TERMO DE REFERÊNCIA

Contratação de solução de análise e proteção avançada de vulnerabilidades em equipamentos servidores (*Deep Security)* e em equipamentos de microinformática (*Smart Protection for Endpoint)*, incluindo garantia, suporte especializado, corretivo e preventivo pelo período de 24 meses

PROCESSO ADMINISTRATIVO PA-PRO-2021/01602

1. 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, conforme especificações e quantidades previstas no termo de referência, para atender as necessidades do Tribunal de Justiça do Estado do Pará.

2. DA FUNDAMENTAÇÃO

2.1. Da motivação

É crescente a preocupação com ataques cibernéticos que causam prejuízos dos mais diversos tipos a instituições públicas e privadas, sendo de extrema importância que o TJPA disponha de um conjunto de ferramentas e práticas que visem aumentar o grau de prevenção contra estes ataques, protegendo a imagem da instituição perante a sociedade paraense e os dados gerados e confiados ao Tribunal.

Uma solução de *deep security* e de *endpoint* é uma ferramenta fundamental para contribuir na proteção da infraestrutura de servidores e dos equipamentos de microinformática que compõem o parque computacional do Tribunal, onde dados sensíveis referentes a atividade institucional desempenhada pelo TJPA são utilizados diariamente, e na maioria das vezes, não é possível realizar uma política de atualizações e correções de vulnerabilidades nestes ativos.

Por reconhecer a criticidade de servidores de datacenter que hospedam serviços e sistemas como PJe, Libra, PROJUDI, SEEU, dentre vários outros, muitas vezes não havendo janela de tempo para corrigir vulnerabilidade e aplicar correções referentes ao sistema operacional, servidor de aplicação ou mesmo ao próprio serviço ou sistema hospedado na infraestrutura de TI do Tribunal.

2.2. Dos objetivos a serem alcançados por meio da contratação

Realizar a aquisição de uma solução de análise e proteção avançada de vulnerabilidades em equipamentos servidores (*Deep Security)* para 350 servidores que compõem a infraestrutura de TI do Tribunal, e em equipamentos de microinformática (*Smart Protection for Endpoint)* para 6000 estações de trabalho, entre computadores e notebooks, incluindo garantia, suporte especializado, corretivo e preventivo pelo período de 24 meses.

2.3. Dos benefícios diretos e indiretos resultantes da contratação

Ao realizar esta contratação, o TJPA avançará mais uma etapa na construção de um ecossistema de segurança que irá abranger equipamentos de microinformática, rede de computadores, infraestrutura e sistemas utilizados pelo Tribunal, ao aplicar camadas de proteção ativa nos computadores utilizados por magistrados e servidores e também nos servidores que hospedam sistemas e serviços essenciais para o Tribunal, permitindo que a equipe de TI possa ter mais tempo para trabalhar na correção de falhas e vulnerabilidades que possam vir a existir no parque computacional do TJPA.

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

A contratação está alinhada ao Macrodesafio 12 (Fortalecimento da Estratégia Nacional de TIC e Proteção de Dados) prevista no Plano de Gestão 2021-2023 do TJPA, além de estar alinhada ao Plano de Contratações de Soluções de TIC 2021 do Tribunal e prevista no plano orçamentário de 2021 do TJPA, atendendo ao objetivo estratégico de modernização da infraestrutura de TIC do TJPA.

2.5. Da referência aos Estudos Preliminares

Os estudos preliminares foram protocolados no sistema SigaDoc através do PA-PRO-2021/01602.

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

Entende-se que as demandas previstas e projetadas pela Secretaria de Informática do TJPA a serem atendidas pela contratação da solução de segurança de perímetro, serão cobertas em sua plenitude, durante o período de vigência de 24 meses, através do contrato estabelecido entre o CONTRATANTE e a CONTRATADA. Abaixo estão elas listadas:

Item	Descrição	QTD
1	Subscrição de software de segurança para endpoints, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses.	6000
2	Subscrição de software de segurança para servidores, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses.	350
3	Serviço de Suporte Especializado para Instalação, Migração e Suportes corretivo e preventivo para 24 (vinte e quatro) meses.	1

2.7. Da análise de mercado de TIC

Sendo uma solução comum de mercado, existem diversos fabricantes que podem oferecer soluções de segurança de perímetro, com diferentes graus de qualidade e diversos preços a serem pagos. Sendo inviável avaliar todas as opções disponíveis, recorreu-se ao Gartner e ao Forrester Wave, empresas referências na área de consultoria em soluções de Tecnologia da Informação, para delimitar as melhores opções a serem consideradas.

Para a solução de análise e proteção avançada de vulnerabilidades para equipamentos de microinformática (*Smart Protection for Endpoint*), o Gartner possui um "quadrante", publicado anualmente, onde são utilizados diversos critérios para avaliar a qualidade das soluções. Como o Tribunal preza pela qualidade das soluções adquiridas para compor sua infraestrutura tecnológica, as soluções consideradas foram as que se enquadram no quadrante "*Leaders*" do quadrante mais recente, publicado em maio/2021. Os fabricantes localizados neste quadrante foram avaliados com os melhores resultados em suas soluções oferecidas.

Figure 1: Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (May 2021)

Ao que podemos verificar no quadrante do Gartner, existem diversos fabricantes líderes em soluções de endpoint como Microsoft, CrowdStrike e Trend Micro.

Para a solução de análise e proteção avançada de vulnerabilidades para equipamentos servidores (*Deep Security*), o Forrester Wave possui também um "quadrante", onde são utilizados diversos critérios para avaliar a qualidade das soluções. Como o Tribunal preza pela qualidade das soluções adquiridas para compor sua infraestrutura tecnológica, as soluções consideradas foram as que se enquadram no quadrante "*Leaders*" do quadrante mais recente, publicado em 2019. Os fabricantes localizados neste quadrante foram avaliados com os melhores resultados em suas soluções oferecidas.

Ao que podemos verificar no quadrante do Forrester Wave, existem três fabricantes líderes em soluções de *deep security*, como Bitdefender, McAfee e Trend Micro.

Em virtude da urgência em aplicar as referidas camadas de proteção nos equipamentos de microinformática e nos equipamentos servidores, hoje inexistente na infraestrutura do Tribunal, devido aos recentes ataques cibernéticos executados contra órgãos do Poder Judiciário, sendo uma solução líder de mercado e possuindo disponibilidade imediata para contratação do quantitativo necessário através de ARP (Ata de Registro de Preço), foi escolhida a solução da fabricante Trend Micro.

Pelo fato do objeto da contratação ser um elemento essencial para contribuir na garantia da segurança da informação no âmbito da administração pública, diversos órgãos dos mais variados tamanhos e com a mais diversas funções o possuem em sua infraestrutura de TI. As aquisições mencionadas abaixo, guardadas as peculiaridades de cada órgão, são similares ao objeto que o TJPA pretende adquirir.

Destaca-se a Defensoria Pública do Estado do Pará (DPEPA) que, 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 Secretaria de Estado de Educação do Piauí (SEDUC-PI), como partícipe do Pregão Eletrônico 003/2021, realizado pela Defensoria Pública do Estado do Pará (DPEPA), também registrou preços, através da Ata de Registro de Preço (ARP) nº 004/2021, para o mesmo objeto citado acima.

A Secretaria de Estado de Educação de Rondônia (SEDUC-RO), através da Ata de Registro de Preço (ARP) nº 213/2019 gerada no Pregão Eletrônico 290/2019, registrou preços para aquisição do objeto "Aquisição de serviços de segurança para proteção de e-mail, *endpoint* e proteção".

Na medida em que as soluções oferecidas pelos fabricantes classificados como líderes nos quadrantes do Gartner e do Forrester Wave, de acordo com o subitem 1.3, b, foram avaliadas pela Secretaria de Informática

do Tribunal e confirmadas que atendem aos padrões técnicos e de confiabilidade exigidos, além da solução que oferecer o menor preço total.

Foi avaliado também a possibilidade da aderir a atas de registro de preço ou realizar procedimento licitatório para adquirir o objeto da contratação. Em virtude do grande impacto que poderia ser gerado para os magistrados e servidores do Tribunal devido a ataques cibernéticos que estão se tornando cada vez mais comuns no Poder Judiciário e a crescente necessidade de acrescentar maior proteção para os equipamentos de microinformática e equipamentos servidores, reconhecida a urgência na proteção desses ativos e avaliando-se sempre o que seria mais vantajoso para o Tribunal em termos de qualidade da solução e preço a ser pago, optou-se pela adesão a uma ARP (Ata de Registro de Preço).

Por ter mostrado um valor abaixo da média das propostas pesquisadas, estar disponível para imediata adesão e atender objetivamente ao objeto da contratação, escolheu-se aderir aos itens 1, 4 e 7 da ata 004/2021//DPEPA, resultante do Pregão Eletrônico 003/2021/DPEPA.

2.8. Da natureza do objeto

Os itens que compõem a solução que é objeto da contratação possuem características comuns de mercado, conforme o parágrafo único do artigo 1º da lei que institui o pregão eletrônico (Lei 10.520/2002).

"Parágrafo único. Consideram-se bens e serviços comuns, para os fins e efeitos deste artigo, aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado."

2.9. Do parcelamento do objeto

Apesar de haver um nível de parcelamento da solução, composta pelos itens que compõem a aquisição da solução de *deep security* e *smart protection for endpoint*, estes itens devem ser fornecidos por um único fabricante, pois o licenciamento, suporte e garantia necessitam ser compatíveis entre si e não funcionam de forma independente, portanto não podendo ser separados, sob vista de impedir o pleno funcionamento da solução.

2.10. Da seleção do fornecedor

Os itens a seguir estão estabelecidos de acordo com os princípios da legalidade, razoabilidade e competitividade.

2.10.1. Da forma e do critério de seleção

A adjudicação do objeto contratado deve ser realizada por item e com a empresa detentora da ARP (Ata de Registro de Preço) nº 004/2021/DPEPA, resultante do Pregão Eletrônico nº 003/2021/DPEPA, que será feita a adesão.

2.10.2. Da modalidade e do tipo de licitação

A aquisição da solução de análise e proteção avançada de vulnerabilidades será realizada através de adesão a ARP (Ata de Registro de Preço) nº 004/2021/DPEPA, resultante do Pregão Eletrônico nº 003/2021/DPEPA, devido a ata ter se mostrado vantajosa do ponto de vista financeiro e atender, de forma objetiva, as necessidades do Tribunal, no que diz respeito ao objeto da contratação.

2.10.3. Dos critérios técnicos de habilitação obrigatórios

Os requisitos de habilitação serão definidos junto ao edital e nos termos da legislação vigente.

Quanto a habilitação técnica, temos:

- Será requerida das empresas licitantes, para fins de habilitação, a comprovação do pleno atendimento a partir de apresentação de comparativo Ponto-a-ponto referente aos itens licitados.

- Será requerida das empresas licitantes, para fins de habilitação, a comprovação de aptidão para a prestação dos serviços em características técnicas compatíveis com o objeto desta licitação, mediante a apresentação de:
- Atestado(s) de capacidade técnica, emitido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove(m) ter fornecido ou estar fornecendo pelo menos 30% do quantitativo de softwares compatíveis em características e prazos de cada item do objeto da licitação;
- Não será definido um quantitativo mínimo aceitável para ampliar a competitividade do certame e consequentemente, obter preços mais vantajosos em meio a possibilidade de participação de um número maior.
- Declaração informando se a licitante é a fabricante, revendedora ou distribuidora autorizada do fabricante, ou ainda, revendedora autorizada de distribuidor autorizado pelo fabricante dos produtos. Caso a licitante não possua uma das qualificações exigidas anteriormente, deverá ser apresentada declaração do próprio licitante de que a aquisição dos softwares, objeto desse edital, será realizada através de um canal do fabricante, para softwares especificados pelo fabricante para uso no Brasil.
- Tais declarações deverão ser emitidas em papel timbrado, com assinatura, identificação e telefone do emitente.
- Admite-se mais de um atestado com vistas a comprovar o atendimento a todos os requisitos de capacidade técnica que asseguram a similaridade do objeto.
- A licitante disponibilizará todas as informações necessárias à comprovação da legitimidade do(s) atestado(s).
- A comprovação de capacidade deverá ser realizada por meio de atestado ou conjunto de atestados que totalizados atendam aos critérios exigidos.
- No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados válidos aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da licitante. Serão consideradas como pertencentes ao mesmo grupo empresarial as empresas controladas ou controladoras da empresa licitante, e ainda as que tenham pelo menos uma pessoa física ou jurídica como sócia em comum.
- O CONTRATANTE reserva-se o direito de realizar diligências, a qualquer momento, com o objetivo de verificar se o(s) atestado(s) e demais documentos são adequados e atendem às exigências contidas neste Termo de Referência, podendo exigir apresentação de documentação complementar referente à prestação de serviços relativos aos atestados apresentados.
- Caso a licitante não comprove as exigências do Edital por meio das documentações requeridas, será desclassificada.
- O pregoeiro examinará a proposta classificada em primeiro lugar quanto à compatibilidade do preço em relação ao estimado para a contratação, de acordo com as exigências do Edital.

Prova de Conceito:

- A licitante melhor classificada será convocada para realizar a Prova de Conceito – POC, com vistas a demonstrar que a solução ofertada atende os requisitos exigidos.
- A POC somente será realizada para a proponente melhor classificada, não sendo requisito prévio de habilitação.
- Caso a licitante melhor classificada não esteja ofertando uma solução que atenda os requisitos exigidos, ela será inabilitada, passando a convocar as licitantes na ordem de classificação da fase de lances.
- A Prova de Conceito acontecerá em até 03 (três) dias úteis, contados da convocação oficial por parte da Defensoria.
- A Prova de Conceito será realizada nas dependências do Tribunal de Justiça do Estado do Pará - TJPA, no horário acordado entre as partes.
- Qualquer licitante poderá participar da Prova de Conceito, entretanto, será na condição de ouvinte e não poderá se manifestar durante a realização.

- A Prova de Conceito consistirá na comprovação de requisitos técnicos existentes neste Termo de Referência, entretanto, o Tribunal de Justiça do Estado do Pará - TJPA se reserva ao direito de somente divulgar os requisitos que deverão ser comprovados no momento da realização da POC, para evitar que as licitantes preparem a solução somente para passar na Prova de Conceito.
- No momento da realização, a equipe de TI irá anotar em registro próprio, todos os requisitos comprováveis e o seu respectivo atendimento, podendo, inclusive, incluir comprovações.
- Somente com a apresentação do(s) atestado(s) de capacidade técnica, declaração e a Prova de Conceito, a proposta será tecnicamente aceita.

2.11. Do impacto ambiental

Não foram encontrados riscos ambientais significativos, em decorrência do fornecimento dos itens que compõem a contratação de segurança de servidores e proteção de *endpoints*.

2.12. Da conformidade técnica e legal

Não há normas específica para as quais o objeto da contratação deve estar em conformidade.

2.13. Das obrigações

2.13.1. Das obrigações do contratante Sem que a isto limite seus direitos, terá o Tribunal de Justiça do Estado do Pará, as seguintes garantias:

2.13.1.1 Receber o objeto de acordo com o que consta neste instrumento, no edital e nos seus anexos.
2.13.1.2 Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta.
2.13.1.3 Sem que a isto limite sua responsabilidade, será o Órgão responsável pelos seguintes itens:
2.13.1.4 Realizar os pagamentos de acordo com o previsto na competente Nota de Empenho.
2.13.1.5 Prestar as informações e os esclarecimentos que venham a ser solicitados pela Contratada.
2,13.1.6 Indicar FISCALIZAÇÃO com competência necessária para proceder ao recebimento dos objetos licitados e atestar as Notas Fiscais após a verificação das especificações, qualidade, quantidade e preços pactuados.
2.13.1.7 Promover o recebimento do objeto licitado, rejeitando o que estiver em desacordo com o exigido neste Termo de Referência

2.13.2. Das obrigações da contratada

2.13.2.1 Atender a todas as condições descritas no presente Termo de Referência e respectivo Contrato;

2.13.2.2 Manter as condições de habilitação e qualificação exigidas durante toda a vigência do Contrato;

2.13.2.3 Facilitar o pleno exercício das funções da fiscalização. O não atendimento das solicitações feitas pela fiscalização será considerado motivo para aplicação das sanções contratuais. O exercício das funções da fiscalização não desobriga a contratada de sua própria responsabilidade quanto à adequada execução do objeto contratado;

2.13.2.4 Entregar os bens e prestar os serviços de acordo com os requisitos de quantidades, especificações técnicas, manuais de operação (quando couber).

2.13.2.5 Entregar os bens e prestar os serviços, impreterivelmente, no prazo previsto e local designado, conforme especificações constantes da proposta e do Edital e seus Anexos.

2.13.2.6 Não divulgar informações, conceder entrevistas ou qualquer tipo de divulgação na mídia geral sobre projetos do CONTRATANTE sem alinhamento prévio com a diretoria/coordenação a que se reporta. Não utilizar a marca do CONTRATANTE sem alinhamento prévio e autorização deste.

2.13.2.7 Prestar garantia técnica na forma e condições estabelecidas.

2.13.2.8 Indicar, formalmente, observado o art. 68, da Lei n.º 8.666, de 1993, Preposto para acompanhar a execução dos serviços e responder perante a CONTRATANTE.

2.13.2.9 Arcar com todos os encargos diretos e indiretos que incidir sobre a comercialização, instalação, garantia técnica integral, suporte e treinamentos contratados em face da venda dos produtos licitados, inclusive sob eventuais substituições e reposições.

2.13.2.10 Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando forem vítimas os seus profissionais no desempenho dos serviços objeto deste instrumento ou em conexão com eles, ainda que acontecido nas dependências do CONTRATANTE.

2.13.2.11. Pagar os tributos, taxas e encargos de qualquer natureza de sua responsabilidade em decorrência do Contrato;

2.13.2.12. Não ceder ou transferir, total ou parcialmente, parte alguma do contrato. A fusão, cisão ou incorporação só serão admitidas com o consentimento prévio e por escrito do CONTRATANTE;

2.13.2.13. Toda informação referente às Áreas de TI de cada Órgão que a Contratada, seus Prepostos e Técnicos vierem a tomar conhecimento por necessidade de execução dos serviços contratados, não poderá, sob hipótese nenhuma, ser divulgada a terceiros.

2.13.2.14. Assumir todos os custos por eventuais deslocamentos da equipe do CONTRATANTE que porventura se façam necessários para fins de atualização tecnológica, reforço de capacitação, conhecer ambientes laborais com solução similar implantada, laboratórios, fábricas, ou seja, todo e qualquer evento que tenha por finalidade agregar conhecimento e potencializar a solução adquirida por parte da equipe do CONTRATANTE.

2.13.2.15. Não deixar de executar qualquer atividade necessária ao perfeito fornecimento do objeto, sob qualquer alegação, mesmo com pretexto de não ter sido executado anteriormente qualquer tipo de procedimento;

2.13.2.16. Manter central de suporte técnico, indicando o número de telefone desta ou endereço eletrônico para abertura de chamados.

2.13.2.17. Deverá a CONTRATADA possuir profissionais devidamente habilitados e qualificados à prestação de assistência técnica, durante todo o período garantia de hardware/software.

2.13.2.18. Providenciar a substituição imediata dos profissionais alocados ao serviço, que eventualmente não atendam aos requisitos deste Termo de Referência ou por solicitação do CONTRATANTE, devidamente justificada;

2.13.2.19 Responsabilizar-se por danos causados ao patrimônio do CONTRATANTE e suas unidades, ou de terceiros, ocasionados por seus empregados, em virtude de dolo ou culpa, durante a execução do objeto contratado;

2.13.2.20. Responsabilizar-se por quaisquer acidentes de que possam ser vítimas seus empregados e prepostos, quando nas dependências do CONTRATANTE e respectivas unidades, devendo adotar as providências que, a respeito, exigir a legislação em vigor;

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: Sidália Souza do Amaral Matrícula: 892 Telefone: 3205-3135 E-mail: sidalia.amaral@tjpa.jus.br

Equipe de gestão e fiscalização da contratação			
Gestor do Contrato Nome: Thiago do Rosário de Castro	Fiscal Demandante Nome: Arilson Galdino da Silva	Fiscal Técnico	Fiscal Administrativo Nome:

Matrícula: 174394 Telefone: 3289-7189 E-mail: thiago.rosario@tjpa.jus.br	Matrícula: 183318 Telefone: 3289-7181 E-mail: arilson.silva@tjpa.jus.br	Nome: Daniel Azevedo Ferreira Matrícula: 116394 Telefone: 98165-1885 E-mail: daniel.ferreira@tjpa.jus.br	Matrícula: Telefone: E-mail:

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

Pela CONTRATADA, deverá ser indicado 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

3.2.1. Etapas

3.2.2. Dos prazos

São prazos observáveis, conforme definido:

Cronograma Físico-Financeiro			
Fase	Atividade	Prazo	Prazo Acumulado
Pós-Licitação	Prazo para celebração do contrato.	Até 5 dias corridos, após	5 dias

		convocação, podendo ser prorrogado por igual período, desde que devidamente justificado e aceito pelo TJPA.	
Contratação	Prazo para a reunião inicial de alinhamento.	Até 3 dias corridos, após conclusão da etapa anterior.	8 dias
Execução	Prazo máximo admitido para fornecimento das subscrições.	Até 5 dias decorridos, contatos do início da execução e mediante Ordem de Fornecimento, podendo ser prorrogado por igual período, desde que devidamente justificado e aceito pelo TJPA.	13 dias
Execução	Prazo máximo para recebimento provisório.	Até 1 dia, após conclusão da etapa anterior.	14 dias
Execução	Prazo máximo para recebimento definitivo.	Até 3 dias, após conclusão da etapa anterior.	17 dias
Execução	Prazo máximo para instalação e configuração inicial das subscrições.	Até 3 dias, após conclusão da etapa anterior.	20 dias
Faturamento	Prazo para entrega da nota fiscal e demais comprovações e evidências.	Até 3 dias, após conclusão da etapa anterior.	23 dias
Pagamento	Prazo para pagamento	Até 30 dias, contados da entrega da nota fiscal, desde que toda a documentação apresentada esteja correta.	53 dias

	Execução contratual	Atendimento de Demandas relativas aos serviços de suporte técnico e garantia (agendamento prévio de 24 horas).	Até 4 horas para iniciar o atendimento.	Até 72 horas para solucionar o problema.
	Execução Contratual	Atendimento das demandas sem previsão de cobertura pela garantia e suporte técnico.	Dentro do prazo estipulado pela Ordem de Serviço.	De acordo com cada Ordem de Serviço.
	Garantia e Manutenção	Os serviços de suporte técnico "On Site", Em Brasilia, deverão ser atendidos sempre que solicitados pelo CONTRATANTE, mediante agendamento prévio.		Antecedência de 24 horas junto à CONTRATADA.

3.2.3.

3.2.3.1. Prazos de entrega dos bens/execução dos serviços

O prazo de entrega dos bens adquiridos a execução dos serviços contratados é de até 30 (trinta) dias, a partir da assinatura do contrato, observando os detalhamentos e suas especificidades, conforme quadro descritivo acima.

3.2.3.2. Prazo de vigência do contrato

A vigência do futuro contrato será de 24 (vinte e quatro) meses, prorrogáveis até o limite máximo permitido pelo art. 57, inciso IV da lei 8666/93 e alterações.

3.2.4. Logística de implantação

Os equipamentos deverão ser entregues na Secretaria de Informática do TJPA, sito à Avenida Nazaré, 582, esquina com a Travessa Rui Barbosa, bairro Nazaré, em Belém, de segunda a sexta-feira, no horário de 08:00 às 14:00, conforme agendamento prévio.

3.2.5. Cronograma

A metodologia de trabalho a ser implementada terá por base as condições, características, prazos e critérios definidos no Cronograma Físico-Financeiro.

3.3. 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.

3.4. Garantia e Nível de Serviço

3.4.1. Garantia do produto/serviço

De acordo com o item 3.6.3 dos estudos preliminares, o prazo de garantia do hardware, software, suporte e licenciamento que serão renovados deverá ser de 24 (vinte e quatro) meses. Dentre os requisitos selecionados, destaca-se:

- O prazo de vigência da garantia e suporte técnico do contrato será de 24 (vinte e quatro) meses, contados a partir do recebimento definitivo da solução adquirida;
- Durante o período de vigência da garantia, a CONTRATANTE terá direito a atualização de versão de todos os softwares contratados;
- O suporte técnico e a garantia deverão ser prestados obrigatoriamente on site quando ocorrer indisponibilidade de qualquer uma das soluções, inclusive em sábados, domingos e feriados;
- A CONTRATADA deverá dispor de equipe técnica qualificada para a entrega, instalação, configuração, repasse de conhecimento, suporte técnico e garantia;
- O serviço de suporte técnico deverá ser prestado no idioma português.
- Toda a manutenção da solução (licenças) durante o período de garantia, será de inteira responsabilidade da futura contratada, nos termos e condições especificados neste termo de referência;
- Garantia e manutenção das licenças durante o período de vigência;
- A total responsabilidade pela garantia e manutenção da solução a ser disponibilizada e de todos os serviços prestados, serão de única e exclusiva responsabilidade da futura empresa a ser CONTRATADA;
- Excepcionalmente, na ocorrência de incidentes tais como o comprometimento sistêmico de uma defensoria ou comprometimento da solução ofertada (indisponibilidade de serviço que afete a efetividade da solução de forma significativa ou que acarrete em parada das atividades dos usuários;
- A CONTRATADA deve atender as demandas de suporte técnico e utilizar o escalonamento com a fabricante sempre que necessário;
- A CONTRATADA deverá providenciar a coleta e transmissão dos arquivos de diagnóstico que o fabricante necessite para diagnosticar e solucionar o problema;
- A CONTRATADA deverá verificar a disponibilização de releases de versões, patches ou atualizações de softwares da solução e informar o CONTRATANTE;
- Caso haja necessidade de atualização de versão da solução, a CONTRATADA deverá confeccionar o plano de mudança do parque institucional, informando as melhorias e os impactos no ambiente do CONTRATANTE. O plano de mudança deve ser devidamente documentado e entregue no prazo máximo de 1 mês, a contar da oficialização de pedido, para análise e aprovação da equipe técnica do CONTRATANTE;
- Fica sob responsabilidade da CONTRATADA acompanhar a atualização do parque de endpoints junto com as equipes técnicas do TJPA;
- O CONTRATANTE deverá fornecer lista de contatos de suas equipes técnicas para a CONTRATADA, atualizando-a sempre que necessário;
- Fica sob responsabilidade da CONTRATADA a entrega de toda plataforma de gerência (locais e central) da solução fornecida atualizada e devidamente configurada, no prazo máximo de 1 mês, após aprovação do plano de mudança;
- Caso haja necessidade de nova máquina servidora para a instalação de quaisquer softwares da solução, a CONTRATADA deverá notificar o CONTRATANTE para que esta providencie uma máquina com sistema operacional devidamente instalado e licenciado, conforme especificação passada pela CONTRATADA;
- A CONTRATADA deverá fornecer script para automação do processo de atualização dos endpoints, ajustado para cada localidade, sempre que necessário;
- CONTRATADA deverá resolver problemas que ocorram no processo de atualização;
- A CONTRATADA deverá informar imediatamente a disponibilização de patches ou pacotes de correção de softwares da solução, caso os mesmos sejam críticos para a correta operação e efetividade da solução. A CONTRATADA deverá obedecer às especificações de execução do serviço descritas no item 15.7.6, ressalvando que o tempo total para execução dessa atualização em todo parque da DPE/PA fica reduzido a 1 mês, entre a notificação e finalização da atividade;

- Caso haja notificação de inconsistências em pacote de atualização por parte do fabricante, a CONTRATADA deve notificar imediatamente a equipe técnica do CONTRATANTE, evitando-se ocorrência de indisponibilidade de serviços da solução;
- Fica a CONTRATADA responsável em coordenar e efetuar as ações no que compete a solução por ela fornecida, bem como acompanhar sua aplicação e tratar eventuais erros;
- A CONTRATADA deverá transferir a equipe técnica do CONTRATANTE o know how das configurações efetuadas, modelo de gerenciamento, diagramas e scripts usados, links para vídeos educativos/webinar1 do fabricante para a solução fornecida, link com documentos do fabricante com guias para administrações e boas práticas, entre outras informações pertinentes;
- Para isso, a futura CONTRATADA deverá disponibilizar meios de comunicação para abertura de chamados técnicos, como telefone, 0800, e-mail, sistema de abertura de chamados, entre outros, em regime comercial "5x8" (oito horas por dia, cinco dias por semana), sendo abertos pela equipe técnica do TJPA;
- O atendimento poderá ser do tipo "On Site", telefônico ou remoto para auxiliar a fiscalização na solução de dúvidas, quando necessário;
- A duração da garantia que engloba manutenção (preventiva e corretiva) terá a duração inicial de 24 (vinte e quatro) meses;
- Em caso de prorrogação de vigência, a futura garantia deverá se estender por toda o novo lapso temporal;
- Os serviços de garantia e manutenção das licenças representam uma necessidade permanente da DPE/PA para este tipo de solução, tendo em vista o fato de permitirem o acesso a atualizações do produto, e do pleno funcionamento de suas funcionalidades, e ao suporte por parte do Fabricante em caso de problemas, considerada parte de infraestrutura crítica da Segurança da Informação do TJPA;
- Caberá à proponente a atualização da versão da solução fornecida, caso necessário e sempre que o fabricante disponibilizar novos upgrades;
- Caberá à futura contratada, realizar o monitoramento remoto e presencial, suporte técnico continuado e garantia de atualização de versão da solução a ser fornecida;
- O atendimento deverá ocorrer em, no máximo, 4 (quatro) horas corridas e o prazo máximo para solução de problemas deverá ser de 72 (setenta e duas) horas corridas, ambos os prazos contados a partir do momento da abertura do chamado;
- Posteriormente ao atendimento da solicitação do CONTRATANTE, a CONTRATADA deverá apresentar relatório de visita contendo a data e hora do chamado, do início e término do atendimento, bem como a identificação do defeito e as providências adotadas;
- A CONTRATADA deverá informar ao CONTRATANTE o lançamento das atualizações dos softwares cobertos pelo presente Contrato e disponibilizá-las, sem qualquer custo adicional, durante todo o período da vigência da garantia de atualização de versão;
- Os profissionais da CONTRATADA que executarão os serviços de suporte técnico deverão ser especializados e certificados pelo fabricante ou distribuidor autorizado no Brasil do software antivírus;

3.4.2. Garantia contratual

Exigência de garantia de execução do contrato, nos moldes do art. 56 da Lei nº 8.666, de 1993, com validade durante a execução do contrato e 90 (noventa) dias após término da vigência contratual, observados ainda os seguintes requisitos:

A contratada deverá apresentar, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do órgão contratante, contado da assinatura do contrato, comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária, o valor da garantia deverá corresponder a 5% (cinco por cento) do valor total do contrato.

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

Prejuízos advindos do não cumprimento do objeto do contrato;

Prejuízos diretos causados à Administração, decorrente de culpa ou dolo durante a execução do contrato;

Multas moratórias e punitivas aplicadas pela Administração à contratada; e

Obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela contratada, quando couber.

A garantia em dinheiro deverá ser efetuada em banco e conta específica com correção monetária, em favor da contratante;

A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, observado o máximo de 2% (dois por cento);

O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei nº 8.666, de 1993;

O garantidor não é parte para figurar em processo administrativo instaurado pelo contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada;

A garantia será considerada extinta:

Com a devolução da apólice, carta-fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Administração, mediante termo circunstanciado, de que a contratada cumpriu todas as cláusulas do contrato; e

Com o término da vigência do contrato, que poderá, independentemente da sua natureza, ser estendido em caso de ocorrência de sinistro.

O contratante executará a garantia na forma prevista na legislação que rege a matéria;

3.4.3. Nível de Serviço

Não haverá.

3.5. 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.

3.6. Do recebimento

3.6.1. Do recebimento provisório

O objeto da contratação será recebido provisoriamente pela Coordenadoria de Suporte Técnico (CST) da Secretaria de Informática (SECINFO) do TJPA, para efeito de posterior verificação da conformidade dos produtos com as especificações deste Termo de Referência.

3.6.2. Do recebimento definitivo

Os equipamentos serão recebidos definitivamente pela SECINFO, com a correspondente emissão do TRD (Termo de Recebimento Definitivo), em até 30 (trinta) dias após o recebimento provisório, mediante termo de liquidação na nota fiscal/fatura, após a verificação da qualidade dos produtos e de seus componentes indissociáveis, ativação no site do fabricante dos serviços de suporte técnico atrelados à garantia e aceitação, pela Equipe de Gestão e Fiscalização da Contratação.

3.7. Da forma de pagamento

Os valores decorrentes dessa contratação foram previstos no Plano Orçamentário do Tribunal de Justiça do Estado do Pará, referente à Secretaria de Informática, vigente para o exercício de 2021. O valor foi provisionado nas Notas de Reserva 2021/509, 2021/540 e 2021/577 relacionadas às ações 8651 (65%), 8652 (9%) e 8653 (26%), fonte 0118, elemento de despesa 3.3.90.40.

O pagamento será efetuado, mediante apresentação de Nota Fiscal devidamente atestada pelo setor competente, após conclusão e aceite dos serviços por meio da emissão do termo de recebimento definitivo.

O pagamento será realizado em 3(três) parcelas, sendo a primeira 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, as demais serão pagas obedecendo um interstício mínimo de 12 meses entre elas

A emissão da Nota Fiscal/Fatura será precedida do recebimento definitivo do serviço, conforme este Termo de Referência.

A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada 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. 29 da Lei nº 8.666, de 1993.

Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

O setor competente para proceder o pagamento deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

O prazo de validade;

A datade emissão;

Os dados do contrato e do órgão contratante;

O período de prestação dos serviços;

O valor a pagar; e

eventual destaque do valor de retenções tributárias cabíveis.

Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante;

Será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

não produziu os resultados acordados;

deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada;

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

Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital;

Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, 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. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante;

Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018;

Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, 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;

Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa;

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

Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante;

Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, em especial a prevista no artigo 31 da Lei 8.212, de 1991;

É vedado o pagamento, a qualquer título, por serviços prestados, à empresa privada que tenha em seu quadro societário servidor público da ativa do órgão contratante, com fundamento na Lei de Diretrizes Orçamentárias vigente;

Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga;
I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX)	$I = \frac{(6 / 100)}{365}$	I = 0,00016438 TX = Percentual da taxa anual = 6%

3.8. Da transferência de conhecimento

Não existe previsão de transferência de conhecimento.

3.9. 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.

3.10. Da qualificação técnica dos profissionais

Os profissionais técnicos do fabricante ou da empresa parceira do fabricante que eventualmente vierem a interagir com a equipe técnica da CONTRATANTE deverão estar devidamente habilitados pelo fabricante para tais interações.

3.11. Das sanções

Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002 e Decreto Distrital nº 26.581/2006 e suas alterações, a CONTRATADA que:

- Inexecução total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

- Ensejar o retardamento da execução do objeto;

- Fraudar na execução do contrato;

- Comportar-se de modo inidôneo;

- Cometer fraude fiscal;

- Não mantiver a proposta.

A CONTRATADA que cometer qualquer das infrações discriminadas nos subitens acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

- Advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a CONTRATANTE;

- Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

- Impedimento de licitar e contratar com o Estado do Pará com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

- Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA ressarcir a CONTRATANTE pelos prejuízos causados;

- Multa moratória de 2% (dois por cento) sobre o valor do Contrato, pela recusa da licitante VENCEDORA em assinar o Contrato, e não apresentar a documentação exigida no Edital para sua celebração, nos prazos e condições estabelecidas, caracterizando o descumprimento total da obrigação assumida, com base no art. 81 da Lei no 8.666, de 1993, independentemente das demais sanções cabíveis (relativas somente ao certame realizado pelo Órgão Gerenciador);

- Multa compensatória 2% (dois por cento) sobre o valor da Ordem de Fornecimento ou Serviço, pela inexecução parcial;

Multa compensatória 20% (vinte por cento) sobre o valor do contrato, quando a ocorrer inexecução total ou execução insatisfatória do contrato e pela interrupção da execução do contrato sem prévia autorização da CONTRATANTE, independentemente das demais sanções cabíveis, ensejando o desfazimento da avença.

- A incidência das glosas advindas do Acordo de Nível de Serviço exigidos poderá ser aplicada juntamente com as sanções e penalidades, facultada a defesa prévia do interessado no respectivo processo, no prazo de cinco (05) dias úteis;

- Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá a CONTRATADA pela diferença, que será descontada dos pagamentos eventualmente devidos pela Administração ou cobrada judicialmente;

4. DOS REQUISITOS TÉCNICOS ESPECÍFICOS

SUBSCRIÇÃO DE SOFTWARE DE SEGURANÇA PARA ENDPOINTS, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 24 (VINTE E QUATRO) MESES:

– Os softwares (solução) necessários à prestação dos serviços deverão ser instalados, de modo a avaliar e proteger contra códigos maliciosos as estações de trabalho do ambiente da CONTRATANTE.

Características Licenciamento:

– Estar dimensionada por 1.000 estações de trabalho.
– Funcionalidades e Requisitos Específicos:
– Realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais: Windows 7 (x86/x64); Windows 8.1 (x86/x64) e Windows 10 (x86/x64);
– Possuir tecnologia de Machine Learning sendo capaz de detectar variantes de malwares desconhecidos por similaridade de código;
– Possuir módulo de monitoração de comportamento malicioso de aplicações de forma a bloqueá-las mesmo quando a assinatura não for reconhecida;
– Possuir regras específicas para detecção de ransomware;
– Detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, key loggers, programas de propaganda, rootkits, phishing, dentre outros;
– Detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos
– Processos em execução em memória principal (RAM);
– Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);
– Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab;
– Arquivos recebidos por meio de programas de comunicação instantânea (msn messenger, yahoo messenger, google talk, icq, dentre outros).
– Permitir configurar o consumo de cpu que será utilizada para uma varredura manual ou agendada;
– Possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;
– Permitir a utilização de servidores locais de reputação para análise de arquivos e URL‟s maliciosas, de modo a prover, rápida detecção de novas ameaças;
– Possuir a capacidade de aferir a reputação das URL‟s acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug- in ao navegador web, de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;
– Permitir proteção dedicada contra URL‟s maliciosas voltadas a clientes utilizando Microsoft Skype for Business e Microsoft Lync Server.

– Permitir a programação de atualizações automáticas e/ou incremental das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;
– Permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utiliza-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;
– O servidor da solução de anti-malware e os agentes de atualização, devem ser capazes de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;
– Permitir proteção dedicada contra códigos maliciosos voltadas a clientes Microsoft Skype for Business e Microsoft Lync Server.
– Permitir bloquear o acesso a qualquer site não previamente analisado pelo fabricante;
– Permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;
– Permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;
– Possuir funcionalidade de Machine Learning em runtime para evitar possíveis métodos de obfuscação que o módulo de Machine Learning em pré-execução não consiga detectar;
– Fornecer um informativo compreensivo de cada simulação que descreva as ações e respectivos metadados, bem como, o porquê do veredito emitido pela Machine Learning;
– As funcionalidades de Endpoint Protection Platform-EPP, tais como antimalware, web reputation, controle de aplicação, host IPS, host Firewall e DLP deverão possuir um unico agente;
– Permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;
– Possibilitar instalação "silenciosa";
– Permitir o bloqueio por nome de arquivo;
– Permitir o travamento de pastas e diretórios;
– Permitir o travamento de compartilhamentos;
– Permitir o rastreamento e bloqueio de infecções;
– Possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;
– Efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;
– Desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;
– Permitir a desinstalação através da console de gerenciamento da solução;
– Ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;
– Permitir a deleção dos arquivos quarentenados;
– Permitir remoção automática de clientes inativos por determinado período de tempo;
– Permitir integração com Active Directory para acesso a console de administração;
– Identificar através da integração com o Active Directory, quais máquinas estão sem a solução de anti-malware instalada;
– Permitir criação de diversos perfis e usuários para acesso a console de administração;
– Permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

– Possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;
– Prover ao administrador informações sobre quais estações de trabalho e notebooks fazem parte do escopo de gerenciamento da console de anti-malware não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias;
– O fabricante da solução deve dispor de laboratório próprio para desenvolvimento de vacinas e engines e possuir analista dedicado a desenvolvimento de defesas contra ameaças e malwares originados no Brasil. Esta informação deve ser comprovada pelo Fabricante através de documentação oficial.

Funcionalidades de Controle de Dispositivos:

– Possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;
– Possuir o controle de acesso a drives de mídias de armazenamento como CD-ROM e DVD, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;
– Possuir a capacidade de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;
– Possuir a capacidade de controlar drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;
– Permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, CD-ROM) mesmo com a política de bloqueio total ativa.

Funcionalidades de Host IPS e Host Firewall:

– Possuir a capacidade de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais: Windows 7 (x86/x64), Windows 8.1 (x86/x64) e Windows 10 (x86/x64);
– Possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall;
– As regras de vulnerabilidades deverão possuir a opção de desativar a regra de forma individual;
– Todas as regras das funcionalidades de firewall e IPS de host devem permitir apenas detecção (log) ou prevenção (bloqueio);
– Permitir ativar e desativar o produto sem a necessidade de remoção;
– Permitir que o usuário altere as configurações de níveis de segurança e exceções;
– Possuir a possibilidade de configurar níveis diferentes de segurança podendo ser eles alto, médio e baixo;
– O modulo de IDS deverá prevenir contra os seguintes tipos de ataque: Too Big Fragment, Ping da morte, Conflito de ARP, SYN Flood, Overlapping Fragment, Teardrop, Tiny Fragment Attack, Fragmented IGMP e Land Attack;
– O modulo de HIPS deverá possuir perfis pré-determinados baseados em performance e segurança;
– O modulo de HIPS deverá possuir regras pra proteger contra ameaças do tipo Ransomware;
– O modulo de HIPS deverá conter regras contra exploit, vulnerabilidades e genericas protegendo contra ameaças conhecidas ou desconhecidas.

Funcionalidades de Controle de Aplicação:

– Possuir a capacidade de realizar o controle de aplicações nos seguintes sistemas operacionais: Windows 7 (x86/x64), Windows 8 e 8.1 (x86/x64) e Windows 10 (x86/x64);

- Deverá pemitir que o programa liberado efetue ou não a execução de outros processos;
- Permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;
- Permitir os seguintes métodos para identificação das aplicações: Assinatura SHA-1 e SHA-256 do executável, atributos do certificado utilizado para assinatura digital do executável, Caminho lógico do executável, Base de assinaturas de certificados digitais válidos e seguros.
- Possuir categorias pré-determininadas de aplicações;
- Permitir a utilização de múltiplas regras de controle de aplicações;
- Possuir uma lista de aplicações mal-intencionados para bloqueio e monitoramento.

Funcionalidades de Proteção contra Vazamento de Informações:

- Possuir a capacidade de realizar a proteção contra vazamento de informação nos seguintes sistemas operacionais: Windows 7 (x86/x64); Windows 8.1 (x86/x64) e Windows 10 (x86/x64);
- Possuir nativamente templates para atender as seguintes regulamentações: PCI/DSS, HIPAA, GLBA, SB-1386 e US PII.
- Ser capaz de detectar informações, em arquivos nos formatos: Documentos: Microsoft office (doc, docx, xls, xlsx, ppt, pptx) openoffice, rtt, wordpad, text; xml, html; Gráficos: visio, postscript, pPA, ff; Comprimidos: win zip, rar, tar, jar, arj, 7z, rpm, cpio, gzip, bzip2, unix/linux zip, lzh; Códigos: c/c++, java, verilog, autocad.
- Ser capaz de detectar informações, com base em: Dados estruturados, como dados de cartão de crédito, dados pessoais, endereços de e-mail, CPF, entre outros; Palavras ou frases configuráveis; Expressões regulares; Extensão dos arquivos.
- Ser capaz de detectar em arquivos compactados;
- Permitir a configuração de quantas camadas de compressão serão verificadas;
- Permitir a criação de modelos personalizados para identificação de informações;
- Permitir a criação de modelos com base em regras e operadores lógicos;
- Possuir modelos padrões;
- Permitir a importação e exportação de modelos;
- Permitir a criação de políticas personalizadas
- Permitir a criação de políticas baseadas em múltiplos modelos;
- Permitir mais de uma ação para cada política, como: Apenas registrar o evento da violação; Bloquear a transmissão; Gerar alertar para o usuário; Gerar alertar na central de gerenciamento; Capturar informação para uma possível investigação da violação.
- Permitir criar regras distintas com base se a estação está fora ou dentro da rede;
- Ser capaz de identificar e bloquear informações nos meios de transmissão: Cliente de e-mail; Protocolos http, https; Mídias removíveis; Discos óticos cd/dvd; Gravação cd/dvd; Aplicações de mensagens instantâneas; Tecla de print screen; Aplicações p2p; Área de transferência do Windows; Webmail; Armazenamento na nuvem (cloud); Impressoras; Scanners; Compartilhamentos de arquivos; Activesync; Criptografia PGP; Bluetooth.
- Permitir a criação de exceções nas restrições dos meios de transmissão.

Funcionalidades de Criptografia:

- Possuir a capacidade de realizar a criptografia nos seguintes sistemas operacionais: Windows 7 (x86/x64); Windows 8.1 (x86/x64) e Windows 10 (x86/x64);
- Possuir módulo de criptografia para as estações de trabalho (desktops e notebooks), permitindo criptografia para: Disco completo (FDE – full disk encryption); Pastas e arquivos; Mídias removíveis; Anexos de e-mails e Automática de disco;
- Possuir autenticação durante a inicialização (boot) da estação de trabalho, antes do carregamento do sistema operacional, para a funcionalidade de criptografia do disco completo;

- Possuir a capacidade de exceções para criptografia automática;
- Possuir compatibilidade de autenticação por múltiplos fatores;
- Permitir atualizações do sistema operacional mesmo quando o disco está criptografado;
- Possuir auto ajuda para usuários que esquecerem a senha com a combinação de perguntas e respostas;
- Possuir mecanismos para wipe (limpeza) remoto;
- Possuir mecanismo para desativar temporariamente a autenticação de pré-inicialização (boot);
- Possuir mecanismo que permita desfazer a criptografia do disco no evento em que se torne corrompido, impedindo a inicialização da estação/notebook; 9.2.1.7.11. O ambiente de autenticação pré-inicialização deve permitir a conexão a redes sem fio (wireless);
- Permitir, em nível de política, a indicação de pastas a serem criptografadas; 9.2.1.7.13. Possibilitar que cada política tenha uma chave de criptografia única;
- Permitir a escolha dos diretórios a serem criptografados em dispositivos de armazenamento USB;
- Possibilitar a desativação de dispositivos de gravação de mídias óticas e de dispositivos de armazenamento USB;
- Possibilitar apagar todos os dados do dispositivo na ocorrência de um número personalizável de tentativas inválidas de autenticação.
- Módulo de proteção para smartphones e tablets
- O módulo de proteção de dispositivos móveis deve possuir agente para os seguintes sistemas operacionais: IOS e Android;
- As funcionalidades estarão disponíveis de acordo com cada plataforma
- Deve permitir o provisionamento de configurações de:
- Wi-fi, Exchange Activesync, vpn, proxy http global e certificados;
- Deve possuir proteção de anti-malware para Android;
- Deve ser capaz de realizar escaneamento de malwares em tempo real, do cartão sd e após atualização de vacinas;
- Possuir capacidade de detecção de spam proveniente de SMS;
- Possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número bloqueados para recebimento de chamadas;
- Possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número permitidos para efetuação de chamadas;
- Possuir funcionalidade de firewall para bloqueio de tráfego de entrada e saída, com possibilidades de enumeração de regras de exceção;
- Permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URL‟s acessadas;
- Permitir o controle de acesso a websites por meio de listas de bloqueio e aprovação;
- Permitir o bloqueio de aplicativos de acordo com sua faixa etária indicativa;
- Possuir controle da política de segurança de senhas, com critérios mínimos de: Padrão de senha; Uso obrigatório de senha; Tamanho mínimo; Tempo de expiração; Bloqueio automático da tela; Bloqueio por tentativas inválidas.
- Controle de acesso à seguinte lista funções e status de ativação de funções dos dispositivos móveis: Bluetooth, Câmera, Cartões de memória, Wlan/wifi, GPS, Microsoft Activesync, MMS/SMS, Alto-falante, Armazenamento USB, 3g, Modo de desenvolvedor, Ancoragem (thetering).

SUBSCRIÇÃO DE SOFTWARE DE SEGURANÇA PARA SERVIDORES INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 24 (VINTE E QUATRO) MESES:

- Os softwares (solução) necessários à prestação dos serviços deverão ser instalados, de modo a prover proteção, identificação e gestão de segurança de servidores virtuais do ambiente da CONTRATANTE;

Características de Licenciamento da Solução:

- Estar dimensionada para 50 servidores físicos e virtuais.
- Funcionalidades e Requisitos Mínimos:
- A solução deverá ser totalmente compatível e homologada com o ambiente Vmware: VMware® vSphere: 5.5/6.0, View 4.5/5.0/5.1, ESX 5.5, 6.2.X, 6.5, NSX 6.2.X, 6.3;
- A solução deverá ser compatível com, pelo menos, os seguintes sistemas operacionais: Windows Server 2000, 2003 e 2003 R2 SP2, 2008 e 2008 R2, 2012 e 2012 R2, 2016 e 2019; Red Hat Enterprise 5, 6, 7 e 8; CentOS 5, 6, 7 e 8; Oracle Linux 5, 6, 7 e 8; SUSE Linux Enterprise Server 10, 11, 12 e 15; Ubuntu 10, 12, 14, 16, 18 e 20; Debian 6, 7, 8, 9 e 10; Cloud Linux 5, 6, 7 e 8; Solaris 10 1/13 Sparc, Solaris 10 1/13 (x86/x64), Solaris 11.2/ 11.3 Sparc e Solaris 11.2/ 11.3 (x86/x64); Amazon Linux e Amazon Linux 2 (x64).
- A solução deverá permitir a integração com VMware vSphere 6 e com NSX estendendo os benefícios da micro-segmentação em um datacenter definido por softwares e fazendo com que as políticas de segurança estejam atreladas às Vms onde quer que elas estejam;
- Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;
- A solução deverá permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet;
- A solução deverá ser gerenciada por console Web, compatível com pelo menos os browsers Internet Explorer e Firefox. Deve ainda suportar certificado digital para gerenciamento;
- A console de administração deverá permitir o envio de notificações via SMTP;
- Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados para fins de auditoria;
- A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas;
- A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos;
- A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;
- A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob-demanda, ou agendado com o envio automático do relatório via e-mail;
- A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PPA e RTF;
- A solução precisa permitir que relatórios no formato PPA, possam ser enviados com uma senha única para cada destinatário;
- A solução deverá prover relatórios contendo no mínimo as seguintes informações; malware, regras de IPS e Firewall;
- A console de gerenciamento deve armazenar políticas e logs em base de dados. A escolha da base de dados pode ser facultativa entre Oracle e SQL;
- A console de gerenciamento deve apresentar alta disponibilidade de modo que na ausência da principal os clientes automaticamente se comuniquem com a secundária e todas as configurações devem permanecer;
- Quando operando em modo alta disponibilidade, ambos os consoles devem compartilhar a mesma database;
- A console deve se integrar com o Active Directory para que os usuários do Active Directory possam administrar a solução de acordo com as permissões;

- A console deve se integrar com o Active Directory para que possa ser efetuado o controle das máquinas no Active Directory;
- Para efeito de administração, deve ser possível de se replicar a estrutura do Active Directory na console de administração;
- A solução de segurança para data center deverá suportar Docker para proteger os containers;
- Os usuários devem ter a capacidade de receber determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";
- Quando configurado o acesso parcial, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar novas políticas de segurança;
- A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;
- Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;
- A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;
- Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL com o servidor de onde ela buscará as informações;
- Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente;
- Os agentes para plataforma Linux deverão ser instalador por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente;
- Para efeito de administração, a solução deverá avisar quando um agente encontrar-se não conectado a sua console de gerenciamento;
- A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;
- Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;
- A solução deverá vir com perfis default pré-definidos e aptos a funcionarem de acordo com sua denominação;
- Deverá possuir uma hierarquia de prevalecimento de configurações, seguindo no mínimo a ordem: Global -> Perfis -> hosts;
- A solução deverá mostrar quais máquinas estão usando determinada política;
- Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;
- Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;
- Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;
- O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;
- Também deverá ser possível realizar o rastreamento por portas abertas, identificando possíveis serviços ativos e escutando;
- A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;
- A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;
- A solução deverá ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;
- A solução deverá ter a capacidade de se integrar com os principais softwares de SIEMs, no mínimo com: IBMQradar, HPArcSight, RSA Envision e NetIQ de modo a permitir enviar os seus logs para essas soluções;

- A solução deverá ter a possibilidade de enviar logs para SYSLOG servers;
- A solução deverá ter a possibilidade de enviar eventos da console via SNMP;
- Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;
- A solução deverá permitir exportar relatórios para no mínimo os formatos PPA e RTF;
- Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;
- A lista de contatos de recebimento de relatório poderá ser obtida através do Active Directory;
- As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando ser até mesmo de hora em hora;
- Após a atualização deve ser informado o que foi modificado ou adicionado;
- Deve ser possível baixar as assinaturas na console de gerenciamento, mas não distribuí-las aos clientes;
- A console de gerenciamento deve apresentar a capacidade de gerar roll back de suas atualizações de regras;
- A solução deverá ter capacidade de gerar pacote de auto diagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;
- Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;
- No gerenciamento de licenças, deve ser informada quantidade contratada e quantidade em utilização de clientes;
- Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;
- Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos;
- Possibilidade de customizar a escolha do serviço de Whois para a identificação dos IPs que estejam realizando ataques;
- Deverá possibilitar colocar etiquetas em eventos para que se possam visualizar apenas os eventos desejados;
- O fabricante deverá participar do programa “Microsoft Application Protection Program” para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;
- A console de gerenciamento deve se integrar com o Vmware vCenter 4.0 ou Superior, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para a console de gerenciamento da solução;
- A partir desta integração, deverá ser possível gerir a segurança dos guests vm, podendo ser atribuídos perfis de segurança, regras únicas para cada host, além de possibilitar a coleta dos logs gerados para cada módulo habilitado;
- Esta integração deve possibilitar que, a partir da instalação e integração de um virtual appliance do fabricante da solução de segurança com o ambiente Vmware e suas APIs, seja possível proteger as guests VMs sem a necessidade de instalação de agentes de segurança do fabricante da solução nas guests VMs;
- Este virtual appliance deverá permitir integração com as seguintes APIs VMware: Vmsafe API e vShield Endpoint API, possibilitando que funcionalidades de Firewall, Proteção de Aplicações Web, Antimalware, Controle de Acesso a Sites Maliciosos, Monitoramento de Integridade de Arquivos, Controle de Aplicações e IDS/IPS, possam ser efetuados diretamente via hypervisor e virtual appliance em conjunto, não necessitando a instalação de agentes adicionais de segurança do fabricante nos guests VMs protegidos;
- A solução deverá ser capaz de implementar as funcionalidades de Antimalware, Controle de Acesso a Sites Maliciosos, Firewall, IDS/IPS, Controle de Aplicações, Proteção de aplicações Web, Inspeção de Logs e Monitoramento de Integridade nos sistemas operacionais Windows através de um único agente;

- A solução deverá ser capaz de implementar as funcionalidades de Antimalware, Firewall, IDS/IPS, Controle de Aplicações, Proteção de aplicações Web, Inspeção de Logs e Monitoramento de Integridade nos sistemas operacionais Linux através de um único agente;
- A solução deverá ser capaz de implementar as funcionalidades de Firewall, IDS/IPS, Controle de Aplicações, Proteção de aplicações Web, Inspeção de Logs e Monitoramento de Integridade nos sistemas operacionais Solaris através de um único agente;
- A solução deverá ser capaz de implementar as funcionalidades de Inspeção de Logs e Monitoramento de Integridade nos sistemas operacionais HP-UX e AIX através de um único agente;
- Precisa ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;
- Precisa ter a capacidade de desabilitar as regras não mais necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador.

Funcionalidades de Antimalware e proteção web

- A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;
- A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;
- A solução deve possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;
- A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção;
- A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas;
- A solução deverá oferecer escanear processos em memória em busca de Malware;
- O scan de arquivos comprimidos deverá ser de no mínimo 6 camadas de compressão;
- O scan de arquivos comprimidos do tipo OLE deverá ser de no minimo 20 camadas de compressão;
- A solução deverá possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta;
- A solução deverá mostrar informação de data sobre o último scan agendado ou manual executado;
- Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware;
- Deve possuir cache dos arquivos verificados de modo a evitar a redundância da varredura;
- Deve possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho no servidor;
- A solução deve possuir opção para forçar a comunicação com o agente e coletar os respectivos logs;
- Deve permitir a proteção contra acesso a websites ou url consideradas maliciosas ou de baixa reputação;
- A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;
- A solução deve permitir alterar o nível de sensibilidade para detecção de URLs maliciosas tendo, pelo menos, os níveis Alto, médio e baixo;
- Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;
- Deve permitir configurar notificações personalizadas para detecções desse módulo, deixando a cargo do administrador exibir ou não tais notificações;
- Deverá ter capacidade de identificar acessos a URLs maliciosas além das portas padrão 80 e 443;
- A solução deve permitir que o administrador reclassifique uma URL através do site do fabricante para evitar falsos positivos;

- A proteção deve possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança.

Funcionalidades de Firewall

- Operar como firewall de host, através da instalação de agente nos servidores protegidos;
- Precisa ter a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;
- Precisa ter a capacidade de controlar conexões TCP baseado nas Flags TCP;
- Precisa ter a capacidade de definir regras distintas para interfaces de redes distintas;
- A solução deverá ser capaz de reconhecer e possibilitar o bloqueio endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYNSYN Scan, TCP Xmas Scan e Computer OS FIngerprint por até 30 minutos;
- Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;
- Precisa ter a capacidade de definição de regras para contextos específicos;
- Precisa ter a capacidade de realização de varredura de portas nos servidores;
- Para facilitar a criação e administração de regras de firewall, as mesmas poderão se apoiar em objetos que podem ser lista de ips, lista de MACs, lista de portas;
- Regras de firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);
- Regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;
- O firewall deverá ser stateful bidirecional;
- O firewall deverá permitir liberar ou apenas logar eventos;
- O firewall deverá ser passível de criação de regras através do protocolo, origem do tráfego, frame type, TCP header flags, destino e direção;
- As regras de Firewall deverão ter as seguintes ações, ou equivalentes: Allow, log only, bypass, force allow, deny;
- A solução, para facilidade de administração, deverá utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado;
- As ações também deverão ser possíveis de terem prioridades diferentes, sendo que a prioridade maior prevalece sobre a prioridade menor;
- Deverá realizar pseudo stateful em tráfego UDP;
- Deverá logar a atividade stateful;
- Deverá permitir limitar o número de conexões entrantes e o número de conexões de saída de um determinado computador;
- Deverá permitir limitar o número de meias conexões vindas de um computador;
- Deverá prevenir ack storm;
- Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras;
- Deverá identificar escaneamentos ativos de porta ou da rede, bloqueando o IP ofensor por um período de tempo configurado pelo administrador;
- Deverá permitir criar listas de exceções para identificar os Ips autorizados a realizar varreduras de portas ou da rede;
- Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

Funcionalidades de Inspeção de Pacotes:

- Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;
- Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do SO, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;
- A solução deverá conter regras pré-definidas para detecções de ransonware para as principais famílias deste tipo de malware;
- Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;
- Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2003, 2008, 2012, 2016, 2019, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris, AIX além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;
- Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;
- Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;
- Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant Messaging;
- Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;
- Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;
- Ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de IPS;
- Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);
- Regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;
- Deverá ser capaz de inspecionar tráfego incoming SSL;
- Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: Sql injection, Crossite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;
- As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;
- Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação;
- Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;
- Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;
- Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;
- As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;
- As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;
- As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVEs;
- As regras de IPS poderão ter sua capacidade de LOG desabilitado;
- As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;

- As regras devem ser atualizadas automaticamente pelo fabricante;
- Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

Funcionalidades de Monitoramento de Integridade

- A solução deverá permitir a implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX, através da instalação de agentes;
- Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;
- A solução deverá fazer uso da tecnologia Intel TPM/TXT para monitorar a integridade contra mudanças não autorizadas a nível do Hypervisor;
- Precisa ser capaz de detectar mudanças no estado de portas em sistemas operacionais Linux;
- Precisa ter a capacidade de monitorar o status de serviços e processos do sistema operacional;
- Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows;
- Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e customização de XML para criação de regras avançadas;
- Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;
- O monitoramento poderá ser realizado em Real-time ou utilizando de scans periódicos para detectar mudanças de integridade;
- Deverá alertar toda vez que uma modificação ocorrer em real time para ambiente Windows e pseudo real time para ambiente Linux, quando utilizamos agente;
- Deverá logar e colocar em relatório todas as modificações que ocorram;
- As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;
- Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;
- Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;
- Algumas regras podem ser modificadas pelo administrador para adequação ao seu ambiente.

Funcionalidades de Inspeção de Logs:

- A solução deverá permitir sua implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX;
- Precisa ter a capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;
- Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de inspeção de logs de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;
- Precisa permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;
- Precisa permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;
- Deverá rastrear e indicar/sugerir ao administrador do sistema quais softwares estão instalados e que possuem logs passíveis de inspeção;
- Deverá possibilitar a criação de regras de inspeção de logs para aplicações customizadas;
- Deverá ter inteligência para que a cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor seja alertada;

- Deverá ter inteligência para que a cada violação relevante no log inspecionado que seja suspeita no servidor seja alertada;
- Deverá logar cada violação e colocar em relatório todas as violações relevantes que ocorram;
- As regras poderão ser modificadas por severidade de ocorrência de eventos;
- As regras devem se atualizar automaticamente pelo fabricante;
- Permitir modificação pelo administrador em regras para adequação ao ambiente.

Funcionalidades de Controle de Aplicação:

- A solução deverá permitir sua implantação nas plataformas Linux e Microsoft Windows;
- O controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256;
- O agrupamento dos eventos deverá ser realizado pelo menos por Hash ou por máquina;
- A console deverá exibir eventos de no mínimo 30 dias;
- A solução deverá possuir um mecanismo ao qual permita a execução de aplicações e scripts automaticamente, sem intervenção manual, por um determinado período de tempo que deve ser no máximo 10 horas;
- A solução deverá possuir no mínimo as funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente.

GERENCIAMENTO CENTRALIZADO DAS SOLUÇÕES:

Funcionalidades e Requisitos Específicos:

- A solução de gerenciamento centralizado deve permitir a integração com as soluções de segurança para servidores, soluções de proteção de endpoints e solução de proteção de ameaças avançadas;
- 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;
- Instalação do servidor na plataforma Windows 2012 Server ou superior, seja o servidor físico ou virtual;
- Suportar base de dados Microsoft SQL;
- Deve gerenciar logs das atividades e eventos gerados pela solução;
- Deve possuir integração com Microsoft Active Directory;
- Deve permitir níveis de administração por usuários ou grupos de usuários;
- Deve permitir a constituição de políticas genéricas aplicáveis a grupos de máquinas, ou aplicáveis a grupos de usuários;
- Deve disponibilizar sua interface através dos protocolos HTTP e HTTPS;
- Deve permitir a alteração das configurações das ferramentas ofertadas, de maneira remota;
- Deve permitir diferentes níveis de administração, de maneira independente do login da rede;
- Geração de relatórios e gráficos e parametrizáveis nos formatos HTML, PPA, XML e CSV;
- Deve gerar relatórios e gráficos pré-definidos nos formatos PPA, ActiveX e Crystal Report (*.rpt);
- Deve permitir criação de modelos de relatórios customizados;
- Deve permitir logon via single sign-on com os demais produtos da solução;
- Deve permitir a atualização de todos os componentes de todos os módulos gerenciados;
- Deve permitir a criação de planos de entrega das atualizações, com hora de início ou postergação da entrega após o download dos componentes;
- Deve permitir o controle individual de cada componente a ser atualizado;
- Deve permitir a definição de exceções por dias e horas para não realização de atualizações;
- Deve permitir ter como fonte de atualização um compartilhamento de rede no formato UNC;
- Deve gerar relatórios e gráficos com o detalhamento das versões dos produtos instalados;

- Deve possuir o acompanhamento dos comandos administrativos em execução, tal como seu status de conclusão, alvo e usuário;
- Deve permitir a configuração dos eventos administrativos ou de segurança que geram notificações, tal como o método de envio e o destinatário;
- Os métodos de envio suportados devem incluir: e-mail, gravação de registros de eventos do Windows, SNMP e SYSlog;
- Deve permitir a configuração do intervalo de comunicação com os módulos gerenciados;
- Deve permitir a escolha do intervalo de tempo necessário para que um módulo seja considerado fora do ar (off-line);
- Deve permitir o controle do intervalo de expiração de comandos administrativos;
- Deve possuir a configuração do tempo de expiração da sessão dos usuários;
- Deve permitir a configuração do número de tentativa inválidas de login para o bloqueio de usuários;
- Deve permitir a configuração da duração do bloqueio;
- Deve permitir pesquisas personalizadas para a consulta de eventos (logs) através de categorias
- Deve permitir pesquisas personalizadas para a consulta de eventos (logs), através de critérios lógicos, com base em todos os campos pertencentes aos eventos consultados;
- Deve permitir a configuração das informações que não são enviadas dos módulos à solução de gerenciamento centralizado;
- Deve permitir a configuração da manutenção dos registros de eventos (logs), com base no intervalo de tempo que devem ser man dos e no número máximo de registros, por tipo de evento;
- Deve de permitir a criação de políticas de segurança personalizadas;
- As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:
- Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;
- Range de endereços IPS;
- Sistema operacional;
- Agrupamento lógicos dos módulos.
- As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;
- Deve permitir visualização de eventos de violação de segurança de todos os módulos gerenciados, agrupado por usuário numa linha de tempo, configurável;
- Deve permitir a gerencia dos módulos baseados no modelo de nuvem (cloud), quando existentes;
- Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;
- Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;
- 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;
- Deve possuir repositório central de identificadores de dados, que podem ser utilizados para a criação de políticas contra possíveis vazamentos de informações;
- Deve permitir a investigação de incidentes de vazamento de informação através de um número identificador de incidentes.

SERVIÇO DE SUPORTE ESPECIALIZADO PARA INSTALAÇÃO, MIGRAÇÃO E SUPORTES CORRETIVO E PREVENTIVO PARA 24 (VINTE E QUATRO) MESES:

- Serviço de suporte especializado para ajustes, configurações, migrações e implementação da solução a ser fornecida.

- Além do serviço inicial de instalação e configuração, neste serviço deverá estar incluso todo tipo de suporte para funcionamento da solução, seja este corretivo ou preventivo, bem como a transferência de conhecimento.
- A Defensoria Pública não dispõe de um corpo técnico suficiente para absorver atividades e atender demandas relativas ao escopo, o que nos obriga a contratar serviços técnicos especializados para tais necessidades.
- Para prestação destes serviços, a contratada deverá empregar funcionários devidamente qualificados na utilização desse tipo de ferramenta, a ser comprovado através de apresentação de certificados emitidos pelo próprio fabricante, ou instituições por ele autorizados.

5. PROPOSTA DE MODELOS A SEREM UTILIZADOS

Os modelos a serem utilizados devem ser como os especificados no Registro de Preço da Defensoria Pública do estado do Pará:

6. INFORMAÇÕES COMPLEMENTARES

Não há

Belém, 06 de junho de 2021.

(ASSINATURA DOS MEMBROS DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO)