ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

1 – ÁREA REQUISITANTE DA SOLUÇÃO	
Unidade: COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO - CMTI	
Chefia da área: Nayana Santos Martins Neiva Sobral	
E-mail: cmti@mpma.mp.br	Telefone: (98) 3219-1773
Nome do Projeto (se houver): Formação de Registro de Preços para aquisição de renovação de licenças Kaspersky Endpoint Security for Business Select Brazilian Edition com upgrade para ADVANCED, para fins de proteção da rede lógica, equipamentos de TI e informações, por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses.	

2 – ALINHAMENTO ESTRATÉGICO

Objetivo Estratégico da PGJMA a ser atendido com a solução:

- A aquisição da solução foi prevista e planejada no Plano Diretor de Tecnologia da Informação – PDTI 2016-2021, sob o objetivo de contribuição (desdobramento tático) nº. 03 – Garantir a Segurança da Informação, através do projeto CMTI n. 30 – Implantar os controles do Sistema de Gestão da Segurança da Informação, alinhado aos objetivos estratégicos da instituição n. 16 – Ampliar a segurança institucional aos membros e servidores e nº. 26 – Aperfeiçoar a infraestrutura e segurança de TI, ambos, existentes no Planejamento Estratégico Institucional 2016-2021.

3 – MOTIVAÇÃO DA CONTRATAÇÃO

Objeto da contratação: Formação de Registro de Preços para aquisição de renovação de licenças Kaspersky Endpoint Security for Business Select Brazilian Edition com upgrade para ADVANCED, para fins de proteção da rede lógica, equipamentos de TI e informações, por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses.

Necessidade institucional:

- Considerando a necessidade de garantir o controle e prevenção de ataques informatizados, oriundos de vírus e software maliciosos, ou demais mecanismos informatizados que violem a segurança das informações eletrônicas;
- Considerando a necessidade de dotar a Instituição de software licenciado e original que contemple uma base de dados constantemente atualizada, além do mapeamento de novos vírus que surgem diariamente e suas respectivas proteções (vacinas), a fim de evitar prejuízos aos equipamentos de tecnologia da informação (TI) e informações eletrônicas da Instituição;
- A solução de segurança e proteção antivírus atua na defesa contra vírus, *ransomwares* e outras ameaças que surgem a cada segundo na rede mundial de computadores (Internet), além de nos permitir a utilização de software para controle de acesso, identificação, contingência e eliminação de códigos e limpeza de mensagens maliciosas via servidores de e-mail, controle de detecção de intrusão, geração e emissão de relatórios e gerenciamento centralizado, além de nos proporcionar o bom funcionamento e proteção dos dados e informações sigilosas;

- Atualmente, a Instituição possui ferramentas de defesa (antivírus), tendo reduzido a praticamente zero o número de incidentes devido a vírus e outras ameaças virtuais nas estações de trabalho e equipamentos servidores. Com isso, faz-se necessário dar continuidade ao uso destas licenças de forma a padronizar as configurações e uniformizar o gerenciamento da solução, haja vista que o licenciamento finda neste exercício;
- Considerando que a ferramenta de gerenciamento e a base de dados de antivírus, já utilizada para realizar essa proteção na Instituição, está com seu licenciamento em vias de expirar e desatualizar-se;
- Considerando que a solução atual de antivírus encontra-se implantada em todos os computadores distribuídos nas unidades da Capital e Interior do Estado;
- Considerando que, com a implantação do sistema de antivírus na rede da Instituição, com gerenciamento centralizado, reduziu-se os casos de infecção por vírus no ambiente computacional e eliminou-se a perda de produtividade causada pelas interrupções nos trabalhos administrativos e finalísticos, bem como otimizou a utilização dos recursos humanos ligados à manutenção da infraestrutura de tecnologia da informação;
- Tendo em vista a impossibilidade de se definir, de forma prévia e precisa, o quantitativo de materiais e serviços a serem demandados, sugere-se a realização de licitação na modalidade de pregão, ata de registro de preços do tipo menor preço ou maior desconto, nos termos do inciso XLI, artigo 6º, da lei 14.133/2021;
- Com relação ao Art. 15, inc. V, da Instrução Normativa nº02/2008-MPOG, por se tratar de um registro de preços, o quantitativo definido não significa, necessariamente, que serão adquiridos na sua totalidade, porém é importante que se tenha esse quantitativo para atendimento da demanda atual e reserva técnica, caso necessário.

Resultados esperados:

- Proteger os dispositivos e dados da instituição, contra ameaças conhecidas e avançadas, como ransomware, malware e ataques de dia zero;
- Detectar, entender e responder a ataques sofisticados, realizando análise de causa raiz e remediação;
- Economizar recursos e simplificar o gerenciamento de soluções de Segurança da Informação;
- Garantir a conformidade com as normas e regulamentos de segurança cibernética do setor público.

Indicação de soluções, paradigmas (se houver):

- Considerando o inciso I, do artigo 41, da Lei 14.133/2021, faz-se necessária a padronização e indicação de marca para a manutenção da proteção atual de ativos de rede (Antivírus), de forma homogênea, no parque computacional do MPMA. Disto, justifica-se a manutenção da marca, devido ao/à:
- **Gerenciamento**: todas as configurações do software de gerenciamento centralizado da solução atual poderão ser aproveitadas sem nenhuma janela de migração, bem como todos os

equipamentos que atualmente são gerenciados irão manter as informações de conexão, gerenciamento e sincronização podem ser configurados e administrados por uma única console proporcionando;

- **Configuração e conhecimento**: a padronização dos equipamentos auxilia e facilita a administração da rede, devido a utilização de apenas um sistema operacional em todos os equipamentos, ou seja, uma única interface de comandos a serem utilizados para configuração de toda a rede. Com isso, torna-se mais fácil o treinamento, a gestão do conhecimento, e auxilia na redução do tempo de configuração e reparo. Este convém a citar o princípio da eficiência.
- **Desempenho**: soluções de mesmo fabricante permitem a utilização de recursos proprietários, ou seja, recursos que garantem maior desempenho dos equipamentos, mas que só podemos utilizá-los com a homogeneidade da malha, como configurações de alta disponibilidade essenciais às necessidades deste Ministério Público.

4 – INDICAÇÃO DO INTEGRANTE REQUISITANTE	
Nome: Diego Walisson Pereira Camara Santos	Telefone: (98) 3219-1773
ASSINATURA: DIEGO WALISSON PEREIRA CAMARA SANTOS:1070278 — Assinado de forma digital por DIEGO WALISSON PEREIRA CAMARA SANTOS:1070278 Dados: 2023.06.12 11:52:53 -03'00'	

ANÁLISE DO DOD

1 – ÁREA DE TECNOLOGIA DA INFORMAÇÃO	
Chefia da área: Nayana Santos Martins Neiva Sobral	
E-mail: cmti@mpma.mp.br	Telefone: (98) 3219-1773

2 – ANÁLISE DA DEMANDA				
Há previsão no PDTI?	X	SIM		NÃO
Manifestação: Sugerindo a continuidade do pleito.				
Favorável ao prosseguimento?	X	SIM		NÃO

3 – DISPONIBILIDADE ORÇAMENTÁRIA				
Há disponibilidade orçamentária?		SIM	X	NÃO
Elemento de Despesa:		Valor disponível:		

4 – COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO				
Manifestação: N/A – Não se aplica. Visto que a referida demanda já se encontra prevista no PDTI 2017-2021.				
Autorizado o prosseguimento?	X	SIM		NÃO

5 – INDICAÇÃO DO INTEGRANTE TÉCNICO	
Nome: Leonardo Dorneles Figueiredo Silva	Telefone: (98) 3219-1773
	ASSINATURA: LEONARDO DORNELES FIGUEIREDO SILVA:1071397 Assinado de forma digital por LEONARDO DORNELES FIGUEIREDO SILVA:1071397 Dados: 2023.06.12 12:00:48 -03'00'

ANÁLISE DA VIABILIDADE DA CONTRATAÇÃO

1 – SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO
Características: Formação de Registro de Preços para aquisição de renovação de licenças Kaspersky Endpoint Security for Business Select Brazilian Edition com upgrade para ADVANCED, para fins de proteção da rede lógica, equipamentos de TI e informações, por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses.

2 – IDENTIFICAÇÃO DAS DIFERENTES SOLUÇÕES
Soluções de mercado: Não se aplica.
Projetos similares: Não se aplica.

3 – REQUISITOS DA CONTRATAÇÃO
Requisitos de Negócio: - Em 2021 o MPMA iniciou um processo de atualização da proteção de rede que compõe sua infraestrutura (Antivírus), juntamente com um software para gerenciamento centralizado dos mesmos. - Com intuito de garantir o melhor desempenho, disponibilidade e estabilidade da Rede Corporativa que, cada vez mais, está sendo utilizada para tráfego sigiloso e sensível do GESP, DIGIDOC e SIMP, faz-se necessário o uso de políticas, protocolos e tecnologias que visam, principalmente, garantir a segurança das informações e o melhor desempenho dos serviços e aplicações. - A criação de políticas de segurança e perfis de acesso do tráfego de dados estão, estreitamente, ligadas às características próprias de cada componente que compõem a solução de antivírus atual. Desse modo, diferentes fabricantes de software antivírus podem apresentar diferentes parâmetros de configuração e de otimização para proteção de diferentes modelos de equipamentos de um mesmo fabricante, resultando numa gestão de proteção de ativos ineficiente. - Consequentemente, à aquisição de soluções de Antivírus, de fabricantes diferentes (heterogeneidade), obriga uma reconfiguração dos equipamentos, reconstrução das políticas, reinstalação de todos os clientes, além da curva de aprendizado da própria equipe de Administração de rede da CMTI. - A falta de uma padronização também não garante a gerenciabilidade do parque, ficando, dessa forma, comprometida a interoperabilidade e o gerenciamento integrado. - É necessário garantir a continuidade da proteção de rede que existe, atualmente, no parque computacional do MPMA, de modo a evitar pontos de falha de segurança e um período longo de exposição insegura do parque computacional até implantação de nova solução, em caso de aquisição de antivírus de fabricante distinto do atual.
Requisitos de Capacitação:

- A CONTRATADA deverá comprovar na data da Assinatura do CONTRATO que a equipe técnica que realizará a instalação será composta por profissionais que possuam, no mínimo, as certificações a seguir:
  - Certificação emitida pelo FABRICANTE, que fornece ao profissional a validação da proficiência necessária para a instalação, configuração e administração da solução;
  - A comprovação da capacitação técnica dar-se-á mediante a apresentação de certificado(s) de cada instituição/FABRICANTE. As certificações deverão ser obrigatoriamente técnicas e do mesmo FABRICANTE dos produtos cotados. Não serão aceitas certificações comerciais;

Requisitos de Manutenção:

- Os chamados de assistência técnica, durante o período de garantia de 36 (trinta e seis) meses, deverão ser abertos pela CONTRATANTE, junto à CONTRATADA ou empresa por ele indicada formalmente por escrito ou através de uma Central de Atendimento;
- Os serviços de abertura de chamados deverão estar disponíveis em regime 24x7;
- O atendimento para a assistência técnica será em horário integral, todos os dias da semana, on-site, em São Luís – MA;
- A CONTRATADA deverá disponibilizar linha telefônica gratuita (0800) ou equivalente ao custo de ligação local, além de e-mail, web site e via acesso remoto ilimitado para abertura de chamados de suporte técnico na Central de Atendimento do fabricante ou fornecedor;
- Todos os chamados, inclusive os que podem resultar em manutenção de natureza corretiva, bem como o fluxo de resolução de problemas, deverão ser documentados. Esta documentação, bem como outras geradas em processos de atendimento, auditorias, manutenção ou configurações, deverá ser entregue à CONTRATANTE através de relatórios (impressos ou em mídia digital) mediante solicitação;
- O serviço de suporte deverá contemplar também atualizações de versões, assinaturas e engines;
- Anexar declaração do FABRICANTE, afirmando que disponibilizará estrutura de suporte de segundo nível ao CONTRATANTE, caso seja vencedor do processo, ou declaração do FABRICANTE comprometendo-se a disponibilizar estrutura de suporte, durante o período de garantia/suporte contratado;
- A CONTRATADA deverá fazer análises dos chamados e enviar recomendações de possíveis treinamentos necessários ao desenvolvimento da equipe da CONTRATANTE;
- A CONTRATADA deverá apresentar relatório contendo as ações adotadas para a solução do problema;
- A CONTRATADA deverá disponibilizar à CONTRATANTE serviço de atendimento de um Gestor do contrato de Suporte, responsável este que será o ponto focal de todas as necessidades de suporte da CONTRATANTE para casos de escalações ou problemas de atendimento do Suporte Técnico. Caso a CONTRATADA tenha seus laboratórios em outros países que não seja o território nacional, o Gestor deverá ter fluência na língua para facilitar a comunicação entre as partes;

- A CONTRATANTE permitirá o acesso dos técnicos credenciados pela CONTRATADA às instalações onde se encontrarem os equipamentos para a prestação dos serviços de manutenção. Entretanto, tais técnicos ficarão sujeitos às normas internas de segurança da CONTRATANTE, notadamente àquelas atinentes à identificação, trânsito e permanência nas dependências;
- Mesmo se permitido pela CONTRATANTE, a permanência do técnico além do tempo de resolução do problema, para a continuidade de solução de um problema, não deverá representar qualquer ônus adicional à CONTRATANTE.

Requisitos de Prazo:

- As licenças de uso dos softwares solicitados pela CONTRATANTE deverão ser entregues para utilização, **no prazo máximo de 30 (trinta) dias corridos**, a contar da data de assinatura do CONTRATO, que será encaminhado pela Comissão Permanente de LICITAÇÃO (CPL);
- O objeto deste TERMO DE REFERÊNCIA deverá ser entregue na Coordenadoria de Modernização e Tecnologia da Informação – CMTI, localizada no prédio sede da PROCURADORIA GERAL DE JUSTIÇA DO ESTADO DO MARANHÃO - PGJMA, Segundo Pavimento, na Avenida Professor Carlos Cunha, s/nº – JARACATI – CEP: 65076-820 – SÃO LUÍS – MA – TELEFONE: (98) 3219-1773, no horário das 08:00hs às 13:00hs, em dias úteis, de segunda-feira a sexta-feira;
- A CONTRATADA deverá comunicar, com a antecedência mínima de 02 (dois) dias úteis, ao Gestor do CONTRATO, a data da entrega dos produtos, licenças e serviços;
- Antes de findar o prazo fixado nos itens anteriores, a empresa CONTRATADA poderá formalizar pedido de sua prorrogação, cujas razões expostas serão examinadas pela CONTRATANTE, que decidirá pela prorrogação ou não do prazo ou aplicação das penalidades previstas no CONTRATO;
- O recebimento do produto será feito nos termos dos Art. 140, II da Lei n° 14.133/21:
- O **Recebimento Provisório** do objeto, para efeito de posterior verificação da sua conformidade, será realizado pelo Fiscal do contrato, mediante termo circunstanciado assinado pelas partes, até o 5º (quinto) dia da apresentação da nota fiscal;
- O **Recebimento Definitivo** será realizado pelo Gestor do contrato, mediante termo circunstanciado assinado pelas partes, após o decurso do prazo para observação ou vistoria que comprove a adequação do objeto aos termos contratuais, não superior a 90 (noventa) dias;
- Caso os objetos entregues (por e-mail ou em mídia física) apresentem defeito ou não atendam às especificações técnicas estabelecidas neste Termo de Referência, a CONTRATADA terá o prazo de 05 (cinco) dias úteis, contados a partir da data da notificação, para substituir o software que apresentar falhas.

4 - REQUISITOS TÉCNICOS

Legais: O objeto deve estar em conformidade com descrição constante na Estratégia da Contratação, em seu item 2 – DETALHAMENTO DOS BENS E SERVIÇOS QUE COMPÕEM A SOLUÇÃO.

Da arquitetura tecnológica: Não se aplica.

De implantação: As licenças de uso dos softwares solicitados pela CONTRATANTE deverão ser entregues para utilização, **no prazo máximo de 30 (trinta) dias corridos**, a contar da data de assinatura do CONTRATO, que será encaminhado pela Comissão Permanente de LICITAÇÃO (CPL).

De garantia e manutenção:

- A CONTRATADA deverá garantir à CONTRATANTE que os softwares licenciados não infrinjam quaisquer patentes, direitos autorais ou "*trade-secrets*";
- A garantia deverá ser prestada pelo período de, no mínimo, **36 (trinta e seis) meses**, a contar do recebimento definitivo do objeto do CONTRATO, sem nenhum custo adicional para a CONTRATANTE, abrangendo a manutenção corretiva com a cobertura de todo e qualquer defeito apresentado, incluindo substituição de peças, partes, mídias, softwares, componentes e acessórios, correções de defeitos que afetem o desempenho, funcionalidade e/ou configuração dos produtos e atualização da versão de novos "*releases*" das licenças de software que incorporem melhorias tecnológicas de desempenho e/ou funcionais (suporte técnico e manutenção), além de eventuais *patches* de segurança e vacinas que surjam durante a vigência da garantia da solução ofertada;
- A CONTRATADA deverá garantir que os programas licenciados para o CONTRATANTE operarão, em todos os aspectos essenciais, da forma descrita na respectiva documentação, desempenhando as funções devidamente contratadas;
    - A garantia a que se refere o Caput desta Cláusula inclui todas as ações, sejam elas de manutenção ou outras necessárias, com vistas a garantir o perfeito funcionamento da plataforma licitada, assim como o atendimento às necessidades do CONTRATANTE;
- Todas as despesas envolvidas no processo de suporte correrão por conta da CONTRATADA, inclusive as despesas com frete de envio e retorno de profissionais técnicos ou componentes da Solução, sem ônus adicional à CONTRATANTE;
- A CONTRATADA deverá disponibilizar linha telefônica em horário comercial, de segunda-feira a sexta-feira, das 08:00hs as 18:00hs, além de e-mail e web site, sem ônus para a CONTRATANTE, visando a abertura e agilização dos chamados e atendimentos técnicos durante a vigência da garantia técnica;
    - Entende-se por hora da solicitação a hora de envio do e-mail, web ou da chamada telefônica;
    - Entende-se por início do atendimento a hora de chegada do técnico ao local determinado no chamado ou a sua atuação de forma remota;
    - Poderá ser solicitado o atendimento *on-site*, restrito ao município-sede do CONTRATANTE, visando à resolução de problemas que não forem solucionados através do atendimento telefônico ou remoto;
    - A CONTRATADA deve possuir pessoal certificado pelo FABRICANTE para a integral execução e manutenção dos serviços;

    - A garantia "*on-site*" deverá observar os prazos estabelecidos neste TERMO DE REFERÊNCIA, contados a partir da data e hora do chamado, com tempo de resposta e solução indicados na proposta, de acordo com item 12;

- Deverá ser informado link (URL) de site na Internet do FABRICANTE da solução ofertada com disponibilidade de informações para suporte, tais como: guias de instalação, informações técnicas, atualização e download de *drivers*, *firmwares*, *upgrade* de BIOS, etc.

- Os técnicos, ou pessoas autorizadas pela CONTRATADA, deverão apresentar, no ato do atendimento, credenciamento (crachá da CONTRATADA) e documento de identidade pessoal (RG), para efetuarem qualquer serviço nas dependências da CONTRATANTE;

- Durante a execução dos serviços o ambiente de trabalho deverá ser mantido em perfeitas condições de higiene e segurança, sendo que, após a conclusão dos serviços deverá ser efetuada limpeza geral no ambiente, decorrente da atuação do técnico;

- Após cada atendimento técnico, a CONTRATADA deverá emitir, no ato, relatório técnico do atendimento onde deverão constar, obrigatoriamente, os seguintes dados: data e horário da abertura do chamado, horário de início e término do atendimento, número do chamado, nome do técnico responsável pelo atendimento, descrição do problema relatado pela CONTRATANTE, descrição do problema realmente encontrado com a solução dada ao problema e local para atesto dos servidores da CONTRATANTE.

    - A CONTRATADA deverá deixar cópia do relatório com servidor da CONTRATANTE responsável pelo acompanhamento do atendimento técnico;

- A CONTRATADA compromete-se a manter registros escritos dos referidos chamados constando o nome do técnico da CONTRATADA e uma descrição resumida do problema.

- Os chamados de assistência técnica, durante o período de garantia de 36 (trinta e seis) meses, deverão ser abertos pela CONTRATANTE, junto à CONTRATADA ou empresa por ele indicada formalmente por escrito ou através de uma Central de Atendimento;

- Os serviços de abertura de chamados deverão estar disponíveis em regime 24x7;

- O atendimento para a assistência técnica será em horário integral, todos os dias da semana, on-site, em São Luís – MA;

- A CONTRATADA deverá disponibilizar linha telefônica gratuita (0800) ou equivalente ao custo de ligação local, além de e-mail, web site e via acesso remoto ilimitado para abertura de chamados de suporte técnico na Central de Atendimento do fabricante ou fornecedor;

- Todos os chamados, inclusive os que podem resultar em manutenção de natureza corretiva, bem como o fluxo de resolução de problemas, deverão ser documentados. Esta documentação, bem como outras

geradas em processos de atendimento, auditorias, manutenção ou configurações, deverá ser entregue à CONTRATANTE através de relatórios (impressos ou em mídia digital) mediante solicitação;

- O serviço de suporte deverá contemplar também atualizações de versões, assinaturas e engines;
- Anexar declaração do FABRICANTE, afirmando que disponibilizará estrutura de suporte de segundo nível ao CONTRATANTE, caso seja vencedor do processo, ou declaração do FABRICANTE comprometendo-se a disponibilizar estrutura de suporte, durante o período de garantia/suporte contratado;
- A CONTRATADA deverá fazer análises dos chamados e enviar recomendações de possíveis treinamentos necessários ao desenvolvimento da equipe da CONTRATANTE;
- A CONTRATADA deverá apresentar relatório contendo as ações adotadas para a solução do problema;
- A CONTRATADA deverá disponibilizar à CONTRATANTE serviço de atendimento de um Gestor do contrato de Suporte, responsável este que será o ponto focal de todas as necessidades de suporte da CONTRATANTE para casos de escalações ou problemas de atendimento do Suporte Técnico. Caso a CONTRATADA tenha seus laboratórios em outros países que não seja o território nacional, o Gestor deverá ter fluência na língua para facilitar a comunicação entre as partes;
- A CONTRATANTE permitirá o acesso dos técnicos credenciados pela CONTRATADA às instalações onde se encontrarem os equipamentos para a prestação dos serviços de manutenção. Entretanto, tais técnicos ficarão sujeitos às normas internas de segurança da CONTRATANTE, notadamente àquelas atinentes à identificação, trânsito e permanência nas dependências;
- Mesmo se permitido pela CONTRATANTE, a permanência do técnico além do tempo de resolução do problema, para a continuidade de solução de um problema, não deverá representar qualquer ônus adicional à CONTRATANTE.

De capacitação Técnica:

- A CONTRATADA deverá comprovar na data da Assinatura do CONTRATO que a equipe técnica que realizará a instalação será composta por profissionais que possuam, no mínimo, as certificações a seguir:
  - Certificação emitida pelo FABRICANTE, que fornece ao profissional a validação da proficiência necessária para a instalação, configuração e administração da solução;
  - A comprovação da capacitação técnica dar-se-á mediante a apresentação de certificado(s) de cada instituição/FABRICANTE. As certificações deverão ser obrigatoriamente técnicas e do mesmo FABRICANTE dos produtos cotados. Não serão aceitas certificações comerciais;

De formação e experiência profissional da equipe que projetará, implementará e implantará a Solução de TI:

- Visando a garantir a qualidade dos serviços ofertados, a CONTRATADA deverá, até 05 (cinco) dias após a **data de assinatura do Contrato**, comprovar que possui em seu corpo técnico permanente, pelo menos 01 (um) técnico com certificação oficial fornecida pelo(s) FABRICANTE(s) dos produtos

(equipamentos e licenças). A comprovação de possuir profissional no quadro permanente far-se-á mediante a apresentação de um dos seguintes documentos:

- Cópia da Carteira de Trabalho e Previdência Social – CTPS;
- Cópia do ato de investidura do cargo ou cópia do Contrato social, quando se tratar de diretor ou sócio;
- Contrato de prestação de serviços, regido pela legislação comum.

De metodologia de trabalho: N/A – Não se aplica.

De segurança da informação:

- Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da CONTRATANTE, ou de terceiros de que tomar conhecimento em razão da execução do objeto do CONTRATO, devendo orientar seus empregados nesse sentido;
- Não veicular publicidade acerca dos serviços contratados, sem prévia autorização, por escrito, da CONTRATANTE;
- Manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do CONTRATO, as informações relativas:

6.5.1 À política de segurança adotada pela CONTRATANTE e as configurações de hardware e de softwares decorrentes;

6.5.2 Ao processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos;

6.5.3 Ao processo de implementação, no ambiente da Contratante, dos mecanismos de criptografia e autenticação.

5 – DEMANDA DOS GESTORES

Descrição: N/A - Não se aplica

6 – ANÁLISE DAS ALTERNATIVAS EXISTENTES

Requisito	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	X		
A Solução está disponível no Portal do Software Público Brasileiro?			X
A Solução é um software livre ou software público?			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?			X
A Solução é aderente às regulamentações da ICP-Brasil? (Quando houver necessidade de certificação digital)			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do – e-ARQ Brasil?			X

7 – SOLUÇÃO ESCOLHIDA
Descrição: Kaspersky
Fundamentação: - Considerando o inciso I, do artigo 41, da Lei 14.133/2021, faz-se necessária a padronização e indicação de marca para a manutenção da proteção atual de ativos de rede (Antivírus), de forma homogênea, no parque computacional do MPMA. Disto, justifica-se a manutenção da marca, devido ao/à: - **Gerenciamento**: todas as configurações do software de gerenciamento centralizado da solução atual poderão ser aproveitadas sem nenhuma janela de migração, bem como todos os equipamentos que atualmente são gerenciados irão manter as informações de conexão, gerenciamento e sincronização podem ser configurados e administrados por uma única console proporcionando; - **Configuração e conhecimento**: a padronização dos equipamentos auxilia e facilita a administração da rede, devido a utilização de apenas um sistema operacional em todos os equipamentos, ou seja, uma única interface de comandos a serem utilizados para configuração de toda a rede. Com isso, torna-se mais fácil o treinamento, a gestão do conhecimento, e auxilia na redução do tempo de configuração e reparo. Este convém a citar o princípio da eficiência. - **Desempenho**: soluções de mesmo fabricante permitem a utilização de recursos proprietários, ou seja, recursos que garantem maior desempenho dos equipamentos, mas que só podemos utilizá-los com a homogeneidade da malha, como configurações de alta disponibilidade essenciais às necessidades deste Ministério Público.

8 – ADEQUAÇÃO DO AMBIENTE		
Descrição das necessidades: Não se aplica		
Ações para adequação do ambiente	Responsável:	Prazo:

	INTEGRANTE REQUISITANTE	INTEGRANTE TÉCNICO
	Nome: Diego Walisson Pereira Camara Santos	Nome: Leonardo Dorneles Figueiredo Silva
	Assinatura: DIEGO WALISSON PEREIRA CAMARA SANTOS:1070278 Assinado de forma digital por DIEGO WALISSON PEREIRA CAMARA SANTOS:1070278 Dados: 2023.06.12 11:53:11 -03'00'	Assinatura: LEONARDO DORNELES FIGUEIREDO SILVA:1071397 Assinado de forma digital por LEONARDO DORNELES FIGUEIREDO SILVA:1071397 Dados: 2023.06.12 12:01:11 -03'00'

ANÁLISE DE RISCOS

1 – RISCOS DO PROCESSO DE CONTRATAÇÃO
Frustração da contratação: Indisponibilidade de recursos orçamentários; Falta de documentação/certidões atualizadas durante a fase de contratação; Demora na instrução dos autos para análise interna da Administração.
Gestão contratual - frustração do contrato: Não atendimento das cláusulas contratuais de obrigatoriedade da empresa contratada; Falha no fornecimento do objeto; Não atendimento dos requisitos pela empresa.

Ações preventivas: manter toda a documentação necessária para o procedimento de contratação.
Responsável: Daniela Nascimento Montelo
Procedimentos de contingência: utilizar solução de antivírus baseada em software livre.
Responsável: Leonardo Dorneles Figueiredo Silva

2 – RISCOS DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO
De não alcançar os resultados e deixar de atender as necessidades: expirar o licenciamento vigente da solução de proteção de rede do MPMA.
Ações preventivas: Efetuar contratação emergencial dos serviços.
Responsável: Nayana Santos Martins Neiva Sobral
Procedimentos de contingência: utilizar solução de antivírus baseada em software livre.
Responsável: Leonardo Dorneles Figueiredo Silva

	INTEGRANTE REQUISITANTE	INTEGRANTE TÉCNICO
	Nome: Diego Walisson Pereira Camara Santos	Nome: Leonardo Dorneles Figueiredo Silva
	Assinatura: DIEGO WALISSON PEREIRA CAMARA SANTOS:1070278 Assinado de forma digital por DIEGO WALISSON PEREIRA CAMARA SANTOS:1070278 Dados: 2023.06.12 11:53:23 -03'00'	Assinatura: LEONARDO DORNELES FIGUEIREDO SILVA:1071397 Assinado de forma digital por LEONARDO DORNELES FIGUEIREDO SILVA:1071397 Dados: 2023.06.12 12:01:36 -03'00'

PLANO DE SUSTENTAÇÃO

1 – INTRODUÇÃO
Descrição: visa a continuidade e manutenção da solução de proteção de rede, alinhada à conformidade preconizada na política Institucional de segurança da informação, ATO-REG-72020, no período de vigência sugerido para a contratação, garantindo-se os mesmos acordos de níveis de serviços, atualmente existentes, e qualidade de serviço.

2 – ESTRATÉGIA DE CONTINUIDADE CONTRATUAL			
Incapacidade de execução total ou parcial dos serviços pela Contratada	Ação de Contingência		Responsável
	1	Utilizar solução de antivírus baseada em software livre.	Leonardo Dorneles Figueiredo Silva
	2		

3 – TRANSIÇÃO E ENCERRAMENTO CONTRATUAL			
	Ação	Responsável	Prazo Máximo
	N/A	N/A	N/A

5 – ESTRATÉGIA DE INDEPENDÊNCIA (transferência de conhecimento)		
	Ação	Forma de execução
1	N/A	N/A

	INTEGRANTE REQUISITANTE	INTEGRANTE TÉCNICO
	Nome: Diego Walisson Pereira Camara Santos	Nome: Leonardo Dorneles Figueiredo Silva
	Assinatura: DIEGO WALISSON PEREIRA CAMARA SANTOS:1070278 Assinado de forma digital por DIEGO WALISSON PEREIRA CAMARA SANTOS:1070278 Dados: 2023.06.12 11:53:35 -03'00'	Assinatura: LEONARDO DORNELES FIGUEIREDO SILVA:1071397 Assinado de forma digital por LEONARDO DORNELES FIGUEIREDO SILVA:1071397 Dados: 2023.06.12 12:02:05 -03'00'

ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA

RESUMO DE CONSULTA AO MERCADO

Pesquisa realizada no Painel de Preços do Governo Federal

TABELA DE VALORES POR PROPOSTA					
Órgão Contratante	**Empresa**	**ITEM**	**Quantidade**	**Preço Unitário (R$)**	**Preço Total (R$)**
UASG: 158143 - INST.FED.DE EDUC.,CIENC.E TEC.DE BRASILIA	**VTECH COMERCIO, SERVICOS E EQUIPAMENTOS DE INFORMATICA LTDA**	Atualização de licença de software antivírus Kaspersky Endpoint Security for Business Select Brazilian Edition, por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses, e demais detalhamentos descritos no termo de referência.	3000	R$ 96,66	R$ 289.980,00
		Aquisição de licença de software antivírus Kaspersky Endpoint Security for Business Select Brazilian Edition, para fins de proteção da rede lógica, equipamentos de TI e informações, por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses, e demais detalhamentos descritos no termo de referência.	1000	R$ 96,66	R$ 96.660,00
				VALOR UNITÁRIO E TOTAL	**R$ 193,32**	**R$ 386.640,00**
UASG: 925125 - TRIBUNAL DE JUSTIÇA DO ESTADO DO MARANHÃO/MA	**NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**	Atualização de licença de software antivírus Kaspersky Endpoint Security for Business Select Brazilian Edition, por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses, e demais detalhamentos descritos no termo de referência.	3000	R$ 143,00	R$ 429.000,00

		Aquisição de licença de software antivírus Kaspersky Endpoint Security for Business Select Brazilian Edition, para fins de proteção da rede lógica, equipamentos de TI e informações, por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses, e demais detalhamentos descritos no termo de referência.	1000	R$ 143,00	R$ 143.000,00
	VALOR UNITÁRIO E TOTAL			**R$ 286,00**	**R$ 572.000,00**
UASG: 926753 - CONSELHO REG.DOS REPRESENTANTES COMERCIAIS-SP	**NETWORK SECURE SEGURANCA DA INFORMACAO LTDA**	Atualização de licença de software antivírus Kaspersky Endpoint Security for Business Select Brazilian Edition, por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses, e demais detalhamentos descritos no termo de referência.	3000	R$ 229,00	R$ 687.000,00
		Aquisição de licença de software antivírus Kaspersky Endpoint Security for Business Select Brazilian Edition, para fins de proteção da rede lógica, equipamentos de TI e informações, por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses, e demais detalhamentos descritos no termo de referência.	1000	R$ 229,00	R$ 229.000,00
	VALOR UNITÁRIO E TOTAL			**R$ 458,00**	**R$ 916.000,00**

ESTRATÉGIA DA CONTRATAÇÃO

1 – SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO A SER CONTRATADA
Descrição: Aquisição de renovação de licenças Kaspersky Endpoint Security for Business Select Brazilian Edition com upgrade para ADVANCED, para fins de proteção da rede lógica, equipamentos de TI e informações, por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses.

2 – DETALHAMENTO DOS BENS E SERVIÇOS QUE COMPÕEM A SOLUÇÃO
Descrição: - O objeto deverá ser entregue de acordo com as especificações técnicas a seguir:

- **Estações de Trabalho Windows nas versões 32 e 64 bits**
- Compatibilidade:
    - Microsoft Windows 10/11 Pro / Enterprise x86 / x64;
- **Estações de Trabalho Linux nas versões 32 e 64 bits**
    - Compatibilidade:
        - Ubuntu 18.04 32/64 bits ou superiores;
- **Servidores Windows nas versões 32 e 64 bits**
    - Compatibilidade:
        - Windows Server 2008 Standard/Enterprise/Datacenter SP1 e posterior nas versões 32 e 64 bits;
        - Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;
        - Windows Server 2016 Essentials/Standard/Datacenter/MultiPoint Premium Server;
- **Servidores Linux nas versões 32 e 64 bits**
    - Compatibilidade:
        - Red Hat® Enterprise Linux® 7 Server e/ou superiores;
        - CentOS-7 e/ou superiores;
        - Ubuntu 18.04.2 LTS e/ou superiores;
        - Debian GNU / Linux 10 e/ou superiores;
        - **Deve prover as seguintes proteções:**
    - Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
    - Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
    - Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
    - O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
    - Firewall com IDS;
    - Autoproteção (contra-ataques aos serviços/processos do antivírus);
    - Controle de dispositivos externos;
    - Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;
    - Controle de execução de aplicativos;

- Controle de vulnerabilidades do Windows e dos aplicativos instalados;
- Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
- Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
- Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;

- **Servidor de Administração e Console Administrativa**
  - Compatibilidade
    - Microsoft Windows Server 2008/2012/2016 (todas as edições) em 32 ou 64 bits;
    - Vmware: vSphere 5.5, vSphere 6 e superiores;
  - Características
    - A console deve ser acessada via WEB (HTTPS) ou MMC;
    - Console deve ser baseada no modelo cliente/servidor;
    - Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;

- Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
- Deve permitir incluir usuários do AD para logarem na console de administração
- Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;
- As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
- Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
- Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
- Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
- Deve armazenar histórico das alterações feitas em políticas;
- Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;
- Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;
- A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
- Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
- Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS e Android;
- Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;

- A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
- Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;
- Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
- Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;
- Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;
- Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
- Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
- Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;
- A comunicação entre o cliente e o servidor de administração deve ser criptografada;
- Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
- Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual.

3 – REQUISITOS DA CONTRATAÇÃO

Necessidades do Negócio:

- Considerando a necessidade de garantir o controle e prevenção de ataques informatizados, oriundos de vírus e software maliciosos, ou demais mecanismos informatizados que violem a segurança das informações eletrônicas;
- Considerando a necessidade de dotar a Instituição de software licenciado e original que contemple uma base de dados constantemente atualizada, além do mapeamento de novos vírus que surgem diariamente e suas respectivas proteções (vacinas), a fim de evitar prejuízos aos equipamentos de tecnologia da informação (TI) e informações eletrônicas da Instituição;
- A solução de segurança e proteção antivírus atua na defesa contra vírus, *ransowares* e outras ameaças que surgem a cada segundo na rede mundial de computadores (Internet), além de nos permitir a

utilização de software para controle de acesso, identificação, contingência e eliminação de códigos e limpeza de mensagens maliciosas via servidores de e-mail, controle de detecção de intrusão, geração e emissão de relatórios e gerenciamento centralizado, além de nos proporcionar o bom funcionamento e proteção dos dados e informações sigilosas;

- Atualmente, a Instituição possui ferramentas de defesa (antivírus), tendo reduzido a praticamente zero o número de incidentes devido a vírus e outras ameaças virtuais nas estações de trabalho e equipamentos servidores. Com isso, faz-se necessário dar continuidade ao uso destas licenças de forma a padronizar as configurações e uniformizar o gerenciamento da solução, haja vista que o licenciamento finda neste exercício;
- Considerando que a ferramenta de gerenciamento e a base de dados de antivírus, já utilizada para realizar essa proteção na Instituição, está com seu licenciamento em vias de expirar e desatualizar-se;
- Considerando que a solução atual de antivírus encontra-se implantada em todos os computadores distribuídos nas unidades da Capital e Interior do Estado;
- Considerando que, com a implantação do sistema de antivírus na rede da Instituição, com gerenciamento centralizado, reduziu-se os casos de infecção por vírus no ambiente computacional e eliminou-se a perda de produtividade causada pelas interrupções nos trabalhos administrativos e finalísticos, bem como otimizou a utilização dos recursos humanos ligados à manutenção da infraestrutura de tecnologia da informação;
- Tendo em vista a impossibilidade de se definir, de forma prévia e precisa, o quantitativo de materiais e serviços a serem demandados, sugere-se a realização de licitação na modalidade de pregão, ata de registro de preços do tipo menor preço ou maior desconto, nos termos do inciso XLI, artigo 6º, da lei 14.133/2021;
- Com relação ao Art. 15, inc. V, da Instrução Normativa nº02/2008-MPOG, por se tratar de um registro de preços, o quantitativo definido não significa, necessariamente, que serão adquiridos na sua totalidade, porém é importante que se tenha esse quantitativo para atendimento da demanda atual e reserva técnica, caso necessário.

Responsabilidades da Contratada:

- Disponibilizar à CONTRATANTE sistema de controle de licenças fornecidas, responsabilizando-se pela atualização de informações;
- Manter, durante todo o período de vigência da Ata de Registro de Preços e do CONTRATO, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
- Emitir **Nota Fiscal/Fatura** no valor pactuado e condições do CONTRATO, apresentando-a a CONTRATANTE para ateste e pagamento;
- Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da CONTRATANTE, ou de terceiros de que tomar conhecimento em razão da execução do objeto do CONTRATO, devendo orientar seus empregados nesse sentido;

- Não veicular publicidade acerca dos serviços contratados, sem prévia autorização, por escrito, da CONTRATANTE;
- Manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do CONTRATO, as informações relativas:
- 6.5.1 À política de segurança adotada pela CONTRATANTE e as configurações de hardware e de softwares decorrentes;
- 6.5.2 Ao processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos;
- 6.5.3 Ao processo de implementação, no ambiente da Contratante, dos mecanismos de criptografia e autenticação;
- Comunicar à CONTRATANTE, por escrito, qualquer anormalidade verificada na entrega dos componentes e prestar à Instituição os devidos esclarecimentos, sempre que solicitados;
- Cumprir, às suas próprias expensas, todas as cláusulas contratuais que definam suas obrigações;
- Prestar todas as informações solicitadas pela CONTRATANTE com referência ao objeto adquirido;
- Responder integralmente pelas obrigações, contratuais nos termos da Lei 14.133/21;
- Executar fielmente o objeto contratado, de acordo com as normas legais, em conformidade com a proposta apresentada e nas orientações da CONTRATANTE, observando sempre os critérios de qualidade;
- Garantir, pelo prazo de 36 (trinta e seis) meses, a contar da data da assinatura do CONTRATO, que cada programa licenciado, não modificado, desempenha as funções contratadas;
- Deverá fornecer, no mínimo, 01 console administrativa com as seguintes Características Mínimas:
    - Compatível com estações de trabalho, nas versões 32 e 64 bits: Microsoft Windows XP, Windows 7, Windows 8, Windows 10, Windows 2000, Windows Vista e demais versões windows que surgirem durante o período de garantia e vigência contratual, e Linux Ubuntu em suas mais atuais distribuições;
    - Plataforma Server, nas versões 32 e 64 bits: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, e demais versões que surgirem durante o período de garantia e vigência contratual, e Linux UBUNTU Server em suas mais atuais distribuições;
    - Enterprise, FreeBSD, OpenBSD, Novel NetWare e Linux Servers (UBUNTU, RED HAT e CENTOS);
    - Desktops, Notebooks, Ultrabooks, Tablets e Celulares com Sistema Operacional Android;
    - Compatível com os clientes de e-mail MSExchange.MS Outlook, Outlook Express e Office 365, Google e Zimbra;
    - Ter uma console única de gerenciamento, permitindo a administração completa de todos os produtos em plataforma Microsoft Windows;
    - Provê toda comunicação entre cliente/servidor através dos protocolos de rede TCP/IP;

- Todos os módulos e/ou partes que compõem a ferramenta de proteção e prevenção efetiva aos ataques de vírus, spyware, worm, trojan, adware e outros malwares;
- Instaladores remotos capazes de instalar automaticamente em determinado período especificado;
- Provê mecanismos de instalação nos clientes (servidores e estações) através de: login ou script;
- Remotamente a partir do console único, via rede LAN e WAN; e de pacotes customizados (autoexecutáveis), dispensando a necessidade de instalações anteriores de agentes ou outros módulos adicionais no computador destino;
- Provê mecanismos de desinstalação nos clientes (servidores e estações), inclusive de outros fabricantes, de forma manual e também remoto, a partir do console único via rede LAN e WAN;
- Possui funcionalidade que permite analisar toda a rede e identificar os computadores que não estejam com antivírus instalado ou que tenham o antivírus instalado, mas desligado;
- Através do console é exibida a lista dos clientes (servidores e estações) que possuem o antivírus instalado, contendo as seguintes informações: nome da máquina, data da última atualização, status das máquinas (on-line, off-line, com vírus, etc.), endereço IP e estado da proteção em Tempo Real;
- Independente das máquinas estarem on-line ou off-line, todas as informações descritas acima estarão disponíveis;
- Permite travar / bloquear as configurações nos clientes (servidores e estações), para que somente o administrador possa alterar a configuração, desinstalar ou parar o antivírus nos clientes;
- O console possui a capacidade de aplicar mudanças na configuração do antivírus nos clientes (servidores e estações) em rede, com possibilidade de mudança para todos os computadores, ou somente um determinado grupo e por computador;
- Integração com tecnologia Wake-On-Lan e desligamento automático das estações de trabalho depois das verificações;
- Políticas especiais ativadas por eventos ocorridos na rede;
- O console envia alertas/e-mail ao administrador no caso de mudanças de configurações, desligamento do antivírus, falha na atualização de vacinas e incidência de vírus;
- O console da ferramenta deve exibir automaticamente logs e alertas de todos os clientes (servidores e estações) em rede, sem a necessidade de processos manuais;
- Permite a instalação do console de gerenciamento em qualquer computador da rede para administração remota do Servidor de Antivírus;
- Instalação em computadores infectados e tratamento de infecções durante a instalação;
- Gerenciamento e administração de estações e servidores de arquivos Linux pela console Gerenciamento;

- A atualização de vacinas e *engines* do servidor de Antivírus é de forma automática (agendada) ou manual, através da internet, utilizando também clientes móveis (notebooks) os protocolos HTTP e FTP, possibilitando a utilização de "proxy";
- A atualização das vacinas ocorre a cada 1 (uma) hora;
- Provê mecanismos de distribuição de vacinas e *engines* para todos os clientes (servidores e estações) na rede LAN e WAN, a partir do servidor de Antivírus, de forma agendada, *real-time* ou manual;
- As atualizações das vacinas e *engines* do Servidor para o Cliente são incrementais, de forma a racionalizar a utilização de banda de rede;
- Permite que em clientes móveis (notebooks) seja possível a configuração da atualização da vacina e engines também a partir da internet. Com isso garante-se que o cliente sempre estará atualizado;
- Permite, através de seu console único, que as atualizações (vacinas, engines, versão) possam ser propagadas para todos os computadores em rede LAN e WAN, somente para um determinado grupo e por computador;
- Provê relatórios a partir do seu console único, com dados sobre alertas de vírus, histórico de verificações (scan) e eventos do antivírus (event logs);

- Gera relatórios estatísticos e gráficos, contendo os seguintes tipos:
  - Máquinas que mais receberam ocorrência de vírus. Relatório de aplicações e produtos de outros fabricantes;
  - Os vírus que mais infectaram a rede;
  - Sumários das ações realizadas (limpos, removidos, quarentenas, etc.);
  - Quantitativo de máquinas atualizadas ou desatualizadas e quais estão com o antivírus desinstalado;
  - Relatório de erros;
  - Relatório de licenças em uso e quando irão expirar;
  - Capacidade de exportar os relatórios para o formato HTML no mínimo;
  - Capacidade de customização de relatórios;
- Fornecer suporte técnico pelo período mínimo de 36 (trinta e seis) meses, através de consultas por e-mail, via internet, suporte via telefone e via acesso remoto ilimitado durante a vigência das licenças.

Responsabilidades do Contratante:

- Acompanhar e fiscalizar a execução do CONTRATO, por meio da equipe de fiscalização, que fará registro de todas as ocorrências relacionadas com a execução, sob os aspectos quantitativos e qualitativos, comunicando as ocorrências de quaisquer fatos que exijam medidas corretivas por parte da CONTRATADA;
- Receber os produtos, objeto deste Termo de Referência, testá-los e, quando atenderem às especificações, aprová-los;

- Supervisionar o fornecimento e implantação do produto;
- Manter representante devidamente autorizado para acompanhar e fiscalizar a execução do objeto deste Termo de Referência;
- Emitir e encaminhar os Termos de Recebimento Provisório após comunicação formal de entrega emitido pela CONTRATADA, e conferência de conclusão de cada etapa prevista no presente projeto;
- Emitir e encaminhar o Termo de Recebimento Definitivo após conclusão de entrega pela CONTRATADA;
- Responsabilizar-se pela utilização dos produtos única e exclusivamente para uso próprio e colaboradores correlatos, não podendo sublicenciar, ceder ou transferir a licença, copiar e distribuir a terceiros, reverter a montagem ou a compilação dos programas ou, de qualquer forma, traduzi-los;
- Responsabilizar-se pelo cumprimento das regras estabelecidas para uso e guarda dos softwares licenciados;
- Promover a fiscalização e conferência dos fornecimentos executados pela CONTRATADA e atestar os documentos fiscais pertinentes, quando comprovada a execução total, fiel e correta dos fornecimentos, podendo rejeitar, no todo ou em parte, os objetos entregues fora das especificações deste Termo de Referência;
- Comunicar à CONTRATADA toda e qualquer ocorrência relacionada à aquisição ou entrega dos objetos;
- Proceder às advertências, multas e demais comunicações legais pelo descumprimento por parte da CONTRATADA das obrigações assumidas;
- Verificar a regularidade da situação fiscal da CONTRATADA e dos recolhimentos sociais trabalhistas sob sua responsabilidade antes de efetuar os pagamentos devidos;
- Prestar informações e esclarecimentos que venham a ser solicitados pela CONTRATADA;
- Notificar a empresa sobre a emissão da nota de empenho, acompanhar a entrega, verificar as condições dos softwares recebidos e certificar a nota fiscal.

4 – INDICAÇÃO DOS TERMOS CONTRATUAIS	
PROCEDIMENTOS E CRITÉRIOS DE ACEITAÇÃO	
Ação	
- Entregar os serviços de acordo com as especificações exigidas;	
ESTIMATIVA DE VOLUME DE SERVIÇOS OU BENS	
Serviço/Bem	Observação
- Aquisição de atualização de licenças de uso de software antivírus, para fins de proteção da rede lógica, equipamentos de TI e informações, por um período de atualização, suporte e assistência técnica	

de, no mínimo, 36 (trinta e seis) meses, aplicação das novas licenças e versões do software, configuração e suporte técnico remotos e on-site, todos necessários para manter atualizada a solução de segurança contra códigos maliciosos, minimizando, assim, os riscos de segurança da informação.	

METODOLOGIA DE AVALIAÇÃO DA QUALIDADE E DA ADEQUAÇÃO
O objeto será avaliado e testado ao ser recebido, pela equipe da Coordenadoria de Modernização e Tecnologia da Informação

INSPEÇÕES E DILIGÊNCIAS	
Tipo	Forma de execução
Não se aplica	

FORMA DE PAGAMENTO
Descrição: Após a realização de ateste da nota fiscal, concluídas as etapas de recebimento provisório e definitivo.

CRONOGRAMA FÍSICO-FINANCEIRO

	Entrega	Data	Percentual/valor
1	- O **Recebimento Provisório** do objeto, para efeito de posterior verificação da sua conformidade, será realizado pelo Fiscal do contrato, mediante termo circunstanciado assinado pelas partes, até o 5º (quinto) dia da apresentação da nota fiscal	- até o 5º (quinto) dia da apresentação da nota fiscal	
2	- O **Recebimento Definitivo** será realizado pelo Gestor do contrato, mediante termo circunstanciado assinado pelas partes, após o decurso do prazo para observação ou vistoria que comprove a adequação do objeto aos termos contratuais, não superior a 90 (noventa) dias;	- não superior a 90 (noventa) dias	

MECANISMOS FORMAIS DE COMUNICAÇÃO MPMA - CONTRATADA

Instrumentos	Hipóteses
Email	Garantia; envio de nota fiscal; notificações; solicitação de informações
Telefone	
Página Web - Chat	

GARANTIAS CONTRATUAIS
De fiscalização: Caberá à equipe de fiscalização da contratação, a saber: fiscal requisitante, fiscal técnico e fiscal administrativo, a fiscalização e a gestão do contrato.
De alterações contratuais: Não se aplica
De exigências técnicas: Não se aplica

DEFINIÇÃO DE MULTAS E SANÇÕES ADMINISTRATIVAS	
Ocorrência	Multa/Sanção
1.1 Pela inexecução total ou parcial do CONTRATO, a CONTRATANTE poderá, garantida a prévia defesa, aplicar à CONTRATADA as seguintes sanções: 1.2 Advertência; 1.3 Multa, na forma prevista no instrumento convocatório ou no CONTRATO; 1.4 Impedimento de licitar ou contratar com a Administração Pública, pelo prazo máximo de 3 (três) anos; 1.5 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 CONTRATANTE, que será concedida sempre que a CONTRATADA ressarcir a Administração pelos prejuízos resultantes, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.	1.1 Em caso de descumprimento de qualquer prazo estabelecido neste instrumento, o fornecedor ficará sujeito à multa diária de 0,5% (cinco décimos por cento) sobre o valor do quantitativo a ser entregue, por dia de atraso injustificado, até o período máximo de 30 (trinta) dias, a partir do qual será cobrada multa no montante de 20% (vinte por cento) sobre o valor do quantitativo a ser entregue, sem prejuízo das demais penalidades previstas na Lei nº 14.133/21.

5 – ORÇAMENTO
(Utilização da Mediana, conforme Art.23, Inciso 1º, Parágrafo I e considerando a pesquisa realizada no Painel de Preços)

Item	Objeto	Quantidade	Valor Unitário (R$)	Valor Total (R$)
1	Atualização de licença de software antivírus Kaspersky Endpoint Security for Business Select Brazilian Edition, por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses, e demais detalhamentos descritos	3000	R$143,00	R$429.000,00

	no termo de referência.			
2	Aquisição de licença de software antivírus Kaspersky Endpoint Security for Business Select Brazilian Edition, para fins de proteção da rede lógica, equipamentos de TI e informações, por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses, e demais detalhamentos descritos no termo de referência.	1000	R$143,00	R$143.000,00
			TOTAL	**R$ 572.000,00**

6 – ADEQUAÇÃO ORÇAMENTÁRIA		
FONTES DE RECURSOS		
	Valor	Fonte
1	**R$ 572.000,00**	
ESTIMATIVA DE IMPACTO ECONÔMICO-FINANCEIRO		

7 – FORMA DE CONTRATAÇÃO					
X	Licitação		Dispensa		Inexigibilidade

LICITAÇÃO			
Modalidade:		Tipo:	
JUSTIFICATIVAS PARA CONTRATAÇÃO DIRETA			
Requisitos de Qualificação Técnica			
1	Não se Aplica		
Requisitos de Capacitação e Experiência			
1	Não se Aplica		
Requisitos de Qualificação das Equipes Técnicas			
1	Não se Aplica		
Condições de mercado/outras			
1	Não se Aplica		

8 – CRITÉRIOS PARA JULGAMENTO			
TIPO: N/A - Não se Aplica			
Critério técnico / documento		Pontos	Pontuação máxima
1	N/A – Não se aplica		

ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA

Equipe de Planejamento da Contratação			
Gestor do Contrato	**Integrante Requisitante**	**Integrante Técnico**	**Integrante Administrativo**
NAYANA SANTOS MARTINS NEIVA SOBRAL:1071386 Assinado de forma digital por NAYANA SANTOS MARTINS NEIVA SOBRAL:1071386 Dados: 2023.06.16 14:42:19 -03'00'	DIEGO WALISSON PEREIRA CAMARA SANTOS:1070278 Assinado de forma digital por DIEGO WALISSON PEREIRA CAMARA SANTOS:1070278 Dados: 2023.06.12 11:53:48 -03'00'	LEONARDO DORNELES FIGUEIREDO SILVA:1071397 Assinado de forma digital por LEONARDO DORNELES FIGUEIREDO SILVA:1071397 Dados: 2023.06.12 12:02:35 -03'00'	DANIELA NASCIMENTO MONTELO:1071575 Assinado de forma digital por DANIELA NASCIMENTO MONTELO:1071575 Dados: 2023.06.12 11:46:17 -03'00'
Nayana Santos Martins Neiva Sobral	**Diego Walisson Pereira Camara Santos**	**Leonardo Dorneles Figueiredo Silva**	**Daniela Nascimento Montelo**
Matrícula: 1071386	**Matrícula: 1070278**	**Matrícula: 1071397**	**Matrícula: 1071575**