicas, o que afetaria severamente a produtividade da gestão.

Outrossim, o início da IRP expande a concorrência na disputa, dado que a elevação do volume total previsto costuma despertar o interesse de mais empresas concorrentes, impulsionando a captação de ofertas financeiramente mais atraentes e alinhadas aos preços praticados pelo mercado.

Por todo o exposto, haja vista o ingresso de novas instituições no processo de compra, a prerrogativa de economia de escala, a simplificação das rotinas de trabalho e, sobretudo, a perseguição pelo melhor custo-benefício para o setor público, encontra-se devidamente respaldada a exigência de abertura de Intenção de Registro de Preços – IRP.

5.6. Adesão de órgãos não participantes à Ata de Registro de Preços

5.6.1. Será admitida a adesão de órgãos ou entidades não participantes à Ata de Registro de Preços, desde que observadas as condições previstas na legislação, nos normativos internos do TJPA, no edital, na Ata de Registro de Preços e neste Termo de Referência.

5.6.2. A adesão por órgão ou entidade não participante dependerá de solicitação formal dirigida ao TJPA, acompanhada de justificativa da vantajosidade, demonstração da compatibilidade dos preços registrados com os praticados no mercado, indicação dos itens e quantitativos pretendidos, aceite prévio do fornecedor e autorização do órgão gerenciador.

5.6.3. A autorização para adesão deverá observar a preservação das obrigações assumidas com o TJPA, a inexistência de prejuízo à execução das contratações próprias do Tribunal, a capacidade de atendimento do fornecedor, a compatibilidade técnica do objeto pretendido e os limites quantitativos estabelecidos na legislação e nos normativos aplicáveis.

5.6.4. O fornecedor beneficiário da Ata de Registro de Preços poderá aceitar ou recusar o fornecimento decorrente de adesão, desde que não haja prejuízo às obrigações presentes e futuras assumidas com o TJPA.

5.6.5. O órgão ou entidade não participante será responsável pelos atos relativos à contratação decorrente da adesão, incluindo emissão de instrumento contratual próprio, gestão, fiscalização, recebimento, pagamento, apuração de descumprimentos, aplicação de sanções e demais providências relacionadas à execução de sua demanda.

5.6.6. O TJPA, na condição de órgão gerenciador, limitar-se-á à análise e autorização do pedido de adesão, observados os requisitos legais e normativos, não lhe competindo a gestão, fiscalização ou administração dos contratos firmados por órgãos ou entidades não participantes.

5.6.7. As adesões não poderão comprometer a padronização, a economicidade, a segurança da informação, a continuidade operacional, a disponibilidade dos quantitativos registrados para o TJPA ou a execução dos serviços contratados pelo Tribunal.

5.6.8. A autorização de adesão poderá ser negada quando houver risco de prejuízo ao atendimento da demanda do TJPA, incompatibilidade técnica, insuficiência de quantitativos, restrição operacional, risco à segurança da informação, ausência de vantajosidade demonstrada ou descumprimento dos requisitos legais e normativos aplicáveis.

5.7. Possibilidade de prever preços diferentes

Não se aplica para o objeto a ser contratado.	☒
Em razão da execução do objeto ser realizada ou os bens entregues em locais diferentes.	☐
Em razão da forma e do local de acondicionamento dos bens a serem contratados.	☐
Quando for admitida a cotação variável em razão do tamanho do lote.	☐
Por outro motivo a ser demonstrado.	☐

Justificativa técnica ou detalhamento da necessidade

A contratação será estruturada em lote único, com adjudicação global, em razão da necessidade de preservar a integração técnica e operacional da solução, a padronização tecnológica, a responsabilidade contratual única, a rastreabilidade das ações executadas e a continuidade dos serviços de segurança cibernética.

O registro de mais de um fornecedor poderia gerar incompatibilidade entre componentes, fragmentação de responsabilidades, divergência de versões, inconsistência de suporte, dificuldade de correlação de eventos e risco de lacunas na resposta a incidentes.

A vedação ao registro de mais de um fornecedor para o lote único não restringe a competição no certame, pois será admitida a participação de licitantes aptos a fornecer integralmente a solução, inclusive fabricantes, distribuidores, revendedores, integradores ou parceiros autorizados, conforme as condições de habilitação e aceitação previstas no edital e neste Termo de Referência.

Belém, 16 de junho de 2026.

Integrante Demandante	**Integrante Técnico**	**Integrante Administrativo**

ANEXO I

ESPECIFICAÇÕES TÉCNICAS DO OBJETO

OBJETO

Contratação envolve a Contratação de solução avançada de segurança, contemplando proteção de endpoints, gestão de exposição a riscos, detecção e resposta estendida (XDR), inspeção de tráfego de rede, fornecimento de appliance dedicado e serviços gerenciados de segurança (MSS), incluindo suporte, monitoramento contínuo e resposta a incidentes.

Item	Produto/serviço	Métrica
1	TrendAi Endpoint Security Essentials	Licença
2	TrendAi Endpoint Security Pro	Licença
3	TrendAi Cyber Risk Exposure Management Core	Licença
4	TrendAi Deep Discovery Inspector Series 9000 - 10Gb software only com XDR	Licença
5	TrendAi Deep Discovery 9000 Hardware	Equipamento
6	Créditos Trend AI Flex Vision One	Créditos
7	Serviços gerenciados de segurança para suporte e monitoramento, contendo ações corretivas, preventivas e de resposta a incidentes	Mês

1. TREND AI ENDPOINT SECURITY ESSENTIALS/PRO

1.1. Características Gerais

1.1.1. A solução deverá contemplar, de forma integrada, os itens de **licenciamento de proteção de endpoints (camada essencial – EPP/NGAV e camada avançada – EDR/XDR)** e **serviços gerenciados de segurança para suporte e monitoramento contínuo**;

1.1.2. A solução deverá ser disponibilizada no modelo SaaS (Software as a Service), com console de gerenciamento em nuvem, mantida e atualizada pelo fabricante;

1.1.3. Deverá possuir console centralizada unificada, permitindo visibilidade, correlação e resposta a incidentes em endpoints;

1.1.4. Deverá suportar Single Sign-On (SSO) e integração com diretórios corporativos (ex.: Active Directory, Azure AD ou equivalente);

1.1.5. Deverá prover arquitetura baseada em múltiplas camadas de proteção, incluindo prevenção, detecção, investigação e resposta automatizada a incidentes;

1.1.6. A solução deverá estar aderente ao conceito de XDR (Extended Detection and Response), permitindo correlação de eventos e telemetria de endpoints, podendo ser expandida para outras camadas (rede, e-mail, identidade);

1.1.7. Deverá permitir operação assistida por serviços gerenciados (MDR – Managed Detection and Response), com atuação proativa e reativa sobre incidentes de segurança.

1.2. Camada Essencial – Proteção de Endpoints (EPP/NGAV)

1.2.1. A solução deverá prover proteção de endpoints baseada em NGAV (Next-Generation Antivirus), com uso de assinaturas, heurística e inteligência artificial;

1.2.2. Deve detectar e bloquear malware conhecido e desconhecido, incluindo vírus, worms, ransomware, spyware, rootkits e ameaças fileless;

1.2.3. Deve possuir proteção em tempo real para arquivos, processos, memória e atividades do sistema;

1.2.4. Deve incluir proteção contra ransomware com capacidade de bloqueio comportamental e rollback de arquivos quando aplicável;

1.2.5. Deve possuir machine learning pré-execução e em runtime para detecção de ameaças avançadas;

1.2.6. Deve prover proteção de navegação com análise de reputação de URLs sem necessidade de plugins adicionais;

1.2.7. Deve permitir políticas de segurança centralizadas com controle de:

1.2.7.1. varredura (tempo real, agendada e sob demanda);

1.2.7.2. exclusões;

1.2.7.3. ações automáticas (quarentena, limpeza, bloqueio).

1.2.8. Deve suportar, no mínimo, os sistemas operacionais:

1.2.8.1. Windows 10 e superiores;

1.2.8.2. Windows Server (versões suportadas pelo fabricante);

1.2.8.3. macOS (versões suportadas);

1.2.8.4. Linux (distribuições suportadas).

1.2.9. Deve permitir atualização automática de assinaturas, engines e componentes de proteção;

1.2.10. Deve possuir mecanismos de autoproteção contra desativação ou manipulação indevida do agente;

1.2.11. Deve permitir integração com inteligência de ameaças global do fabricante.

1.3. Camada Avançada – Detecção e Resposta (EDR/XDR)

1.3.1. A solução deverá possuir módulo EDR/XDR nativo do fabricante, integrado à console central;

1.3.2. Deve coletar e correlacionar telemetria detalhada dos endpoints, incluindo processos, arquivos, conexões de rede e atividades de usuários;

1.3.3. Deve utilizar inteligência artificial, análise comportamental e threat intelligence para detecção de ataques avançados;

1.3.4. Deve mapear eventos e ataques com base no framework MITRE ATT&CK®, identificando táticas e técnicas utilizadas;

1.3.5. Deve permitir investigação avançada de incidentes, com:

1.3.5.1. análise de causa raiz;

1.3.5.2. linha do tempo (timeline) dos eventos;

1.3.5.3. correlação automática de alertas.

1.3.6. Deve permitir execução de ações de resposta remota, incluindo:

1.3.6.1. isolamento de endpoint da rede;

1.3.6.2. finalização de processos maliciosos;

1.3.6.3. bloqueio de hashes, IPs, URLs e domínios;

1.3.6.4. coleta remota de arquivos para análise.

1.3.7. Deve disponibilizar busca avançada (Threat Hunting) com linguagem de consulta estruturada;

1.3.8. Deve permitir integração com APIs e soluções externas (ex.: SIEM, SOAR);

1.3.9. Deve armazenar logs e eventos por período mínimo de 30 dias, ou superior conforme licenciamento;

1.3.10. Deve apresentar dashboards executivos e operacionais com priorização de incidentes por criticidade.

1.4. Serviços Gerenciados de Segurança (MDR)

1.4.1. A solução deverá incluir serviços gerenciados de segurança, com monitoramento contínuo dos eventos gerados pelos endpoints;

1.4.2. O serviço deverá operar em regime 24x7 para eventos críticos, com equipe especializada do fornecedor;

1.4.3. Deve contemplar atividades de:

1.4.3.1. monitoramento contínuo de alertas;

1.4.3.2. triagem e classificação de incidentes;

1.4.3.3. investigação inicial;

1.4.3.4. recomendação de ações corretivas;

1.4.3.5. resposta assistida ou automatizada.

1.4.4. Deve prover caça a ameaças (Threat Hunting) de forma proativa;

1.4.5. Deve realizar ajustes contínuos de políticas de segurança, visando melhoria da postura de segurança;

1.4.6. Deve emitir relatórios periódicos contendo:

1.4.6.1. incidentes detectados;

1.4.6.2. ações executadas;

1.4.6.3. indicadores de segurança;

1.4.6.4. recomendações de melhoria.

1.4.7. Deve disponibilizar canal de comunicação para interação com a equipe do TJPA;

1.4.8. Deve atuar como interface com o fabricante para resolução de incidentes complexos.

1.5. Funcionalidades de Administração e Governança

1.5.1. A solução deverá permitir gerenciamento centralizado de políticas e dispositivos;

1.5.2. Deve permitir criação de múltiplos perfis de usuários com diferentes níveis de acesso;

1.5.3. Deve registrar logs de auditoria de todas as ações administrativas;

1.5.4. Deve permitir exportação de relatórios em formatos como PDF e CSV;

1.5.5. Deve possuir dashboards com visualização de:

1.5.5.1. ameaças detectadas;

1.5.5.2. status dos endpoints;

1.5.5.3. nível de risco do ambiente.

1.5.6. Deve permitir integração com ferramentas corporativas via API REST;

1.5.7. Deve garantir comunicação segura entre agentes e console por meio de criptografia.

1.6. Requisitos Gerais Complementares

1.6.1. A solução deverá ser do mesmo fabricante para todos os módulos (EPP/NGAV, EDR/XDR e console), garantindo integração nativa;

1.6.2. Não serão aceitas soluções compostas por múltiplos fabricantes sem integração nativa;

1.6.3. O licenciamento deverá contemplar todos os recursos necessários ao pleno funcionamento da solução, sem custos adicionais ocultos;

1.6.4. A solução deverá estar em conformidade com boas práticas de segurança da informação e frameworks reconhecidos de mercado;

1.6.5. Deverá permitir escalabilidade conforme crescimento do ambiente do TJPA.

2. TREND AI CYBER RISK EXPOSURE MANAGEMENT CORE

2.1. Características Gerais da Solução

2.1.1. A solução deverá permitir a gestão centralizada da superfície de ataque, consolidando a visibilidade de ativos, vulnerabilidades e configurações incorretas em uma única plataforma SaaS;

2.1.2. Deverá operar de forma contínua para identificar e avaliar a exposição a riscos, independentemente da presença de agentes em todos os ativos (suportando varreduras externas e integração via API);

2.1.3. A solução deverá fornecer um Índice de Risco Cibernético dinâmico e quantificável, permitindo a comparação da postura de segurança ao longo do tempo;

2.1.4. Deve ser dimensionada para suportar a quantidade de créditos necessária para cobrir o inventário de ativos do órgão (Endpoints, Identidades, Ativos de Nuvem e Internet);

2.1.5. A solução deverá possuir console de gerenciamento unificada com suporte a Single Sign-On (SSO) e autenticação multifator (MFA).

2.2. Gestão da Superfície de Ataque Externa (EASM) e Interna

2.2.1. A solução deve realizar a descoberta automática de ativos expostos na internet, incluindo domínios, subdomínios, endereços IP, certificados SSL e portas abertas;

2.2.2. Deve identificar "Shadow IT", detectando ativos e aplicações não mapeados oficialmente pela equipe de TI;

2.2.3. A solução deve monitorar vulnerabilidades em ativos externos e priorizá-las com base na probabilidade de exploração por agentes de ameaça;

2.2.4. Deve permitir a integração com provedores de nuvem (AWS, Azure, GCP) para identificar configurações incorretas (misconfigurations) em buckets de armazenamento, workloads e instâncias.

2.3. Avaliação e Priorização de Riscos (Risk Insights)

2.3.1. A solução deverá correlacionar dados de vulnerabilidades (CVE), severidade (CVSS) e inteligência de ameaças em tempo real;

2.3.2. Priorização Inteligente: Deve classificar os riscos não apenas pela severidade técnica, mas pela criticidade do ativo e pela evidência de exploração ativa no mundo real;

2.3.3. Deverá monitorar o risco de Identidades, identificando contas com privilégios excessivos, falta de MFA ou comportamento anômalo;

2.3.4. A solução deve fornecer recomendações de remediação claras, indicando as ações que mais impactarão positivamente na redução do índice de risco global.

2.4. Funcionalidades de Integração e Resposta (XDR Core)

2.4.1. A solução deve integrar-se nativamente com módulos de detecção e resposta (XDR) para correlacionar eventos de ataque com superfícies expostas;

2.4.2. Deve permitir a busca avançada (Threat Hunting) em todo o inventário de ativos para identificar indicadores de comprometimento (IoCs);

2.4.3. A solução deverá permitir a exportação de dados e alertas via API REST e integração com sistemas de

tickets (ITSM) ou SIEM via Syslog/Webhooks;

2.4.4. Deverá possuir mapas de topologia de ataque, demonstrando os possíveis caminhos que um atacante percorreria para atingir um ativo crítico.

2.5. Relatórios, Dashboards e Conformidade

2.5.1. A solução deverá fornecer dashboards executivos com métricas de MTTR *(Mean Time to Remediation)* e evolução do índice de risco;

2.5.2. Deve permitir a criação de relatórios customizados para diferentes níveis (Operacional, Gerencial e Executivo) nos formatos PDF e CSV;

2.5.3. Deve possuir módulos de avaliação de conformidade baseados em frameworks internacionais (como NIST, CIS Benchmarks ou ISO 27001) e suporte à LGPD;

2.5.4. A solução deve permitir a comparação da postura de risco do órgão com a média de mercado do mesmo segmento (Benchmarking).

2.6. Modelo de Licenciamento Flexível (AI Flex)

2.6.1. O licenciamento deverá ser baseado em unidades de créditos flexíveis, permitindo ao administrador alocar recursos conforme a mudança do ambiente tecnológico (ex: converter créditos de endpoints para ativos de nuvem);

2.6.2. A plataforma deverá fornecer visibilidade clara sobre o consumo de créditos por tipo de ativo em tempo real;

2.6.3. A contratante poderá optar por redirecionar créditos entre diferentes vetores (Email, Endpoint, Network ou Cloud) dentro da plataforma Vision One sem a necessidade de novos processos de aquisição.

3. TREND AI DEEP DISCOVERY INSPECTOR SERIES 9000 - 10GB SOFTWARE ONLY COM XDR

3.1. Características Gerais e Implementação

3.1.1. A solução deverá ser fornecida em formato de software (Virtual Appliance) ou licenciamento de capacidade, capaz de inspecionar o tráfego de rede de forma profunda e independente de agentes instalados nos ativos;

3.1.2. Deve ser dimensionada para suportar um throughput de inspeção de, no mínimo, 10 Gbps;

3.1.3. A solução deve permitir a implementação em modo inline (com capacidade de bloqueio) ou em modo de monitoramento passivo via porta espelhada (SPAN/Mirror) ou Network TAP;

3.1.4. Quando operando em modo inline, deverá possuir suporte a mecanismos de fail-open (by-pass) para garantir a continuidade do tráfego em caso de falha do software ou do host;

3.1.5. Deve possuir a capacidade de realizar a inspeção e decodificação de tráfego criptografado TLS/SSL, permitindo a visibilidade de ameaças ocultas em túneis seguros.

3.2. Módulos de Detecção e Análise Avançada

3.2.1. A solução deverá integrar, em um único ecossistema, módulos de:

3.2.1.1. Monitoramento;

3.2.1.2. Identificação;

3.2.1.3. Análise e Resposta de Incidentes, com foco específico em Ameaças Avançadas (APT);

3.2.1.4. Ataques direcionados.

3.2.2. Deve possuir motor de análise de comportamento de tráfego até o Nível 7 (Camada de Aplicação) do modelo OSI;

3.2.3. Deve ser capaz de detectar movimentos laterais, ataques de força bruta, varreduras de rede (scans) e

exfiltração de dados;

3.2.4. A solução deverá identificar comunicações com servidores de Comando e Controle (C&C), utilizando bases de reputação global atualizadas em tempo real;

3.2.5. Deve possuir suporte para análise de mais de 100 protocolos e aplicações, incluindo, mas não se limitando a: SMB, HTTP/HTTPS, DNS, FTP, SMTP, IMAP4, protocolos de banco de dados (SQL) e protocolos industriais (OT).

3.3. Analisador Virtual (Sandbox) e Tratamento de Artefatos

3.3.1. A solução deve incluir um Analisador Virtual de Ameaças (Sandbox) integrado, capaz de executar arquivos suspeitos em ambientes isolados e seguros;

3.3.2. O ambiente de sandbox deve suportar múltiplos sistemas operacionais, incluindo

3.3.2.1. Windows (7, 10, 11);

3.3.2.2. Windows Server (2012 a 2022);

3.3.2.3. Android;

3.3.2.4. Distribuições Linux (CentOS/RHEL).

3.3.3. Deve possuir tecnologia para detecção de técnicas de evasão de sandbox e capacidade de derivação de arquivos protegidos por senha através de um vocabulário de conhecimento (brute-force de senhas comuns);

3.3.4. Deve permitir a extração e o download de amostras de arquivos suspeitos e dos respectivos arquivos de captura de pacotes (PCAP) para análise forense detalhada.

3.4. Integração com Plataforma XDR (Extended Detection and Response)

3.4.1. A solução deve estar nativamente integrada à plataforma de investigação e resposta centralizada, enviando metadados e objetos suspeitos para correlação multi-camada;

3.4.2. Flexibilidade de Licenciamento: A solução deve permitir que o licenciamento seja dinamicamente alocado ou redirecionado para outros vetores da plataforma (como Endpoint, Email ou Server) conforme a necessidade da CONTRATANTE, sem alteração contratual;

3.4.3. Deve permitir a visualização do ataque em uma linha do tempo gráfica, correlacionando eventos de rede com eventos detectados em estações de trabalho e servidores;

3.4.4. A integração deve permitir a resposta automatizada, como o isolamento de um host na rede ou o bloqueio de um IP malicioso, diretamente a partir da console XDR.

3.5. Gerenciamento, Visibilidade e Relatórios

3.5.1. A console de gerenciamento deverá ser baseada em interface Web, com Dashboards customizáveis que exibam o índice de risco, top hosts afetados e estatísticas de tráfego em tempo real;

3.5.2. Deverá possuir mapa geográfico de ameaças, identificando a origem e o destino das comunicações maliciosas;

3.5.3. Deve permitir a criação de alertas personalizados e o encaminhamento de logs via protocolo Syslog (formato CEF/LEEF) para integração com ferramentas de SIEM/SOAR;

3.5.4. Os relatórios devem ser gerados nos formatos PDF e CSV, contemplando visões executivas (índices de risco) e técnicas (detalhes de IOCs - Indicadores de Comprometimento).

4. TREND AI DEEP DISCOVERY 9000 HARDWARE

4.1. Características Gerais do Hardware e Performance

4.1.1. O equipamento deverá ser uma unidade física dedicada (Appliance), projetada para instalação em rack

padrão 19 polegadas;

4.1.2. A solução deverá suportar uma taxa de transferência (throughput) de inspeção de tráfego de, no mínimo, 10 Gbps em ambiente real;

4.1.3. O hardware deverá possuir fontes de alimentação redundantes e hot-swappable para garantir alta disponibilidade;

4.1.4. Deverá possuir interfaces de rede de alta velocidade, incluindo suporte a interfaces SFP+ (10GbE) para monitoramento de tráfego via portas Mirror/SPAN ou Network TAP.

4.2. Detecção de Ameaças e Análise de Tráfego

4.2.1. A solução deve realizar a inspeção de tráfego de rede em todas as portas e protocolos, incluindo, mas não se limitando a:

4.2.1.1. HTTP;

4.2.1.2. HTTPS;

4.2.1.3. SMTP;

4.2.1.4. POP3;

4.2.1.5. IMAP;

4.2.1.6. FTP;

4.2.1.7. SMB;

4.2.1.8. DNS, e protocolos de comunicação interna.

4.2.2. Deve ser capaz de detectar ataques de movimentação lateral dentro da rede interna, como varreduras de rede, tentativas de exploração de vulnerabilidades e força bruta;

4.2.3. A solução deverá possuir motores de detecção baseados em:

4.2.3.1. Assinaturas de malware e vulnerabilidades conhecidas;

4.2.3.2. Análise heurística e Machine Learning para ameaças desconhecidas;

4.2.3.3. Detecção de comunicações com servidores de Comando e Controle (C&C);

4.2.3.4. A solução deve ser capaz de detectar e extrair arquivos suspeitos do tráfego de rede para análise profunda (Sandbox); 7

4.2.3.5. A solução deve realizar a inspeção e detecção de ameaças em protocolos de rede industrial (OT/ICS), se configurada para tal.

4.3. Integração com Sandbox e Inteligência

4.3.1. O appliance deverá possuir integração nativa com sandbox (local ou em nuvem) para detecção de ameaças de "dia zero" (Zero-day);

4.3.2. A solução deve suportar a detecção de ataques de Ransomware, identificando comportamentos de criptografia em compartilhamentos de rede (SMB/NFS);

4.3.3. Deve permitir a detecção de técnicas de evasão de sandbox, como atrasos de execução e verificação de ambiente virtual.

4.4. Visibilidade e Resposta a Incidentes (NDR)

4.4.1. A solução deverá fornecer visibilidade completa sobre o tráfego Norte-Sul (perímetro) e Leste-Oeste

(movimentação interna);

4.4.2. Deverá permitir o armazenamento de metadados de rede para fins de investigação forense e retrobusca de ameaças;

4.4.3. A solução deve gerar alertas detalhados contendo: IP de origem, IP de destino, protocolo utilizado, tipo de ameaça detectada e nível de criticidade;

4.4.4. A solução deve permitir a integração com a plataforma de análise e correlação de eventos para correlacionar eventos de rede com eventos de Endpoint (XDR), fornecendo uma visão unificada do ataque.

4.5. Gerenciamento e Relatórios

4.5.1. A solução deverá possuir console de gerenciamento baseada em interface Web (HTTPS);

4.5.2. Deverá permitir a configuração de perfis de inspeção distintos para diferentes segmentos de rede (ex: rede administrativa vs. rede de servidores);

4.5.3. A solução deve suportar o envio de logs para sistemas de terceiros via protocolo Syslog em formato CEF (Common Event Format);

4.5.4. Deve fornecer relatórios executivos e técnicos sobre a postura de risco da rede, principais ativos infectados e protocolos mais utilizados em ataques;

4.5.5. A solução deverá permitir atualizações automáticas de regras de detecção, assinaturas e motores de busca diretamente dos servidores do fabricante.

5. CRÉDITOS TREND AI FLEX VISION ONE

5.1. Características Gerais do Modelo de Licenciamento

5.1.1. A solução deverá ser provida através de um modelo de unidades de créditos flexíveis, permitindo a ativação e desativação dinâmica de sensores de proteção e visibilidade conforme a demanda do ambiente tecnológico da CONTRATANTE;

5.1.2. Os créditos adquiridos deverão permitir o licenciamento de múltiplos vetores de segurança em uma única plataforma unificada, incluindo, no mínimo: Endpoints (Estações e Servidores), Cargas de Trabalho em Nuvem (Cloud Workloads), E-mail, Rede (NDR) e Identidades;

5.1.3. A solução deverá permitir o remanejamento dos créditos entre os diferentes vetores citados sem a necessidade de novos processos de aquisição ou substituição de chaves de licença durante a vigência do contrato;

5.1.4. A plataforma de gestão de créditos deverá ser baseada em nuvem (SaaS), eliminando a necessidade de infraestrutura local para o console de gerenciamento de licenças.

5.2. Funcionalidades de Análise e Correlação (XDR)

5.2.1. Os créditos deverão habilitar a funcionalidade de Extended Detection and Response (XDR), capaz de correlacionar alertas de diferentes camadas (rede, endpoint e e-mail) para identificar ataques complexos e movimentações laterais;

5.2.2. A solução deverá oferecer uma visão única de incidentes, priorizando os alertas com base no risco e no impacto ao negócio, utilizando inteligência artificial para reduzir falsos positivos;

5.2.3. Deverá permitir a análise forense e a busca histórica de ameaças (Threat Hunting) através de um banco de dados de telemetria centralizado;

5.2.4. A solução deve possibilitar a integração nativa com o módulo de detecção de rede (NDR), permitindo que a telemetria de rede de 10 Gbps ou superior seja correlacionada com eventos de sistema operacional.

5.3. Gestão e Transparência do Consumo

5.3.1. A CONTRATANTE deverá ter acesso a um dashboard em tempo real demonstrando:

5.3.1.1. Total de créditos adquiridos;

5.3.1.2. Créditos consumidos por tipo de sensor;

5.3.1.3. Saldo de créditos remanescentes;

5.3.1.4. Projeção de consumo baseada na utilização atual.

5.3.2. A solução deve permitir a exportação de relatórios de uso de créditos em formato CSV ou PDF para fins de auditoria e conformidade;

5.3.3. O modelo deve permitir a escalabilidade imediata, possibilitando a ativação de novos sensores em casos de emergência cibernética, utilizando o saldo de créditos disponível.

5.4. Integração e Resposta a Incidentes

5.4.1. Os créditos de consumo deverão garantir o acesso a APIs de integração (REST) para comunicação com ferramentas de terceiros como SIEM, SOAR e sistemas de chamados (ITSM);

5.4.2. A solução deverá permitir ações de resposta automatizadas ou manuais a partir do console central, tais como: isolamento de host, encerramento de processos maliciosos, bloqueio de remitentes de e-mail e quarentena de arquivos;

5.4.3. Deve incluir acesso a bases de inteligência de ameaças globais do fabricante, atualizadas em tempo real para correlacionar eventos locais com campanhas de ataques globais conhecidas.

5.5. Requisitos de Retenção de Dados

5.5.1. O licenciamento via créditos deverá contemplar a retenção de logs e telemetria para investigação por um período mínimo de 30 dias na plataforma de correlação (XDR), sem custo adicional de armazenamento além dos créditos de consumo previstos para o sensor.

5.6. Tabela de Referência de Consumo

5.6.1. Para fins de dimensionamento, a proposta deverá considerar a conversão de créditos conforme a tabela de consumo do fabricante (exemplo de pesos usuais no modelo Trend AI Flex):

Recurso Protegido	Unidade de Consumo	Créditos (Estimativa)
Endpoint (EDR)	Por Agente / Ano	X Créditos
Server / Cloud Workload	Por Servidor / Ano	Y Créditos
Email Sensor	Por Usuário / Ano	Z Créditos
Network Sensor (NDR)	Por Appliance Virtual / Ano	W Créditos

6. SERVIÇOS GERENCIADOS DE SEGURANÇA PARA SUPORTE E MONITORAMENTO, CONTENDO AÇÕES CORRETIVAS, PREVENTIVAS E DE RESPOSTA A INCIDENTES

5.7. Características Gerais dos Serviços

5.7.1. A CONTRATADA deverá prover serviços gerenciados de segurança cibernética (Managed Security Services – MSS), contemplando operação de Centro de Operações de Segurança (SOC), com monitoramento contínuo, análise de eventos, resposta a incidentes e suporte técnico especializado para toda a solução contratada (EPP/EDR, XDR, NDR e gestão de exposição a riscos).

5.7.2. Os serviços deverão operar de forma integrada à plataforma de segurança contratada, garantindo correlação de eventos, visibilidade centralizada e resposta coordenada a incidentes.

5.7.3. O serviço deverá abranger, no mínimo:

5.7.3.1. Monitoramento contínuo de eventos de segurança;

5.7.3.2. Detecção e análise de ameaças;

5.7.3.3. Investigação de incidentes;

5.7.3.4. Resposta a incidentes de segurança;

5.7.3.5. Apoio à contenção, erradicação e recuperação;

5.7.3.6. Gestão de vulnerabilidades e exposição a riscos;

5.7.3.7. Geração de relatórios técnicos e executivos.

5.8. Monitoramento e Operação de SOC

5.8.1. A CONTRATADA deverá disponibilizar SOC com operação:

5.8.1.1. 24x7 (vinte e quatro horas por dia, sete dias por semana) para eventos críticos;

5.8.1.2. Em horário comercial para demandas administrativas e operacionais.

5.8.2. O SOC deverá:

5.8.2.1. Monitorar logs e eventos provenientes de endpoints, rede e demais ativos;

5.8.2.2. Realizar correlação de eventos com base em inteligência de ameaças;

5.8.2.3. Detectar atividades suspeitas, comportamentos anômalos e ataques avançados;

5.8.2.4. Priorizar incidentes com base em criticidade e impacto ao negócio.

5.8.3. O SOC deverá utilizar inteligência de ameaças atualizada, incluindo:

5.8.3.1. Indicadores de comprometimento (IoCs);

5.8.3.2. Táticas, técnicas e procedimentos (TTPs);

5.8.3.3. Bases globais de reputação e análise comportamental.

5.9. Resposta a Incidentes

5.9.1. A CONTRATADA deverá atuar de forma proativa e reativa na resposta a incidentes, incluindo:

5.9.1.1. Classificação e priorização de incidentes;

5.9.1.2. Investigação detalhada (forense básica);

5.9.1.3. Recomendações de contenção e mitigação;

5.9.1.4. Apoio na execução de ações corretivas (isolamento de máquinas, bloqueios, etc.).

5.9.2. A solução deverá permitir, no mínimo:

5.9.2.1. Isolamento remoto de endpoints comprometidos;

5.9.2.2. Bloqueio de arquivos maliciosos;

5.9.2.3. Bloqueio de conexões e domínios suspeitos;

5.9.2.4. Remediação automatizada sempre que possível.

5.10. Suporte Técnico Especializado

5.10.1. O serviço deverá contemplar suporte técnico contínuo por equipe especializada e certificada nas soluções fornecidas.

5.10.2. O suporte deverá incluir:

5.10.2.1. Atendimento remoto e presencial (quando necessário);

5.10.2.2. Apoio na configuração e ajustes de políticas;

5.10.2.3. Apoio na análise de incidentes e eventos;

5.10.2.4. Intermediação com o fabricante em casos de falhas críticas.

5.10.3. A CONTRATADA deverá disponibilizar ferramenta para:

5.10.3.1. Abertura, acompanhamento e encerramento de chamados;

5.10.3.2. Registro histórico de incidentes;

5.10.3.3. Emissão de relatórios periódicos.

5.11. Relatórios e Governança

5.11.1. A CONTRATADA deverá fornecer relatórios periódicos, no mínimo mensais, contendo:

5.11.1.1. Quantidade e tipos de incidentes detectados;

5.11.1.2. Tempo de resposta e resolução;

5.11.1.3. Principais ameaças identificadas;

5.11.1.4. Recomendações de melhoria de segurança;

5.11.1.5. Indicadores de desempenho (KPIs e SLAs).

5.11.2. Deverão ser realizadas reuniões periódicas (mínimo bimestrais) para:

5.11.2.1. Apresentação de resultados;

5.11.2.2. Análise de incidentes relevantes;

5.11.2.3. Revisão de estratégias de segurança.

5.12. Atualizações e Sustentação

5.12.1. O serviço deverá incluir:

5.12.1.1. Atualizações contínuas de assinaturas, engines e mecanismos de detecção;

5.12.1.2. Aplicação de correções de segurança;

5.12.1.3. Evolução da plataforma conforme novas ameaças.

5.12.2. A CONTRATADA deverá garantir o pleno funcionamento da solução durante toda a vigência contratual, sem ônus adicional.

5.13. Acordo de Nível de Serviço (SLA)

Criticidade	Ocorrência	Tempo Máximo de Resposta	Tempo Máximo de Solução	Glosa por Descumprimento
Crítica	Interrupção total da solução	30 minutos	4 horas	10%
Crítica	Falha generalizada em agentes	30 minutos	4 horas	10%
Crítica	Vazamento ativo de dados	30 minutos	4 horas	10%
Crítica	Indisponibilidade da console	30 minutos	4 horas	10%
Alta	Indisponibilidade de componente essencial	1 hora	8 horas	7%
Alta	Falha em políticas de segurança	1 hora	8 horas	7%
Alta	Degradação da console	1 hora	8 horas	7%
Alta	Falha em atualização crítica	1 hora	8 horas	7%
Média	Erro em relatórios	4 horas	24 horas	4%
Média	Problemas em políticas específicas	4 horas	24 horas	4%
Média	Falhas localizadas	4 horas	24 horas	4%
Baixa	Solicitação de suporte técnico	8 horas úteis	48 horas úteis	2%
Baixa	Dúvidas operacionais	8 horas úteis	48 horas úteis	2%
Baixa	Geração de relatórios	8 horas úteis	48 horas úteis	2%
Baixa	Agendamento de reuniões	8 horas úteis	48 horas úteis	2%

5.13.1. Os serviços deverão estar plenamente integrados aos demais itens da solução (EPP/EDR, XDR, NDR e gestão de exposição a riscos), garantindo uma abordagem unificada de segurança.

5.13.2. A execução dos serviços deverá observar as melhores práticas de mercado, incluindo frameworks como:

5.13.2.1. NIST Cybersecurity Framework;

5.13.2.2. ISO/IEC 27001;

5.13.2.3. CIS Controls.

Documento assinado eletronicamente por **JORGE ANDRE SILVA ABDON**, **CHEFE DA DIVISAO DE DEFESA E MONITORAMENTO CIBERNETICO**, em 29/07/2026, às 20:21, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ARILSON GALDINO DA SILVA**, **COORDENADOR(A) DE SEGURANCA DA INFORMACAO**, em 29/07/2026, às 20:26, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://www.tjpa.jus.br/sei-autenticador informando o código verificador **0000780059** e o código CRC **E456D858**.