TERMO DE REFERÊNCIA

Aquisição de Solução para Análise, Detecção e Resposta a Ameaças e Incidentes de Segurança Cibernética, com garantia, suporte e atualização pelo período de 36 meses.

PROCESSO ADMINISTRATIVO PA-PRO-2022/04525

1. DO OBJETO

Esta contratação tem como objeto a aquisição de Análise, Detecção e Resposta a Ameaças e Incidentes de Segurança Cibernética, com garantia, suporte e atualização pelo período de 36 meses.

2. DA FUNDAMENTAÇÃO

2.1. Da motivação

Nos últimos anos tem se percebido um aumento exponencial no que diz respeito a ataques cibernéticos, gerando grandes incidentes que acabam por tornar os principais sistemas de entidades governamentais indisponíveis. Estes ataques tornaram-se um dos maiores riscos para a credibilidade das instituições, seja de domínio público ou domínio privado, devido aos prejuízos causados na prestação de serviços essenciais para a sociedade em geral.

O cenário atual nos mostra que, diante, não apenas do aumento dos ataques cibernéticos, mas também de sua complexidade, tornando cada vez mais oneroso o restabelecimento dos serviços afetados, as instituições devem possuir controles, políticas, procedimentos, ferramentas e, principalmente, soluções que possam mitigar e responder efetivamente aos incidentes e ataques diversos, que visam o roubo de dados ou tão somente tornar o acesso às informações de determinada instituição inacessíveis.

Ter o conhecimento e estrutura de como agir antes, durante e após determinado incidente, torna-se cada vez mais crucial para o negócio, visto que a capacidade de uma instituição em responder de forma tempestiva a estes incidentes é fundamental para mitigar os impactos causados, permitir o reestabelecimento dos serviços afetados no menor tempo possível e aumentar o nível de prevenção de futuras ocorrências.

Nos anos de 2021 e 2022, o Tribunal de Justiça do Estado do Pará realizou grandes investimentos, com o objetivo de adquirir soluções de segurança da informação que pudessem construir um ecossistema de proteção nas diversas camadas existentes na infraestrutura de TI do tribunal. Assim, tomando como base os incidentes identificados em outras entidades governamentais, contratou-se plataformas de proteção de servidores, *endpoints*, soluções de proteção de acesso privilegiado, *firewall* de aplicação web, dentre outros.

A solução pretendida poderá concentrar informações enviadas por diversas ferramentas já existentes em nosso parque, como *firewalls*, serviços de e-mail, proteção de *endpoint* e de servidor, dentre diversas outras, com o objetivo de analisar de forma inteligente o andamento de ataques e a detecção de incidentes que possam estar ocorrendo na infraestrutura de TI, além da possibilidade de responder a estes incidentes de forma automática, o que poderia aumentar o nível de prevenção e proteção para um período de 24 horas, por 7 dias na semana.

Assim, a referida solução visaria garantir um maior campo de proteção, tanto para a infraestrutura, quanto para o ambiente de aplicações, mantendo o sigilo, disponibilidade e integridade das informações.

Assim, a referida solução visa garantir um maior campo de proteção, tanto para a infraestrutura, quanto para o ambiente de aplicações, mantendo o sigilo, disponibilidade e integridade das informações, através de uma análise e detecção proativa de incidentes de segurança cibernéticas existentes no parque computacional do Tribunal, além da possibilidade de responder a esses incidentes de forma automatizada, cumprindo os seguintes objetivos:

- Identificação de falhas complexas, permitindo que as equipes multidisciplinares mantenham os níveis de segurança da infraestrutura tecnológica;
- Proteger os diversos elementos corporativos de ataques cibernéticos, frustrando prejuízos financeiros e da imagem da instituição;
- Melhoria na confiabilidade e na integridade das informações, evitando vazamento de informações que possam abalar a credibilidade da instituição;
- Efetividade na identificação de incidentes de segurança e ataques cibernéticos;
- Análise inteligente de *logs* originados das mais diversas fontes (soluções de segurança, servidores, *Active Directory,* dentre outras que possam se integrar na solução*).*
- Possibilidade de ações proativas e automatizadas, em resposta a incidentes detectados.

2.2. Dos objetivos a serem alcançados por meio da contratação

2.2.1. Maior proteção dos diversos componentes do ambiente computacional do TJPA;

2.2.2. Monitoramento proativo de ameaças e incidentes existentes no parque computacional do Tribunal;

2.2.3. Possibilidade de ações automatizadas em resposta a esses incidentes e ameaças.

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

2.3. Dos benefícios diretos e indiretos resultantes da contratação

2.3.1. Avaliar de forma contínua os riscos dos ativos de TI do Tribunal.

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

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

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

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

A contratação está alinhada ao **Plano de Gestão 2021-2023 do TJPA**.

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

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

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

A contratação também foi prevista no **Plano de Contratações** no item:

- Contratação de serviço de Identificação e Gerenciamento de Vulnerabilidades, incluindo acompanhamento operacional.

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

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

2.5. Da referência aos Estudos Preliminares

Os estudos preliminares foram protocolados no sistema SigaDoc através do PA-PRO-2022/04525.

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

Esta contratação se destina, fundamentalmente, a possibilitar a análise inteligente da infraestrutura de TI do Tribunal, visando identificar possíveis ameaças e incidentes em andamento e automatizar o processo de resposta a estas ameaças e incidentes que possam afetar as informações e ativos do TJPA.

E ainda ampliar a atuação conjunta entre as coordenadorias atuantes na SECINFO, com o objetivo de conscientização sobre o papel de cada coordenadoria no processo de análise, detecção e resposta a ameaças e incidentes de segurança cibernética.

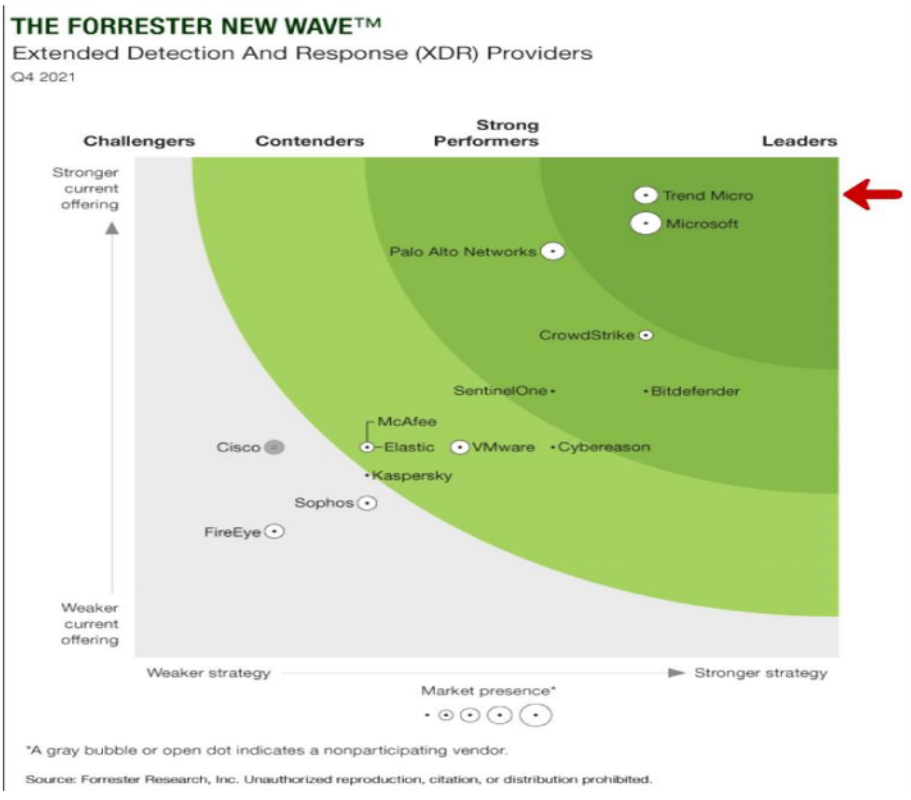
Entende-se que as demandas previstas e projetadas pela Secretaria de Informática do TJPA a serem atendidas pela contratação da solução de análise, detecção e resposta a incidentes de segurança cibernética, serão cobertas em sua plenitude, durante o período de vigência de 36 meses, através do contrato estabelecido entre o CONTRATANTE e a CONTRATADA. Abaixo estão elas listadas:

Item	Descrição	QTD

1	Solução de proteção contra ameaças avançadas - 4 Gbps	01
2	Pacote de instalação (40 Horas)	02
3	Treinamento Hands-On (40 Horas)	01

2.7. Da análise de mercado de TIC

Sendo uma solução comum de mercado, existem diversos fabricantes que podem oferecer soluções de análise, detecção e resposta a ameaças e incidentes de segurança cibernética, com diferentes graus de qualidade e diversos preços a serem pagos. Cumprindo destacar que, atualmente, o TJPA não possui a solução específica de proteção mencionada e, conforme detalhamento do potencial da solução, busca-se a contratação da solução que apresentar melhor custo-benefício, em qualidade e preço a ser pago. Sendo inviável avaliar todas as opções disponíveis, recorreu-se ao Forrester Wave, empresa referência na área de consultoria em soluções de Tecnologia da Informação, para delimitar as melhores opções a serem consideradas.



O Forrester Wave realiza a mensuração da qualidade e relevância de soluções de TI através de um gráfico que ficou conhecido como "**Quadrante**", o qual reflete os estudos publicados anualmente sobre categorias de produtos e serviços, ou as opiniões emitidas pelos

clientes que utilizaram determinada solução. Como o TJPA preza pela qualidade das soluções contratadas para compor sua infraestrutura tecnológica, as soluções consideradas foram as que se estavam mais bem posicionadas no quadrante "***Leaders***" da avaliação mais recente, publicada em setembro de 2021. Os fabricantes mais bem localizados neste quadrante foram avaliados com as melhores opiniões a respeito da sua solução oferecida.

Ao que podemos verificar no quadrante do Forrester Wave, o fabricante que está melhor posicionado é a **Trend Micro**, cumprindo lembrar que o Tribunal ainda não possui qualquer solução de análise, detecção e resposta a ameaças e incidentes de segurança cibernética.

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

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

Destaca-se a Secretaria de Estado da Administração e Previdência do Piauí (SEADPREVI/PI) que, através da Ata de Registro de Preço (ARP) gerada no Pregão Eletrônico 09/2021, registrou preços para aquisição do objeto "Registro de Preço para contratação, SOB DEMANDA, de solução unificada para proteção de e-mail, proteção de Endpoint e proteção contra-ataques avançados, com garantia de 36 meses, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico, para atendimento das necessidades dos órgãos e entes da Administração Pública, de acordo com as especificações técnicas contidas no Termo de Referência, conforme condições, quantidades e exigências estabelecidas no Anexo I **–** Termo de Referência".

A Defensoria Pública do Estado do Pará (DPEPA), através da Ata de Registro de Preço (ARP) nº 004/2021 gerada no Pregão Eletrônico 003/2021, registrou preços para aquisição do objeto "Contratação de empresa para fornecimento de subscrição de softwares de segurança, incluindo garantia, atualização de versão, suporte técnico por 24 meses, transferência de conhecimento e serviços técnicos especializados, para atender as necessidades da Defensoria Pública do Estado do Pará".

A Polícia Rodoviária Federal (PRF), através do Contrato nº 1/2022 gerado no Pregão Eletrônico 19/2021, cujo objeto é a "contratação de serviço de TIC para a utilização de programas de informática, do tipo solução avançada de segurança, composta de: Plataforma de Proteção de Endpoint (EPP), Solução de EDR (Detecção e Respostas a Ameaças) e Solução Contra APT (Proteção Contra Ameaças Persistentes Avançadas) contemplando o licenciamento, implantação, suporte técnico, capacitação, garantia e atualização por 12 (doze) meses, no âmbito da Sede Nacional, nas Unidades Regionais e na Universidade Corporativa da Polícia Rodoviária Federal, que serão prestados nas condições estabelecidas no Termo de Referência, anexo do Edital.".

2.8. Da natureza do objeto

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

Além disso, trata-se de prestação de serviço continuado, uma vez que sua interrupção pode comprometer a segurança das informações e da infraestrutura de TI do Tribunal, já que não será possível detectar, em tempo hábil, possíveis ameaças e incidentes que possam causar a interrupção dos serviços oferecidos pelo Tribunal.

2.9. Do parcelamento do objeto

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

2.9.2. O disposto, no entanto, não se aplica na presente demanda, sendo necessário o agrupamento em Lote, tendo em vista a garantia da uniformidade na prestação dos serviços, uma vez que os itens agrupados possuem a mesma natureza e guardam relação entre si, afastando possíveis prejuízos à competitividade, ao mesmo tempo em que exerce maior atratividade perante os licitantes. Ademais, considerando o número de itens, a organização em lote evita que inúmeros contratos sejam celebrados com diferentes fornecedores, situação que, tecnicamente, afeta diretamente a rotina da Administração, prejudicando a eficiência administrativa, que passa pela otimização do gerenciamento de seus contratos de fornecimento, uma vez que lidar com um único fornecedor diminui o custo administrativo de gerenciamento de todo o processo de contratação.

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

2.9.4. Dessa forma a presente contratação será realizada por meio de lote único com 03 (três) itens, considerando para efeito de adjudicação, o MENOR PREÇO GLOBAL POR LOTE.

2.10. Da seleção do fornecedor

A seleção do fornecedor será feita para o licitante que apresentar menor preço por lote único, desde que sejam atendidos plenamente às condições do edital, com toda a documentação e comprovação técnica exigida.

2.10.1. Da forma e do critério de seleção

O critério de aceitabilidade de preços será realizado por LOTE ÚNICO, mediante a análise de proposta. Além disso, cita-se que não será aceita proposta, após a fase de lances e negociação, cujo valor do lote único esteja superior ao estimado pelo TJPA na fase de cotação de preços.

2.10.2. Da modalidade e do tipo de licitação

Licitação, na modalidade PREGÃO, na forma ELETRÔNICO, com regime de execução indireta, tendo como critério de julgamento o MENOR PREÇO POR LOTE, que será regida pela

Lei n.º 10.520, de 17/07/2002, Decreto nº 5450/05, Decreto 7892/2013 e Lei Complementar nº 123/06 e, subsidiariamente, pela Lei N.º 8.666, de 21/06/1993 e suas alterações posteriores.

2.10.3. Dos critérios técnicos de habilitação obrigatórios

HABILITAÇÃO JURÍDICA

a) No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

b) No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório da indicação de seus administradores;

c) No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

d) No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização;

e) No caso de microempresa ou empresa de pequeno porte: certidão expedida pela Junta Comercial ou pelo Registro Civil das Pessoas Jurídicas, conforme o caso, que comprove a condição de microempresa ou empresa de pequeno porte– segundo determinado pelo Departamento de Registro Empresarial e Integração - DREI;

f) Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva; indicar o responsável pela administração com poderes para assumir obrigações e assinar documentos em nome do licitante; apontar a sua sede; além de explicitar o objeto social, que deverá ser compatível com o objeto desta licitação, conforme a tabela da Classificação Nacional de Atividades Econômicas – CNAE, do IBGE.

QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

a) Certidão negativa de falência ou de recuperação judicial, expedida pelo distribuidor da sede da pessoa jurídica. Para efeito de constatação da validade de tal certidão, será observado o prazo de validade constante na própria certidão. Caso a licitante esteja em recuperação judicial, será válida, para fins de qualificação econômico-financeira, a emissão de certidão, pela instância judicial competente, afirmando que a interessada está apta econômica e financeiramente a participar de procedimento licitatório, conforme Acórdão TCU nº 1201/2020 – Plenário.

b) O licitante deverá apresentar os seguintes índices contábeis, extraídos do último balanço patrimonial ou do balanço patrimonial referente ao período de existência da sociedade, atestando a boa situação financeira, conforme art. 7.2 da IN/MARE 05/95, Portaria GAB. SEAD. Nº 88/15:

LG= Liquidez Geral – superior a 1

SG= Solvência Geral – superior a 1

LC= Liquidez Corrente – superior a 1

Sendo,

LG= (AC+RLP) / (PC+PNC)

SG= AT / (PC+PNC)

LC= AC / PC

Onde:

AC= Ativo Circulante

RLP= Realizável a Longo Prazo

PC= Passivo Circulante

PNC= Passivo Não Circulante

AT= Ativo Total

c) As demonstrações contábeis apresentadas poderão ser submetidas à apreciação do Conselho Regional de Contabilidade.

d) O balanço patrimonial e as demonstrações contábeis, bem como os índices contábeis exigidos, deverão estar assinados por contador ou outro profissional equivalente, devidamente registrado no Conselho Regional de Contabilidade.

e) A licitante que apresentar índice econômico igual ou inferior a 01 (um) em qualquer dos índices de Liquidez Geral, Solvência Geral e Liquidez Corrente, deverá comprovar que possui patrimônio líquido mínimo não inferior a 10% (dez por cento) do valor estimado da contratação ou item pertinente, por meio de Balanço Patrimonial e demonstrações contábeis do último exercício, já exigíveis e apresentados na forma da lei, vedada a sua substituição por balancetes ou balanços provisórios.

REGULARIDADE FISCAL e TRABALHISTA

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);

b) Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto deste certame.

c) Prova de regularidade com o Fundo de Garantia do Tempo de Serviço – FGTS (CRF, fornecido pela Caixa Econômica Federal). Será aceito certificado da matriz em substituição ao da filial ou vice-versa quando, comprovadamente, houver arrecadação centralizada;

d) Prova de regularidade para com a Justiça do Trabalho emitida pelo TST (Certidão Negativa de débitos Trabalhistas);

e) Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradoria-Geral da Fazenda Nacional;

f) Prova de regularidade para com a Fazenda Estadual e Municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;

Se, pelas documentações fornecidas diretamente pelo representante legal, não se puder inferir que o subscritor de tais declarações tem poderes para representar a empresa, esta será inabilitada.

Todos os documentos apresentados para habilitação deverão estar:

- Em nome da licitante, com número do CNPJ e com o respectivo endereço da mesma;
- Se a licitante for a matriz de uma empresa, todos os documentos deverão estar em nome da matriz;
- Se a licitante for a filial de uma empresa, todos os documentos deverão estar em nome desta filial;
- Se a licitante for a matriz da empresa e a fornecedora do objeto for uma de suas filiais, este fato deve ser expressamente registrado em declaração apresentada na qual a licitante indicará qual filial executará o objeto da licitação. Neste caso, os documentos relativos à regularidade fiscal, exigidos para a habilitação, deverão ser apresentados em nome da matriz e da filial, simultaneamente;
- Serão dispensados da filial aqueles documentos que, pela sua própria natureza, comprovadamente, forem emitidos somente em nome da matriz;
- Serão aceitos registros de CNPJ de licitantes matriz e filiais com diferenças de números nos documentos pertinentes ao CND e ao FGTS quando for comprovada a centralização do recolhimento dessas contribuições pela licitante.

A licitante ainda deverá apresentar declaração de que inexiste, no quadro funcional da empresa, menor de dezoito anos desempenhando trabalho noturno, perigoso ou insalubre ou menor de dezesseis anos executando qualquer trabalho, salvo na condição de aprendiz, a partir dos quatorze anos, conforme modelo constante nos anexos do Edital.

Caso permitida a participação de sociedades cooperativas, será exigida, ainda, a seguinte documentação complementar:

1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764 de 1971;
2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;
3. A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;
4. O registro previsto na Lei n. 5.764/71, art. 107;
5. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato; e
6. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa:
    - ata de fundação;
    - estatuto social com a ata da assembleia que o aprovou;
    - regimento dos fundos instituídos pelos cooperados, com a ata da assembleia;

- editais de convocação das três últimas assembleias gerais extraordinárias;
- três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e
- ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

7. A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764/71 ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

2.11. Do impacto ambiental

De acordo com os estudos preliminares referentes a esta contratação, o impacto que pode ocorrer é o acréscimo de energia elétrica e dissipação de calor no datacenter onde o equipamento pertencente a solução será instalado.

2.12. Da conformidade técnica e legal

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

2.13. Das obrigações

2.13.1. Das obrigações do CONTRATANTE

2.13.1.1. Cumprir fielmente o Contrato de modo que a CONTRATADA possa realizar os serviços com esmero e perfeição;

2.13.1.2. Receber os empregados e prepostos da CONTRATADA, devidamente credenciados, para manutenção e conservação dos equipamentos, tomando as providências administravas que garantam o livre desempenho de tais atividades;

2.13.1.3. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos, após assinatura do Contrato, conforme disposto artigo 30 da IN04-SLTI/MPOG;

2.13.1.4. Encaminhar formalmente a demanda, preferencialmente por meio de Ordem de Serviço, de acordo com os critérios estabelecidos neste Termo de Referência observando-se o disposto nos artigos 19 e 33 da IN04-SLTI/MPOG;

2.13.1.5. Receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita, conforme inspeções realizadas, de acordo com o disposto no artigo 21 da IN04-SLTI/MPOG;

2.13.1.6. Aplicar à CONTRATADA as sanções administravas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando se tratar de contrato oriundo de Ata de Registro de Preços;

2.13.1.7. Liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em Contrato;

2.13.1.8. Comunicar à CONTRATADA todas e quaisquer ocorrências relacionadas com o fornecimento da Solução de Tecnologia da Informação;

2.13.1.9. Definir produtividade ou capacidade mínima de fornecimento da Solução de Tecnologia da Informação por parte da CONTRATADA, com base em pesquisas de mercado, quando aplicável;

2.13.1.10. Realizar, no momento da licitação e sempre que possível, diligências e/ou Prova de Conceito com o licitante classificado provisoriamente em primeiro lugar, para fins de comprovação de atendimento das especificações técnicas, exigindo, no caso de fornecimento de bens, a descrição em sua proposta da marca e modelo dos bens ofertados;

2.13.1.11. A CONTRATANTE se reserva o direito a qualquer momento de realizar diligências junto à CONTRATADA e aos fabricantes para esclarecimento de dúvidas;

2.13.1.12. Faculta-se ao CONTRATANTE e à CONTRATADA, sempre quando necessário, agendar reuniões periódicas de caráter gerencial ou técnico para avaliar os trabalhos, adotar resoluções e obter esclarecimento de pendências durante toda a vigência do contrato.

2.13.1.13. Efetuar o pagamento de acordo com as normas orçamentárias e financeira do TJPA.

2.13.2. Das obrigações da CONTRATADA

2.13.2.1. Cumprir fielmente o Contrato de modo que o serviço se realize com esmero e perfeição, executando-os sob sua inteira e exclusiva responsabilidade;

2.13.2.2. Cumprir rigorosamente as normas e regulamentos pertinentes à solução objeto deste Termo de Referência;

2.13.2.3. Garantir o perfeito funcionamento da solução objeto deste Termo de Referência, através de equipe técnica dimensionada de forma a atender as solicitações dentro dos prazos necessários ao cumprimento dos cronogramas estabelecidos;

2.13.2.4. Emitir, sempre que solicitado pelo TJPA, relatórios gerenciais e/ou técnicos referentes aos serviços produzidos;

2.13.2.5. Dar ciência, imediatamente e por escrito, de qualquer anormalidade que verificar na implantação da solução, bem como, prestar esclarecimentos que forem solicitados pelo TJPA;

2.13.2.6. Utilizar profissionais devidamente capacitados e habilitados para os serviços contratados, impondo-lhes rigorosos padrões de qualidade, segurança e eficiência, correndo por sua conta todas as despesas com salários, impostos, contribuições previdenciárias, encargos trabalhistas, seguros e outras correlatas;

2.13.2.7. Manter sigilo absoluto sobre todas as informações provenientes dos serviços realizados;

2.13.2.8. Refazer serviços nos prazos estabelecidos, quando apresentarem padrões de qualidade inferiores aos definidos, sem ônus para o TJPA;

2.13.2.9. Disponibilizar os Serviços para uso pela contratante dentro do prazo pactuado pela CONTRATANTE;

2.13.2.10. Disponibilizar aplicações de monitoramento da solução para os analistas do TJPA;

2.13.2.11. Manter a qualidade dos Serviços dentro dos padrões estabelecidos;

2.13.2.12. Atender a reclamações da contratante sobre falhas nos Serviços;

2.13.2.13. Fazer diagnóstico das falhas dos Serviços, eliminando os defeitos nos componentes sob sua responsabilidade;

2.13.2.14. Atender a reclamações ou pedidos de esclarecimentos da CONTRATANTE sobre cobrança dos Serviços;

2.13.2.15. Tomar todas as providências necessárias para a fiel execução deste Instrumento;

2.13.2.16. Toda solução a que se refere este documento deverá estar implementada, assim como, os profissionais, devidamente habilitados, referidos neste termo aptos em até 10 (dez) dias corridos após a assinatura do contrato;

2.13.2.17. A CONTRATADA deverá garantir o serviço de suporte à customização, à parametrização e à configuração voltadas à utilização de funcionalidades disponibilizadas na versão apresentada ou em versões superiores do sistema utilizado durante a vigência do contrato;

2.13.2.18. A CONTRATADA deverá garantir que, durante a vigência do contrato, quando da descontinuidade de um produto e lançamento de outro, o CONTRATANTE passará a ter direito de uso do produto mais recente (sucessor) e a documentação completa sem custos adicionais. Além disso, o produto mais recente deverá possuir substancialmente o mesmo nível de características, valores e funcionalidades do anterior. Caso o novo produto seja um software desenvolvido no âmbito da execução do Objeto;

2.13.2.19. Caso haja atualização de release do software, a CONTRATADA deverá manter o funcionamento do ambiente durante a vigência do contrato ininterruptamente;

2.13.2.20. A manutenção deverá incluir o acesso, livre de qualquer ônus, ao website e à base de conhecimento da solução ofertada, bem como ao seu repositório de programas contendo correções, atualizações recentes, "drivers", programas de controle e informações;

2.13.2.21. Nos casos em que as manutenções necessitarem de paradas das soluções, o CONTRATANTE deverá ser imediatamente no ficado para que se proceda à aprovação da manutenção ou para que seja agendada nova data, a ser definida pelo CONTRATANTE, para execução das atividades de manutenção;

2.13.2.22. Correrá por conta exclusiva da CONTRATADA a responsabilidade pelo deslocamento de sua equipe aos locais de prestação dos serviços, bem como as despesas de transporte, frete e seguro correspondente, quando acionado pelo CONTRATANTE e não resolvido remotamente;

2.13.2.23. Caso haja migração da solução, todo o processo se dará sem ônus para o CONTRATANTE;

2.13.2.24. Em caso de remanejamento ou de mudança física do ambiente de produção, a CONTRATADA deverá realizar a orientação na utilização, o acompanhamento pós-instalação, a orientação e a execução do planejamento de migração;

2.13.2.25. A CONTRATADA deverá solucionar problemas inerentes a todos os produtos e garantir que possam ser instalados em outro ambiente de produção desde que este ambiente esteja na sua matriz de compatibilidade e suportabilidade, em qualquer das unidades funcionais do CONTRATANTE;

2.13.2.26. A CONTRATADA prestará toda orientação técnica necessária para a perfeita utilização dos produtos, para obtenção do máximo desempenho destes durante o período de vigência do contrato, conforme definido abaixo:

2.13.2.26.1. Identificar e corrigir problemas de funcionamento;

2.13.2.26.2. Apoio nas definições do produto para composição de soluções;
2.13.2.26.3. Apoio na customização do produto para melhor adequação às necessidades do CONTRATANTE e para composição de soluções;
2.13.2.26.4. Avaliações, diagnósticos e proposições de soluções de melhoria em ambiente de produção;
2.13.2.26.5. A CONTRATADA deverá garantir a priorização de correções e melhorias dentro dos níveis de serviços estabelecidos no contrato;
2.13.2.26.6. A CONTRATADA deverá prestar orientações para identificação de causa de falhas da solução e seus componentes e apoio na recuperação de ambientes em caso de panes ou perda de dados;
2.13.2.26.7. A CONTRATADA deverá garantir disponibilização de correções e upgrade de versões e releases durante a vigência do contrato.

3. ESPECIFICAÇÃO TÉCNICA DETALHADA

3.1. Dos papeis a serem desempenhados

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

PAPEL	ENTIDADE	RESPONSABILIDADE
Equipe de Apoio da Contratação	TJPA	Equipe responsável por subsidiar a área de licitações em suas dúvidas, respostas aos questionamentos, recursos e impugnações, bem como na análise e julgamento das propostas das licitantes.
Equipe de Gestão e Fiscalização do Contrato	TJPA	Equipe composta pelo gestor do contrato, responsável por gerir a execução contratual, e pelos fiscais demandante, técnico e administrativo, responsáveis por fiscalizar a execução contratual.
Fiscal Demandante do Contrato	TJPA	Servidor representante da área demandante da contratação, indicado pela referida autoridade competente, responsável por fiscalizar o contrato quanto aos aspectos funcionais do objeto, inclusive em relação à aplicação de sanções.
Fiscal Técnico do Contrato	TJPA	Servidor representante da área técnica, indicado pela respectiva autoridade competente, responsável por fiscalizar o contrato quanto aos aspectos técnicos do objeto, inclusive em relação à aplicação de sanções.
Fiscal Administrativo do Contrato	TJPA	Servidor representante da Secretaria de Administração, indicado pela respectiva autoridade, responsável por fiscalizar o contrato

		quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.
Gestor do Contrato	TJPA	Servidor com atribuições gerenciais, técnicas ou operacionais relacionadas ao processo de gestão do contrato, indicado por autoridade competente do órgão.
Preposto	Contratada	Funcionário representante da empresa contratada, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao órgão contratante, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual.

Equipe de apoio da contratação (quando se tratar de licitação)		
INTEGRANTE DEMANDANTE Nome: **Arilson Galdino Da Silva** Matrícula: 183318 Telefone: 3289-7181 E-mail: arilson.silva@tjpa.jus.br	**INTEGRANTE TÉCNICO** Nome**: Thiago do Rosário de Castro** Matrícula: 174394 Telefone: 3289-7189 E-mail: thiago.rosario@tjpa.jus.br	**INTEGRANTE ADMINISTRATIVO** Nome: **Luciano Santa Brigida das Neves** Matrícula: 147460 Telefone: 3205-3571 E-mail: luciano.neves@tjpa.jus.br

Equipe de gestão e fiscalização da contratação			
GESTOR DO CONTRATO Nome: **Arilson Galdino da Silva** Matrícula: 183318 Telefone: 3289-7181 E-mail: arilson.silva@tjpa.jus.br	**FISCAL DEMANDANTE** Nome: **Arilson Galdino da Silva** Matrícula: 183318 Telefone: 3289-7181 E-mail: arilson.silva@tjpa.jus.br	**FISCAL TÉCNICO** Nome**: Thiago do Rosário de Castro** Matrícula: 174394 Telefone: 3289-7189 E-mail: thiago.rosario@tjpa.jus.br	**FISCAL ADMINISTRATIVO** Nome: Matrícula: Telefone: E-mail:

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

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

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

Cabe ao PREPOSTO e ao RESPONSÁVEL TÉCNICO:

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

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

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

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

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

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

3.2. Da dinâmica de execução do contrato

3.3. Etapas

3.4. Dos prazos

3.4.1. Prazos de entrega dos bens/execução dos serviços

Os prazos de início dos serviços são contados a partir da assinatura, do CONTRATANTE e da CONTRATADA, na Ordem de Serviço (OS) de cada serviço solicitado. Os prazos de execução poderão ser prorrogados, desde que devidamente justificada a necessidade e anuído pelas partes.

Os serviços serão executados e os produtos entregues preferencialmente na sede da CONTRATANTE, na cidade de Belém-PA. Eventualmente, alguns serviços poderão ser executados nas dependências da empresa CONTRATADA, quando de interesse da CONTRATANTE e da empresa CONTRATADA, sendo previamente autorizado pela CONTRATANTE. Os serviços serão realizados durante à jornada de trabalho habitual de 06 (seis) horas diárias, de segunda a sexta-feira, no horário de expediente da CONTRATANTE.

3.4.2. Prazo de vigência do contrato

O prazo de vigência do contrato a ser firmado será de 12 (Doze) meses, a contar da data de sua assinatura, prorrogável na forma do art 57, IV, da Lei Nº 8.666/93, até o limite de 48 (Quarenta e Oito) meses.

3.4.3. Logística de implantação

Os equipamentos deverão ser entregues no Almoxarifado Central do TJPA, sito à Rodovia Augusto Montenegro, Km 4, bairro Parque Verde, em Belém, de segunda a sexta-feira, no horário de 08:00 às 14:00, conforme agendamento prévio.

3.4.4. Cronograma

Não haverá nenhum cronograma a ser cumprido pela CONTRATADA, mas somente a exigência de cumprimento do prazo de entrega dos equipamentos.

3.5. Dos instrumentos formais de solicitação

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

3.6. Garantia e Nível de Serviço

3.6.1. Garantia do produto/serviço

De acordo com o item 3.6.3 dos estudos preliminares, o prazo de garantia do software, suporte e licenciamento que serão adquiridos deverá ser de 36 (trinta e seis) meses.

3.6.2. Garantia contratual

Haverá depósito em garantia da execução do contrato no valor de 2%, com validade de 90 dias após o término da vigência contratual devendo ser renovada a cada prorrogação efetivada no contrato nos moldes do art.18 inciso XVII do decreto estadual 14.483/2011, e somente será liberada ante a comprovação de que empresa contratada quitou todas as suas obrigações para a satisfatória entrega do objeto deste TERMO DE REFERÊNCIA.

3.6.3. Nível de Serviço

Não haverá

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

A CONTRATADA deverá fornecer previamente os contatos de e-mail e telefone dos envolvidos na execução do objeto da contratação. Estes serão os principais canais de comunicação a serem utilizados durante a execução do contrato, devendo a comunicação ser realizada preferencialmente por e-mails, para geração de registros documentais. Pela CONTRATANTE, os componentes da Equipe de Gestão e Fiscalização da Contratação se encarregarão da comunicação com a CONTRATADA no tocante à execução do contrato.

3.8. Do recebimento

3.8.1. Do recebimento provisório e definitivo

3.8.1.1. As contratações devem observar os seguintes prazos para recebimento dos serviços:

3.8.1.1.1. O **Recebimento Provisório** do objeto no prazo de 15 (quinze) dias pelo fiscal do contrato, mediante termo circunstanciado, assinado pelas partes;

3.8.1.1.2. O **Recebimento Definitivo** do objeto por servidor ou comissão designada pela autoridade competente e presidida pelo fiscal do contrato, mediante termo circunstanciado, assinado pelas partes, após o decurso do prazo de observação, ou vistoria que comprove a adequação do objeto aos termos contratuais, que se dará a cada 30 (trinta) dias, sem prejuízo da obrigação de o contratado reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados, na forma prevista no art. 73, I, "b", c/c art. 69 da Lei n. 8.666/1993, no prazo de até 03 (três) dias uteis;

3.8.1.2. O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança da obra ou do serviço, nem ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos pela lei ou pelo contrato;

3.8.1.3. Na hipótese de o termo circunstanciado ou a verificação a que se refere item 3.8.1.1 não serem, respectivamente, lavrado ou procedida dentro dos prazos fixados, reputar-se-ão como realizados, desde que comunicados à Administração

3.9. Da forma de pagamento

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

O pagamento será realizado no prazo máximo de até 30 (trinta) dias, contados a partir da data final do período de adimplemento a que se referir, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo CONTRATADO.

O preço consignado no contrato será corrigido anualmente, observado o interregno mínimo de um ano, contado a parr da data limite para a apresentação da proposta, pela variação do Índice Nacional de Preços ao Consumidor Amplo – IPCA divulgado pelo Instuto Brasileiro de Geografia e Estasca – IBGE, ou outro índice que venha a substuí-lo exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

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

Os valores serão remanejados das Notas de Reservas 2023, ações 8651, 8652 e 8653, fonte 0118, elemento de despesa 3.3.90.40, as quais estão rateadas em 65% no 1G, 9% no 2G e 26% no Apoio Indireto.

3.10. Da transferência de conhecimento

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

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

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

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

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

3.11. Dos direitos de propriedade intelectual e autoral

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

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

3.12. Da qualificação técnica dos profissionais

a) A licitante será habilitada a participar do certame com a apresentação de, pelo menos, 01 (um) Atestado(s) de Capacidade Técnica, a ser(em) fornecido(s) por pessoa jurídica de direito público ou privado, em documento timbrado, e que comprove(m) a aptidão da licitante para desempenho de atividade pertinente e compatível em características e volume com o objeto da licitação, por meio da prestação satisfatória de serviços técnicos em território nacional.

b) O atestado deverá possuir informações suficientes para qualificar o seu objeto, bem como possibilitar ao CONTRATANTE confirmar sua veracidade junto à instituição emissora do atestado;

c) No caso deste processo licitatório, o fornecimento do(s) atestado(s) de capacidade técnica, deve referenciar um quantitativo mínimo de 30% (trinta por cento) para o fornecimento dos volumes prospectados para cada licença.

d) Para verificar a autenticidade dos atestados apresentados, o CONTRATANTE poderá realizar diligências ou requerer acompanhados dos comprovantes fiscais da execução do objeto.

e) Da Declaração de que possui profissional qualificado: A licitante deverá apresentar declaração, datada e assinada por seu representante legal, de que, caso se sagre vencedora do certame, no momento da assinatura do contrato, disporá de profissionais com nível superior e com as seguintes certificações ou equivalentes: profissionais capacitados e certificados nos produtos objeto desta licitação visando à execução de serviços de instalação e/ou de manutenção dos produtos componentes da solução ofertada.

3.13. Das sanções

3.13.1. Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, o licitante ou adjudicatário que:

3.13.1.1. Não assinar a ata de registro de preços quando convocado dentro do prazo de validade da proposta, não aceitar/retirar a nota de empenho ou não assinar o termo de contrato decorrente da ata de registro de preços;

3.13.1.2. Apresentar documentação falsa;

3.13.1.3. Deixar de entregar os documentos exigidos no certame;

3.13.1.4. Ensejar o retardamento da execução do objeto;

3.13.1.5. Não mantiver a proposta;

3.13.1.6. Cometer fraude fiscal;

3.13.1.7. Comportar-se de modo inidôneo;

3.13.1.7.1. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

3.13.2. O licitante/adjudicatário que cometer qualquer das infrações discriminadas no subitem anterior ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

3.13.2.1. Multa de 10% (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;

3.13.2.2. Impedimento de licitar e de contratar com o Estado do Pará e descredenciamento no SICAF, pelo prazo de até cinco anos.

3.13.3. A penalidade de multa pode ser aplicada cumulativamente com a sanção de impedimento.

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

4. Da confidencialidade de informações

4.1 A CONTRATADA será expressamente responsabilizada quanto à manutenção de sigilo absoluto sobre quaisquer dados, informações, códigos-fonte e artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venha a ter conhecimento durante a execução dos

trabalhos, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo TJPA, tais documentos.
4.2 A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto sem autorização por escrito do TJPA, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.
4.3 Cada profissional deverá assinar termo de responsabilidade e sigilo, comprometendo-se a não divulgar nenhum assunto tratado nas dependências do TJPA ou a serviço desses, salvo se expressamente autorizado.
4.4 Cada profissional deverá assinar termo declarando estar ciente de que a estrutura computacional disponibilizada pelo TJPA não poderá ser utilizada para fins par celulares e que a navegação em sítios da Internet e as correspondências em meio eletrônico utilizando o endereço do TJPA, ou acessadas a partir dos seus equipamentos, poderão ser auditadas.
4.5 Cada profissional da CONTRATADA deverá assinar termo de compromisso declarando total obediência às normas de segurança vigentes ou que venham a ser implantadas, a qualquer tempo, no TJPA.
4.6 Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. Abrange toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE.
4.7 As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto.
4.8 As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que sejam comprovadamente de domínio público no momento da revelação, tenham sido comprovadas e legitimamente recebidas de terceiros e estranhos, sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido no ficadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.
4.9 A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.
4.10 A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO sobre a existência deste TERMO bem como da natureza sigilosa das informações.
4.11 A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.
4.12 A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

5. DOS REQUISITOS TÉCNICOS ESPECÍFICOS

5.1. Solução de proteção contra ameaças avançadas - 4 Gbps

5.1.1. Deverá fornecer solução integrada de proteção contra ameaças avançadas de acordo com funcionalidades e características técnicas especificadas neste documento, contendo, no mínimo os seguintes módulos:

5.1.1.1. Monitoramento, Identificação, Análise e Resposta de Incidentes de Segurança;
5.1.1.2. Detecção de ataques direcionados;
5.1.1.3. Analisador virtual de ameaças;
5.1.1.4. Correlação de regras para detecção de conteúdo malicioso;
5.1.1.5. Análise de todos os estágios de uma sequência de ataques.

5.2. Características Gerais da Solução

5.2.1. Esta solução deverá ser atendida através do fornecimento de solução de um único Fabricante, contendo:

5.2.1.1. Serviço de Monitoração e Análise de Ameaças Digitais em rede;

5.2.1.2. Serviço de Monitoração e gestão de riscos que permita a identificação de ameaças digitais conhecidas e não conhecidas por soluções de antivírus tradicionais, permitindo a composição de serviços de mitigação complementares para a segurança do ambiente;

5.2.1.3. Serviço que entenda ameaça digital como a representação de um spyware malicioso ou ação maliciosa tal como: spyware, phishing, worms, bot, trojan, adware, network exploit, web exploit, Cross-site scripting, spear phishing, information stealing malware e outras ações que podem compor ataques ao patrimônio computacional do ambiente;

5.2.1.4. Visibilidade e relatório de incidentes de conexões da rede interna com sites maliciosos ou servidores de central de comando (C&C) externos.

5.2.1.5. Análise e correlação de atividades maliciosas tais como:

5.2.1.5.1 Detecção específica de malwares conhecidos e arquivos contaminados através de assinaturas de antivírus tradicional no tráfego da rede;
5.2.1.5.2. Detecção de vermes de rede e de e-mail no tráfego de rede;
5.2.1.5.3. Detecção de programas de exploração de vulnerabilidades (Exploits) na rede;
5.2.1.5.4. Detecção de empacotamentos maliciosos no tráfego da rede;
5.2.1.5.5. Validação de tráfego web malicioso através de consultas a sistemas de reputação na Internet;
5.2.1.5.6. Visibilidade e relatório de estatísticas de ameaças, fontes de infecção na rede monitorada e máquinas comprometidas.

5.2.1.6. Permitir a rápida identificação da criticidade dos eventos de segurança;

5.2.1.7. Permitir realizar pesquisas avançadas e customizadas dos incidentes de segurança através da console de gerenciamento;

5.2.1.8. Possibilidade de criação de filtros para visualização de eventos específicos conforme contexto, localização e outras variáveis que permitam investigação profunda sobre causa raiz de incidentes de segurança;

5.2.1.9. Permitir a customização de alertas em base ao tipo de incidente de segurança através da console de gerenciamento;

5.2.1.10. Permitir a integração com sistemas de serviço de diretório;

5.2.1.11. Capacidade de verificar em tempo real a reputação de endereços web (URL's) e servidores de correio SMTP;

5.2.1.12. A análise de SMTP será realizada em uma solução separada do sensor de HTTP e demais protocolos;

5.2.1.13. A análise em SMTP será realizada de modo MTA (Inline);

5.2.1.14. A análise de e-mail em sandbox deverá ocorrer em arquivos Microsoft Office, PDF, arquivos compactados e executáveis do tipo PE;

5.2.1.15. A análise em sandbox será realizada na própria solução, não sendo necessário integrações com demais soluções ofertadas;

5.2.1.16. A solução devera possuir mecanismo de derivar senhas de arquivos protegidos, para análise em sandbox;

5.2.1.17. A solução devera possuir mecanismo de conhecimento de senhas de pelo menos 90 palavras chaves em seu vocabulário de conhecimento, para derivação de arquivos protegidos;

5.2.1.18. Capacidade de criar e salvar investigações customizadas dos incidentes de segurança;

5.2.1.19. Deve possuir pelo menos 1 sensor para "escutar" o tráfego de rede de throughput de 4Gbps de análise;

5.2.1.20. Deve possuir a capacidade de detectar ameaças direcionadas, ataques do dia zero e documentos que viabilizem ataques;

5.2.1.21. Deve detectar atividades maliciosas que trafegam na rede através de motor de análise de comportamento de tráfego até o nível 7 (camada de aplicação) em protocolo TCP/IP;

5.2.1.22. Capacidade de detectar ameaças web tais como vulnerabilidades e download de conteúdo malicioso;

5.2.1.23. Os módulos de captura de rede deverão suportar a coleta de arquivos pelo menos nos protocolos HTTP e HTTPS;

5.2.1.24. Deve possuir a habilidade de detectar e analisar os seguintes protocolos e aplicavos: P2P, SMTP, POP3, IRC, DNS, HTTP, FTP, TFTP, SMB, MSN, AIM, YMSG, Yahoo Mail, Hotmail, RDP, DHCP, TELNET, File Transfer, VNC, Cisco-TELNET, Kerberos, DCE-RPC, SQL, HTTPS, SMB2, MMS, IMAP4, RTSP/RTP-UDP, RTSP/RTP-TCP, RTSP/RDT-UDP, RTSP/RDT-TCP, WMSP, SHOUTCast, RTMP, Bi orent, Kazaa, Blubster, eDonkeyeMule, Gnucleus LAN, Gnutella/Limewire/Bearshare/Shareaza, Winny, WinMX, MLDonkey, DirectConnect, SoulSeek, OpenNap, Kuro, iMesh, Skype, Google Talk, Zultrax, Foxy, eDonkey, Ares, Miranda, Kceasy, MoodAmp, Deepnet

Explorer, FreeWire, Gimme, GnucDNA GWebCache, Jubster, MyNapster, Nova GWebCache, Swapper GWebCache, Xnap, Xolox, Ppstream, AIM Express, Chikka SMS Messenger, eBuddy, ICQ2Go, ILoveIM Web Messenger, IMUni ve, mabber, meebo, Yahoo Web Messenger, GPass, IP, ARP, TCP, UDP e IGMP;

5.2.1.25. Deve possuir capacidade de disponibilizar facilmente as amostras dos arquivos suspeitos detectados e do arquivo PCAP do contexto de captura;

5.2.1.26. Capacidade de oferecer informações para análise forense de artefatos suspeitos de serem maliciosos;

5.2.1.27. Gerenciamento centralizado de todas as etapas dos eventos de segurança identificados como possíveis ameaças;

5.2.1.28. Capacidade de identificar artefatos maliciosos direcionados para dispositivos móveis rodando o sistema operacional Android, tais como smartphones e tablets;

5.2.1.29. Deve analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos PDF´s, executáveis, PPT, DOC, XLS, ZIP e RAR;

5.2.1.30. Deve analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos PDF´s, executáveis, PPT, DOC, XLS, ZIP e RAR;

5.2.1.31. A solução deve detectar ameaças do dia zero, vulnerabilidade, URL's maliciosas e spams dirigidos no protocolo SMTP;

5.2.1.32. Deve possuir tecnologia de análise de arquivos binários através de simulação e avaliação de execução dos artefatos suspeitos para identificação de comportamento malicioso, com capacidade de operar vários ambientes simultâneos e integrados a solução para processamento de alto desempenho;

5.2.1.33. Deve permitir o uso de base de conhecimento na Internet do próprio fabricante para correlacionamento de informações sobre ameaças conhecidas e prover recomendações de ações;

5.2.1.34. Deve permitir o rastreio por malwares utilizando métodos de detecção baseados no po de arquivo (True File Type), múlplas camadas de empacotamento (Mul-packed/Mul-layered files) e arquivos comprimidos (compactados);

5.2.1.35. Deverá analisar arquivos maliciosos na rede ulizando vacinas e técnicas de heurísca;

5.2.1.36. Deve possuir foco em proteção contra APTs (Advanced Persistent Threats);

5.2.1.37. Deve possuir tecnologia de proteção contra ameaças desconhecidas (ataques dirigidos e ameaças de dia zero), sendo que este módulo deve pertencer ao mesmo fabricante;

5.2.1.38. Deverá possuir suporte para monitorar múltiplas interfaces de rede conectadas a diferentes VLANs ou Switches;

5.2.1.39. Deverá possuir suporte para balanceamento de carga no sensor de inspeção de tráfego, possibilitando assim obter uma melhor performance;

5.2.1.40. Deverá permitir a análise específica de eventos de segurança de computadores suspeitos de atividade maliciosa;

5.2.1.41. Os módulos que compõem a solução devem atuar de forma integrada, centralizando logs de incidentes em ponto único;

5.2.1.42. Deve possuir atualização automática de regras e assinaturas, sendo que estas devem ser disponibilizadas via web pelo fabricante da solução;

5.2.1.43. Deve possuir mecanismo de consultas automáticas em bases de reputação externas de propriedade do fabricante da solução;

5.2.1.44. Deve ser capaz de identificar movimentos laterais em uma rede corporativa;

5.2.1.45. Deve atuar de forma passiva na captura de tráfego sem oferecer impacto no desempenho da rede;

5.2.1.46. Deve possuir interface web para busca e investigação local de incidentes;

5.2.1.47. Deve possuir capacidade de envio de artefatos para analisador virtual dedicado, externo, sendo que este deverá suportar no mínimo os sistemas operacionais Windows XP e Windows 7;

5.2.1.48. Deve possuir possibilidade de habilitação e desabilitação de regras de inspeção, individualmente, através de interface de gerenciamento web;

5.2.1.49. Deve possuir capacidade de análise virtual de artefatos internamente;

5.2.1.50. Deve possuir regras que identifiquem comunicações dos seguintes tipos: C&C, Exploits, Executáveis Maliciosos, Comunicação com Sites Maliciosos, backdoors e Botnets;

5.2.1.51. Deve possuir regras que identifiquem comunicações de estações de trabalho e servidores com serviços não autorizados, tais como: consultas DNS em servidor não autorizado, utilização de SMTP server não autorizado, Proxy Server não autorizado;

5.2.1.52. Deve possuir regras que identifiquem comunicações P2P, instant messengers e streaming;

5.2.1.53. Deve possuir capacidade de geração de relatórios dos seguintes tipos e contendo as seguintes características:

5.2.1.53.1. Resumidos;
5.2.1.53.2. Visão Geral dos Incidentes de Segurança;
5.2.1.53.3. Discriminação dos Tipos de Incidentes;
5.2.1.53.4. Top Ameaças Analisadas;
5.2.1.53.5. Top Hosts Infectados;
5.2.1.53.6. Recomendações de Segurança;
5.2.1.53.7. Executivos.

5.2.1.54. Deve possuir detalhes técnicos dos incidentes detectados;

5.2.1.55. Deve possuir estatística do tráfego analisado;

5.2.1.56. Deve possuir indicadores de risco do ambiente;

5.2.1.57. Recomendações de Segurança;

5.2.1.58. Deve ser capaz de identificar, filtrar e exibir em interface gráfica, e dinamicamente atualizada, hosts com alto nível de risco, classificando os tipos de riscos/eventos detectados;

5.2.1.59. Deve possuir interface que apresente em Real Time estatísticas de top ameaças detectadas, top arquivos analisados, top hosts afetados, top URL's maliciosas acessadas, etc.;

5.2.1.60. Quando detectada uma ameaça, a solução deve prover, podendo esta realizar consultas em site do fabricante, informações sobre ameaça, família da ameaça, estatísticas de segmentos de mercado afetados e recomendações de segurança para eliminar ameaça, correlacionando estas informações com sites ou outros vetores por onde esta ameaça é disseminada;

5.2.1.61. As atualizações do produto (patterns e outros componentes) não devem causar downtime ou impacto na operação;

5.2.1.62. Deve possibilitar customização de Sandbox, permitindo ao cliente simular seu padrão de imagens e sistemas operacionais no módulo de análise virtual;

5.2.1.63. Deve ser capaz de identificar ameaças que afetam dispositivos móveis (Ex. Detecção de comunicação de aplicativo malicioso na plataforma Android);

5.2.1.64. Deve ser capaz de detectar tentativas de mascaramento ou evasão de detecção através do uso de portas comuns ou protocol tunneling;

5.2.1.65. Deve ser capaz de detectar tentativas de scan de rede;

5.2.1.66. Deve ser capaz de detectar propagação de malwares na rede;

5.2.1.67. Deve ser capaz de detectar tentativas de brute-force;

5.2.1.68. Deve ser capaz de detectar tentativas de fuga e roubo de informação;

5.2.1.69. Deve ser capaz de detectar ameaças que se replicam na rede;

5.2.1.70. Deve ser capaz de detectar Exploits na rede;

5.2.1.71. O Monitoramento de protocolos de comunicação deve ser feito através de appliance único (ou virtual appliance);

5.2.1.72. A console de gerenciamento deve possuir mapa mundial, onde são marcadas origens de ataques e eventos de segurança monitorados pela solução;

5.2.1.73. Deve permitir busca por informações do destino e origem, incluindo estas: endereço IP, endereço MAC, porta e protocolo;

5.2.1.74. Deve permitir consultas personalizáveis, usando comandos SQL ou atributos pré-definidos;

5.2.1.75. Capacidade de salvar uma investigação antes de ser finalizada;

5.2.1.76. Capacidade de restaurar uma investigação para continuá-la ou consultá-la;

5.2.1.77. Capacidade de emitir relatórios baseados nas investigações;

5.2.1.78. Deve permitir apresentação dos dados consultados em vários formatos, incluindo tabela e gráficos;

5.2.1.79. Deve trabalhar com geolocalização para identificar a origem geográfica de um ataque;

5.2.1.80. Deve ter a capacidade de sugerir termos de busca, de acordo com o conteúdo já buscado numa investigação, para agilizar a obtenção do resultado;

5.2.1.81. Deve permitir exportar sob demanda os logs em texto puro (CSV ou similar);

5.2.1.82. Deve sugerir consultas a bases de reputação e whois quando encontrados hosts e nomes de domínio;

5.2.1.83. Deve permitir investigação por tags (palavras-chave) pré-configuradas para facilitar a busca de eventos;

5.2.1.84. Deve permitir investigação por tags (palavras-chave) pré-configuradas para facilitar a busca de eventos;

5.2.1.85. Deve permitir recebimento de logs via syslog;

5.2.1.86. Deve permitir encaminhamento de logs via syslog;

5.2.1.87. Deve permitir receber logs de diferentes dispositivos;

5.2.1.88. Deve possuir engine de correlação de eventos;

5.2.1.89. Deve inserir tags personalizadas nos logs, de acordo com regras especificadas pelo usuário;

5.2.1.90. Deve enviar alertas via e-mail para pelo menos 100 e-mails diferentes;

5.2.1.91. Deve permitir a configuração de alarmes personalizados, com base em investigações;

5.2.1.92. Deve informar em sua console alarmes que dispararam, até que o usuário tome alguma ação.

5.3. Características do Módulo de Análise Virtual

5.3.1. Deve suportar análise de documentos do Microsoft Office (DOC, DOCX, XLS, XLSX, PPT, PPTX);

5.3.2. Deve suportar análise de documentos em PDF;

5.3.3. Deve submeter um documento PDF a pelo menos duas versões do Adobe Reader;

5.3.4. Deve analisar dinamicamente arquivos compactados (ZIP, BZIP2, RAR);

5.3.5. Deve analisar dinamicamente binários PE de 32-bits;

5.3.6. Deve analisar dinamicamente binários PE de 64-bits;

5.3.7. Deve permitir criação de sandbox personalizada pelo usuário;

5.3.8. Deve permitir criação de sandbox utilizando Windows XP 32-bits em inglês e português;

5.3.9. Deve permitir criação de sandbox utilizando Windows 7 em inglês e português;

5.3.10. Deve permitir criação de sandbox utilizando Windows 8 em inglês e português;

5.3.11. Deve permitir criação de sandbox utilizando Windows 8.1 em inglês e português;

5.3.12. Deve permitir criação de sandbox utilizando Windows 10 em inglês e português;

5.3.13. Deve permitir criação de sandbox utilizando Windows 2003/2003 R2 em inglês e português;

5.3.14. Deve permitir criação de sandbox utilizando Windows 2008/2008 R2 em inglês e português;

5.3.15. Deve permitir criação de sandbox utilizando Windows 2012/2012 R2 em inglês e português;

5.3.16. Deve permitir criação de sandbox utilizando Windows 2016 em inglês e português;

5.3.17. Deve analisar dinamicamente bibliotecas dinâmicas (DLL);

5.3.18. Deve analisar dinamicamente binários BHO;

5.3.19. Deve poder funcionar em ambiente totalmente virtualizado;

5.3.20. Deve possuir tecnologia própria de análise de artefatos em sandboxing;

5.3.21. Deve prover possibilidade de isolamento total da rede de sandbox da rede de gerência;

5.3.22. Deve prover possibilidade de isolamento total da rede de uso da rede dedicada para a internet na análise de sandbox;

5.3.23. Deve analisar dinamicamente arquivos do Adobe Flash (SWF);

5.3.24. Deve realizar a análise localmente podendo ter consultas externas para reputação de IP e URL, mas sem envio da amostra;

5.3.25. Deve ter a capacidade de gerar relatórios com eventos realizados pela amostra no sistema alvo, ao nível de API, exibindo as funções com argumentos e retornos de execução;

5.3.26. Deve analisar dinamicamente rootkits;

5.3.27. Caso uma ameaça baixe outra enquanto na sandbox, essa também deverá ser analisada num evento correlacionado;

5.3.28. Deve submeter uma amostra a sistemas operacionais diferentes, a fim de detectar ações específicas para um sistema;

5.3.29. Capacidade de integração via API com soluções terceiras;

5.3.30. O Fabricante deverá disponibilizar acesso a base de dados externa que possibilite a correlação entre informações geradas no ambiente com informações de outros clientes que foram afetados pelo mesmo padrão ou tipo de ameaça. Este acesso deverá ser web, e deverá possuir referências e atalhos nos próprios relatórios e logs locais da solução.

5.4. Características da Console de Gerenciamento da Solução de Proteção contra Ameaças Avançadas

5.4.1. A console de gerenciamento deverá ser web, apresentando alta disponibilidade de modo que na ausência da principal, o restante da solução permaneça ativa e funcionando;

5.4.2. A solução deve ser escalável horizontalmente, permitindo que novas instâncias sejam habilitadas, aumentando suas capacidades de detecção e análise;

5.4.3. A console de gerenciamento deverá ter dashboards para facilidade de monitoração. As janelas deverão ser customizadas pelo administrador em quantidade e período de monitoração;

5.4.4. O administrador deve poder optar por janelas de monitoramento no dashboard a sua disposição e poderá livremente adicionar ou remover de acordo com sua necessidade de visualização;

5.4.5. Deverá possuir mapa geográfico que permita a identificação visual sobre a origem de ameaças de modo a facilitar a visualização de eventos críticos para que ações imediatas sejam providenciadas;

5.4.6. Deverá possuir a capacidade de atualizar as vacinas, engines, assinaturas e recursos de inspeção de conteúdo de forma agendada e automática;

5.4.7. A console de gerenciamento deverá ser gerenciada por Internet Explorer e Firefox;

5.4.8. Solução deverá ter mecanismo de busca em sua console de gerenciamento de modo que seja facilitada a busca por detecções;

5.4.9. Deverá ser capaz de identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques;

5.4.10. Deverá possuir capacidade de identificar a origem de ataques direcionados, incluindo a análise de artefatos por meio de analisador virtual com a capacidade de gerar no mínimo 24 máquinas virtuais de análise;

5.4.11. Deverá ser capaz de correlacionar regras de detecção de conteúdo malicioso durante todas as fases de um ataque.

5.4.12. Deverá permitir a adição e remoção dos diversos recursos de visualização de informações na tela principal de monitoramento da ferramenta, permitindo no mínimo a visualização das seguintes informações;

5.4.12.1. Uso de CPU;
5.4.12.2. Uso de Disco;
5.4.12.3. Uso de Memória;
5.4.12.4. Tráfego malicioso analisado;
5.4.12.5. Todo o tráfego analisado.

5.5. Logs e Relatórios da Solução de Proteção Contra Ameaças Avançadas

5.5.1. A solução deverá permitir o envio de logs dos recursos para servidor de logs por meio do protocolo syslog e deverá conter no mínimo:

5.5.1.1. Tipo de evento de detecções: Conteúdo malicioso, reputação de URL's, comportamentos maliciosos, comportamentos suspeitos, Exploits, correlações de eventos, Grayware;

5.5.1.2. Tipo de eventos de sistemas: Eventos de sistema e eventos de atualizações.

5.5.2. A solução deverá ter integração com ferramentas de SIEM;

5.5.3. Deve possuir capacidade de entregar relatório contendo informações da sequência de execução do artefato malicioso, assim como, detalhes de alterações locais da máquina, conexões externas e envio da informação para fora da rede corporativa;

5.5.4. A solução deve prover serviço de agregação e correlação de logs de eventos de segurança possibilitando coleta de fontes de monitoração para proporcionar informação e identificação de ameaças digitais conhecidas e desconhecidas em trânsito através de logs de sensor;

5.5.5. Solução deverá apresentar relatórios customizados de todas as suas funcionalidades e deverá conter no mínimo:

5.5.5.1. Computadores infectados;

5.5.5.2. Origem de infecções;

5.5.5.3. Estatísticas de ameaças;

5.5.5.4. Riscos potenciais de segurança;

5.5.5.5. Riscos de perda de informações;

5.5.5.6. Risco de sistema comprometido;

5.5.5.7. Risco de disseminação de ameaças;

5.5.5.8. Eventos suspeitos;

5.5.5.9. Infecções de malware.

5.5.6. A solução deverá apresentar função de pesquisa por logs contendo no mínimo:

5.5.7. Critérios de pesquisa por dia, mês e ano;

5.5.8. Possibilidade de pesquisa pelo nome do computador, domínio ou conta, endereço IP, endereço MAC e grupos;

5.5.9. Possibilidade de pesquisa por ameaças, URL's maliciosas, análises virtuais, correlação de incidentes, nome de malware, protocolo e direção da detecção;

5.5.10. Os relatórios e logs deverão ser exportados nos formatos PDF ou CSV.

5.6. Gerenciamento centralizado para todos os itens

5.6.1. A solução de gerenciamento centralizado deve permitir a integração com a solução de segurança para proteção de estações de trabalho (desktops e notebooks), com todos os seus módulos, solução de anti-spam e solução contra ameaças avançadas;

5.6.2. Instalação do servidor na plataforma Windows 2012 Server ou superior, seja o servidor físico ou virtual;

5.6.3. Suportar base de dados Microsoft SQL;

5.6.4. Deve gerenciar logs das atividades e eventos gerados pela solução;

5.6.5. Deve possuir integração com Microsoft Active Directory;

5.6.6. Deve permitir níveis de administração por usuários ou grupos de usuários;

5.6.7. Deve permitir a constituição de políticas genéricas aplicáveis a grupos de máquinas, ou aplicáveis a grupos de usuários;

5.6.8. Deve disponibilizar sua interface através dos protocolos HTTP e HTTPs;

5.6.9. Deve permitir a alteração das configurações das ferramentas ofertadas, de maneira remota;

5.6.10. Deve permitir diferentes níveis de administração, de maneira independente do login da rede;

5.6.11. Geração de relatórios e gráficos e parametrizáveis nos formatos html, pdf, xml e csv;

5.6.12. Deve gerar relatórios e gráficos pré-definidos nos formatos r, pdf, ActiveX e crystal report (*.rpt);

5.6.13. Deve permitir criação de modelos de relatórios customizados;

5.6.14. Deve permitir logon via single sign-on com os demais produtos da solução;

5.6.15. Deve permitir a atualização de todos os componentes de todos os módulos gerenciados;

5.6.16. Deve permitir a criação de planos de entrega das atualizações, com hora de início ou postergação da entrega após o download dos componentes;

5.6.17. Deve permitir o controle individual de cada componente a ser atualizado;

5.6.18. Deve permitir a definição de exceções por dias e horas para não realização de atualizações;

5.6.19. Deve permitir ter como fonte de atualização um compartilhamento de rede no formato UNC;

5.6.20. Deve gerar relatórios e gráficos com o detalhamento das versões dos produtos instalados;

5.6.21. Deve possuir o acompanhamento dos comandos administrativos em execução, tal como seu status de conclusão, alvo e usuário;

5.6.22. Deve permitir a configuração dos eventos administrativos ou de segurança que geram notificações, tal como o método de envio e o destinatário;

5.6.23. Os métodos de envio suportados devem incluir: e-mail, gravação de registros de eventos do Windows, SNMP e SYSlog;

5.6.24. Deve permitir a configuração do intervalo de comunicação com os módulos gerenciados;

5.6.25. Deve permitir a escolha do intervalo de tempo necessário para que um módulo seja considerado fora do ar (off-line);

5.6.26. Deve permitir o controle do intervalo de expiração de comandos administrativos;

5.6.27. Deve possuir a configuração do tempo de expiração da sessão dos usuários;

5.6.28. Deve permitir a configuração do número de tentativa inválidas de login para o bloqueio de usuários;

5.6.29. Deve permitir a configuração da duração do bloqueio;

5.6.30. Deve permitir pesquisas personalizadas para a consulta de eventos (logs) através de categorias;

5.6.31. Deve permitir pesquisas personalizadas para a consulta de eventos (logs), através de critérios lógicos, com base em todos os campos pertencentes aos eventos consultados;

5.6.32. Deve permitir a configuração das informações que não são enviadas dos módulos à solução de gerenciamento centralizado;

5.6.33. Deve permitir a configuração da manutenção dos registros de eventos (logs), com base no intervalo de tempo que devem ser mantidos e no número máximo de registros, por tipo de evento;

5.6.34. Deve permitir a criação de políticas de segurança personalizadas;

5.6.35. As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:

5.6.35.1. Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;

5.6.35.2. Range de endereços IPS;

5.6.35.3. Sistema operacional;

5.6.35.4. Agrupamento lógicos dos módulos.

5.6.36. As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;

5.6.37. Deve permitir visualização de eventos de violação de segurança de todos os módulos gerenciados, agrupado por usuário numa linha de tempo, configurável;

5.6.38. Deve permitir a gerência dos módulos baseados no modelo de nuvem (cloud), quando existentes;

5.6.39. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

5.6.40. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

5.6.41. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

5.6.42. Deve possuir repositório central de identificadores de dados, que podem ser utilizados para a criação de políticas contra possíveis vazamentos de informações;

5.6.43. Deve permitir a investigação de incidentes de vazamento de informação através de um número identificador de incidentes.

5.7. Pacote de Horas de Instalação (40 horas)

5.7.1. Os softwares de solução de segurança a serem instalados no TJPA deverão ser configurados em equipamentos (estações de trabalho e servidores) fornecidos pela CONTRATANTE;

5.7.2. Caberá à CONTRATADA a implantação da solução sob o acompanhamento da CONTRATANTE;

5.7.3. No que tange ao processo de implantação da solução, a CONTRATADA deve apresentar um cronograma para a implantação e seguir as atividades tomando como base o seguinte escopo do serviço:

5.7.3.1. Planejamento da instalação incluindo identificação de pré-requisitos;

5.7.3.2. Instalação e configuração do módulo de gerenciamento central;

5.7.3.3. Criar a senha de acesso com privilégio administrativo para o Tribunal de Justiça do Estado do Pará.

5.7.3.4. Instalação e configuração do software de endpoint protection em pelo menos 10 (dez) equipamentos;

5.7.3.5. Realizar customizações caso sejam solicitadas ou necessárias;

5.7.3.6. Realizar testes e apresentar os resultados que comprovem a correta e completa implantação da solução;

5.7.3.7. Realizar backup das configurações;

5.7.3.8. Documentar todas as configurações realizadas no ambiente.

5.7.4. Após a conclusão da instalação e implantação, a solução deverá ser formalmente homologada pela Coordenadoria de Suporte Técnico (CST), pertencente a Secretaria de Informática do TJPA, o qual possuirá o prazo de 5(cinco) dias consecutivos contados a par□r da data de conclusão do serviço de instalação e configuração contratado, para emitir o relatório de homologação (aceite).

5.8. Treinamento (Hands-on) (40 horas)

5.8.1. A CONTRATADA deverá ministrar treinamento on-site do tipo prático cobrindo todos os softwares inclusos na suíte de solução de segurança;

5.8.2. O conteúdo do treinamento deve abordar os assuntos de natureza teórica e prática, abrangendo todos os módulos envolvidos na solução de segurança em seus aspectos mais relevantes;

5.8.3. O treinamento pode ser separado conforme o produto a ser instalado no ambiente do Tribunal de Justiça do Estado do Pará, contendo ao menos os seguintes módulos:

5.8.3.1. Instalação do módulo de gerenciamento central;

5.8.3.2. Instalação do software de endpoint protection em estações de trabalho e servidores;

5.8.3.3. Descrição e configuração de todas as funcionalidades contratadas da solução;

5.8.3.4. Resolução de problemas **–** troubleshooting;

5.8.3.5. Melhores práticas u□lizadas no mercado para aproveitamento dos softwares e suas funcionalidades.

5.8.4. A carga horária mínima será de 16 horas divididas em expedientes de 4h/dia, das 9h às 13h;

5.8.4.1. O treinamento terá um total de cinco (5) participantes definidos pelo Tribunal de Justiça do Estado do Pará;

5.8.4.2. O material didático fornecido deve abordar todos os tópicos do curso;

5.8.4.3. A CONTRATADA deverá fornecer apostilas em formato digital que incluam o conteúdo referente ao produto;

5.8.4.4. É de responsabilidade da contratante a disponibilização de instalações físicas para a realização do treinamento;

5.8.4.5. Após a conclusão, o serviço de treinamento deverá ser formalmente homologado pelo Tribunal de Justiça do Estado do Pará, o qual possuirá o prazo de 5 (quinze) dias consecutivos contados a partir da data de conclusão do treinamento contratado, para emitir o relatório de homologação (aceite).

6. PROPOSTA DE MODELOS A SEREM UTILIZADOS

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

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

Deverá constar, obrigatoriamente, na proposta:

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

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

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

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

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

7. INFORMAÇÕES COMPLEMENTARES

Não há

Belém, 02 de dezembro de 2022

(ASSINATURA DOS MEMBROS DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO)