PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO MARANHÃO
DIRETORIA DE INFORMÁTICA E AUTOMAÇÃO
COORDENADORIA DE INFRAESTRUTURA E TELECOMUNICAÇÕES

Estudo Técnico Preliminar

OBJETO: Aquisição de Licenças de Software Antivírus

São Luís/MA

2022

Sumário

1. APRESENTAÇÃO

Este Estudo Técnico Preliminar (ETP) foi elaborado conforme o Documento de Oficialização da Demanda (DOD), constante no processo nº 26856/2022, em atendimento aos seguintes regramentos:

1. Resolução n. 182/2013, que regulamenta as diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação (STIC) realizadas pelos órgãos submetidos ao controle administrativo e financeiro do CNJ;

2. Resolução n. 44/2021, que dispõe sobre o Planejamento Estratégico do PJMA para o período de 2021-2026, em seu objetivo estratégico expresso no art. 3º, nos incisos X e XX;

3. Resolução GP n. 27/2022, que institui a Política de Governança de Contratações do TJMA, em conformidade com a Resolução CNJ n. 347/2020 - Política de Governança das contratações públicas no Poder Judiciário;

4. Resolução GP n. 37/2022, que institui o Plano de Logística Sustentável do PJMA para o período de 2021-2026, em conformidade com a Resolução CNJ n. 400/2021, que trata da Política de sustentabilidade do Poder Judiciário;

5. Resolução GP 59/2021, que Institui o Código de Ética Profissional, Conduta e Integridade dos Servidores do Poder Judiciário do Estado do Maranhão; e

6. Ato da Presidência n. 72/2022, que regulamenta a Política Estadual Começar de Novo no âmbito do TJMA, instituída no âmbito do Poder Judiciário por meio da Resolução CNJ n. 307/2019 - Política de Atenção às Pessoas Egressas do Sistema Prisional no mercado de trabalho, que garante a disponibilização de vagas nos contratos de serviços terceirizados com mão de obra em regime de exclusividade, bem como nas contratações de obras e serviços de Engenharia que necessitam da contratação de mão de obra.

2. ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO (ART.14)

Neste item, objetivamos demonstrar as viabilidades de negócio, técnicas e funcionais, pelos aspectos da eficácia, eficiência, economia e padronização na renovação de novas licenças de uso de software antivírus, com suporte técnico, por um prazo de 36 (trinta e seis) meses para todo o TJMA.

2.1 DEFINIÇÃO E ESPECIFICAÇÃO DOS REQUISITOS DA DEMANDA (ART.14, I)

É fundamental para o TJMA garantir que os processos de TI estejam alinhados com a estratégia e os objetivos do negócio, agregando valor para a organização, proporcionando segurança da informação para os usuários dos sistemas concentrados em seu ambiente.

Considerando a importância vital que os sistemas e serviços de TI adquiriram para as organizações e a constante diversificação e desenvolvimento de novas ameaças cibernéticas ao longo do tempo, torna-se mandatório o uso de uma solução de antivírus e a disponibilidade de apoio técnico especializado na ferramenta para atingir as metas de segurança da informação, garantir a continuidade dos serviços essenciais e que esteja totalmente alinhada ao ambiente e às melhores práticas de segurança de TI.

O uso de software antivírus corporativo padronizado em seus diversos equipamentos é uma das várias ações tomadas ao longo do tempo para implantar ferramentas que possam viabilizar os processos de segurança objetivando a repercussão positiva na promoção da cultura da segurança.

O Documento de Oficialização da Demanda (DOD) constante no Processo nº 26856/202 apresenta a necessidade de contratar uma empresa para fornecimento de novas licenças de uso de software antivírus, com suporte técnico, por um prazo de 36 (trinta e seis) meses, para substituir as atuais licenças Kaspersky Endpoint Security for Business SELECT em uso no TJMA, atendendo aos seguintes requisitos:

a) Licenças de uso consistindo no direito de atualização de softwares e de assinaturas de vírus, fornecendo atualizações tecnológicas de correções de erros e/ou de melhorias da solução, além das bases de conhecimento;
b) Suporte técnico especializado na Solução para registro e solução de quaisquer incidentes referentes ao seu uso e funcionamento, com atendimento remoto e com mecanismo adequado para abertura e acompanhamento de chamados de suporte técnico em horário comercial;
c) Serviço de verificação de pragas virtuais, promovendo a segurança na camada de usuário e servidores, visando mitigar riscos de incidentes de segurança;
d) Uma única plataforma integrada de segurança que compreenda as soluções de endpoints para estações de trabalhos e servidores físicos e virtuais, sendo que o suporte à solução e suas funcionalidades sejam fornecida por um único fabricante;
e) Controle centralizado dos endpoints, possibilitando o monitoramento deles, mantendo todos os dispositivos protegidos de maneira automática, bloqueando ações indesejadas e sempre reportando as ocorrências de quaisquer incidentes;
f) Contratação de solução centralizada de segurança do tipo endpoint protection, atendendo a quantidade atual (sete mil licenças) e a expansão prevista do parque tecnológico pelos próximos três anos (dez mil licenças), visando garantir a proteção dos ativos de TIC contra as várias ameaças virtuais e de malware;
g) Permita o controle de vulnerabilidades em aplicativos, a aplicação de paths de sistema operacional além de ter Integração com sistemas SIEM; e
h) Garanta a preservação do conhecimento existente no uso da solução atualmente em uso.

A análise comparativa de soluções de software antivírus visa elencar as possíveis alternativas capazes de atender as necessidades do TJMA, considerando a eficiência, a eficácia e a economia para o alcance dos objetivos da contratação. Este estudo considerou as seguintes possíveis alternativas:

1. Aquisição de novas licenças de outro fabricante de software de antivírus;
2. Renovação de novas licenças para a versão atual do software em uso; e
3. Renovação de novas licenças com upgrade para a versão ADVANCED do software em uso;

1. Instalar uma nova plataforma de antivírus de outro fabricante necessitaria de grandes esforços na sua execução, tendo em vista o tempo necessário para estudo e elaboração dos artefatos para contratação de uma nova solução, o tempo e gasto necessários para a equipe técnica dominar a nova solução, bem como o tempo e custo de adaptação e treinamento dos usuários na nova solução e por fim, o tempo e a complexidade de implantação da nova solução nos servidores e endpoints; além de não atender a todos os requisitos da demanda, o que inviabiliza essa opção;
2. Atualmente o TJMA possui licenças perpétuas do software antivírus Kaspersky Endpoint Security for Business SELECT adquiridas por meio do Processo nº 16418/2019 - TJMA. A renovação dessas licenças de antivírus não atendem integralmente aos requisitos listados no item 2.1;
3. A renovação das licenças do software antivírus com upgrade para a versão Kaspersky Endpoint Security for Business ADVANCED,que atende a todos os requisitos citados no item 2.1, possibilita a proteção adequada e atualizada do ambiente computacional, garantindo integridade, confiabilidade, segurança e continuidade das atividades da organização.

https://www.kaspersky.com.br/small-to-medium-business-security/endpoint-select

Produtos | Serviços | Downloads | Suporte | Centro de recursos

Comparação entre versões

Escolha a melhor opção para a sua empresa. Quer adicionar mais funções? Basta fazer o upgrade para o próximo nível.

	Select	Advanced SAIBA MAIS	Total SAIBA MAIS
Defesa para PC, Linux, Mac, Android e iOS	✓	✓	✓
Defesa para aplicativos e servidores de terminal		✓	✓
Defesa para gateways da Web e servidores de e-mail			✓
Defesa contra ameaças em dispositivos móveis	✓	✓	✓
Detecção de comportamento, mecanismo de remediação	✓	✓	✓
Avaliação de vulnerabilidade e prevenção contra Exploit	✓	✓	✓
Permissões variáveis de ambiente e HIPS	✓	✓	✓
AMSI, Microsoft Active Directory, Syslog, RMM, PSA, EMM integration	✓	✓	✓
Gerenciamento de criptografia		✓	✓
Integração do Kaspersky Sandbox e Kaspersky EDR Optimum	✓	✓	✓
Proteções de ameaças da Web e de e-mails e controles para servidores		✓	✓
Controle adaptativo de anomalias e gerenciamento de correções		✓	✓
Criptografia e gerenciamento de criptografia integrado no SO		✓	✓
Integração de SIEM avançada, instalação de software de terceiros e de SO		✓	✓
Filtragem de conteúdo de entrada e saída			✓
Proteção anti-spam no nível de gateway			✓
Segurança de tráfego e controles da Web a nível de gateway			✓

Figura 1 – Diferença entre as versões SELECT, ADVANCED e TOTAL.

Dentre as características da versão ADVANCED, que interessam para as atuais necessidades do TJMA, as quais não se encontram na versão SELECT estão: integração de SIEM avançada, instalação de softwares de terceiro e de SO e o controle adaptativo de anomalias e gerenciamento de correções.

Deve-se observar que a versão TOTAL do kaspersky também atende aos requisitos da demanda e ainda apresenta outras funcionalidades, mas essas funcionalidades exclusivas da versão TOTAL já são supridas por outras soluções já existentes do parque tecnológico do TJMA, o que justifica a sua exclusão como possível solução para este estudo técnico.

As soluções implantadas em outros órgãos ou entidades da Administração Pública, que realizaram contratações com objetos similares, quanto à solução proposta neste Estudo Técnico Preliminar, encontram-se em processos licitatórios evidenciados no **Anexo B**.

2.2 IDENTIFICAÇÃO DAS SOLUÇÕES (ART. 14, II)

Opção 1: Renovação das licenças Kaspersky Endpoint Security for Business SELECT

É a versão em uso atualmente com as funções de segurança dos endpoints. Renovar as licenças desta versão somente possibilita a manutenção das funcionalidades básicas já existentes e apresentadas na Figura 1 acima, não adicionando novas funcionalidades, tais como a instalação de sistema operacional e de softwares de terceiros, controle adaptativo de anomalias e gerenciamento de correções. Apesar de ser a de menor custo, não atende totalmente aos requisitos citados no item 2.1 deste documento.

Opção 2: Renovação das licenças do software antivírus com upgrade para a versão Kaspersky Endpoint Security for Business ADVANCED.

Esta versão tem todas as funcionalidades da versão SELECT e mais: gerenciamento de criptografia, proteção contra ameaças da Web e de e-mails, controles para servidores, controle adaptativo de anomalias, gerenciamento de criptografia e de criptografia integrado ao SO, Integração de SIEM avançada, atualização de path do sistema operacional e de softwares de terceiros e a verificação de vulnerabilidades de aplicativos. O que possibilita um melhor controle dos riscos sobre os hardwares, softwares

e dados, visando combater e prevenir riscos na operação e na utilização dos mesmos. A versão ADVANCED atende aos requisitos da demanda, dando maior segurança às operações no ambiente tecnológico do TJMA.

2.2.1 SOLUÇÕES DISPONÍVEIS EM OUTROS ÓRGÃOS (ART. 14, II, A)

Por força da natureza da demanda, não se vislumbra outras soluções disponíveis no mercado além das apresentadas no item 2.2 deste Estudo Técnico Preliminar.

2.2.2 PORTAL DO SOFTWARE PÚBLICO BRASILEIRO (ART. 14, II, B)

Até o presente momento, não foram identificados, dentre os softwares existentes no Portal do Software Público Brasileiro, soluções que possam atender plenamente as necessidades e expectativas almejadas nesta contratação.

2.2.3 SOLUÇÕES DISPONÍVEIS NO MERCADO DE TIC (ART. 14, II, C)

Dadas às características da demanda, não existem soluções de software livre ou software público capazes de satisfazer plenamente as necessidades e requisitos deste planejamento.

2.2.4 MODELO NACIONAL DE INTEROPERABILIDADE – MNI (ART. 14, II, D)

Não se aplica, pois se trata de uma solução que não possui o requisito para intercâmbio de informações de processos judiciais e assemelhados entre os diversos órgãos de administração de justiça, nem tampouco serve de base para implementação das funcionalidades pertinentes no âmbito do sistema processual, nos termos tratados pela Resolução Conjunta CNJ n. 3/2013.

2.2.5 INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA – ICP-BRASIL (ART. 14, II, E)

As alternativas de solução levantadas são capazes de fazer uso dos recursos tecnológicos disponíveis em certificados digitais, estando alinhadas à Infraestrutura de Chaves Públicas – ICP Brasil e em conformidade com a Medida Provisória n. 2.200-2/2014 e demais arcabouço de normativos aplicáveis à solução.

2.2.6 MODELO DE REQUISITOS MOREQ-JUS (ART. 14, II, F)

Por se tratar de uma solução que não possui o requisito de gestão de processos e documentos, nos termos da Resolução CNJ n. 91/2009, não se aplicam as recomendações quanto ao Modelo de Requisitos Moreq-Jus.

2.2.7 ANÁLISE DOS CUSTOS TOTAIS DA DEMANDA (ART. 14, III)

Para a estimativa dos custos totais para atender a demanda, não foi considerada a aquisição de novas licenças de outro fabricante de software de antivírus, pois já se mostrou tecnicamente inviável e por isso não se justifica precificá-la. Para as alternativas restantes foram utilizadas as informações de preços levantadas em contratações públicas constantes no painel de preços e em propostas encaminhadas ao TJMA constantes no **ANEXO B**.

Cabe observar que tais estimativas devem ser ponderadas, pois as licitações foram realizadas para atender as necessidades intrínsecas de cada órgão, as licitações e propostas foram realizadas em períodos diferentes e, os serviços contratados apresentam prazos de vigência diversos e diferenças nos serviços ofertados. Também não se localizou no painel de preços nenhuma contratação com o exato quantitativo das licenças existentes no TJMA, nem a projeção de necessidade futura do objeto.

De posse destas informações, partiu-se para a análise dos custos totais da demanda sob o enfoque das necessidades do TJMA. As tabelas abaixo apresentam os valores identificados.

Item	Descrição	Órgão	Qtd	Valor unitário (R$)	Valor total (R$)
1	Renovação do licenciamento de direitos de uso do software Kaspersky Endpoint Security – ADVANCED, com Kaspersky Endpoint Detection and Response Standard, pelo período de 2 (dois) anos.	TJMG	10.875	199,29	2.167.278,75
2	Fornecimento software (licenças) de proteção antivírus Kaspersky EndPoint Security for Business ADVANCED, incluindo transferência de conhecimento, com garantia de atualizações e suporte técnico pelo período de 36 (trinta e seis) meses.	Governo Estado Roraima	5.841	160,00	934.560,00
3	Licença do software antivírus Kaspersky Endpoint Security for Business SELECT pelo período de doze meses.	Câmara dos Deputados	9.025	30,00	270.750,00

Tabela 1 – Valores de soluções Antivírus Kaspersky no Banco de Preços.

Item	Descrição	Qtd	Valor unitário (R$)	Valor total (R$)
1	Kaspersky Endpoint Security for Business - ADVANCED – 1 ano	7.000	114,26	799.820,00
2	Kaspersky Endpoint Security for Business - ADVANCED – 1 ano	10.000	108,81	1.088.100,00
3	Kaspersky Endpoint Security for Business – ADVANCED – Base Plus – 1 ano	10.000	109,81	1.098.100,00

Tabela 2 – Valores de Antivírus Kaspersky – Propostas TJMA – período de 1 ano.

Item	Descrição	Qtd	Valor unitário (R$)	Valor total (R$)
1	Kaspersky Endpoint Security for Business - ADVANCED – 3 anos	7.000	228,51	1.599.570,00
2	Kaspersky Endpoint Security for Business – ADVANCED – 3 anos	7.000	198,00	1.386.000,00

Item	Descrição	Qtd	Valor unitário (R$)	Valor total (R$)
3	Solução de antivírus Kaspersky Endpoint Security For Business ADVANCED, prazo de licenciamento 36 meses, com serviços de instalação e suporte técnico, pelo período 03 anos	7.000	238,51	1.668.170,00
4	Kaspersky Endpoint Security for Business - ADVANCED – 3 anos	10.000	217,63	2.176.300,00
5	Kaspersky Endpoint Security for Business – ADVANCED – 3 anos	10.000	162,00	1.620.000,00
6	Kaspersky Endpoint Security for Business – ADVANCED – Base Plus – 3 anos	10.000	227,63	2.276.300,00
7	Solução de antivírus Kaspersky Endpoint Security For Business ADVANCED, prazo de licenciamento 36 meses, com serviços de instalação e suporte técnico, pelo período 03 anos	10.000	219,63	2.196.300,00

Tabela 3 – Valores de Antivírus Kaspersky – Propostas TJMA – período de 3 anos.

Após análise das três tabelas pode-se destacar o seguinte:

A versão SELECT tem um custo unitário menor que a versão ADVANCED, mas devemos lembrar que a versão SELECT é menos provida de recursos que a versão ADVANCED e não atende a demanda deste estudo;

O quantitativo de licenças adquiridas afeta o custo unitário, sendo que quanto mais licenças, menor o custo individual da licença, o que é um fator a justificar a aquisição de um número maior de licenças;

O período de validade das licenças também influi no custo unitário, sendo que quanto maior o tempo, menor o valor unitário por ano de validade, sendo também um fator importante na escolha da melhor solução.

2.3 ESCOLHA E JUSTIFICATIVA DA SOLUÇÃO (ART. 14, IV)

A Diretoria de Informática e Automação tem a competência exclusiva de promover a aplicação e fiscalização da Política de Gestão de Ativos de Tecnologia da Informação do Poder Judiciário do Maranhão conforme Resolução GP 05/2017. Conforme

redação dada pela própria Resolução, art. 2º, Inc. I - entende-se por ativo de tecnologia da informação todo e qualquer componente de hardware, software e rede de dados e telefonia em uso no Poder Judiciário do Maranhão.

O TJMA conta hoje com sete mil licenças do software antivírus Kaspersky Endpoint Security for Business SELECT instaladas nos Servidores e nas estações de trabalho em todas as suas unidades no Estado, atuando na defesa contra vírus e outras ameaças que surgem constantemente no mundo da informática, proporcionando o bom funcionamento dos equipamentos e proteção dos dados neles existentes.

Considerando a relação custo x benefício avaliada no item 2.2.7, a quantidade de funcionalidades existentes em cada solução (Figura 1) e os requisitos da demanda no item 2.1, a equipe optou pela opção 2 do item 2.2 - Renovação das licenças do software antivírus com upgrade para a versão Kaspersky Endpoint Security for Business ADVANCED. O período de validade das licenças será de 36 (trinta e seis) meses e para um quantitativo total de dez mil licenças, por ser mais vantajoso tecnicamente e financeiramente considerando a necessidade atual e a perspectiva de expansão do parque computacional, principalmente de dispositivos móveis, para esse período.

2.3.1 DESCRIÇÃO DA SOLUÇÃO (ART. 14, IV, A)

Contratação de empresa especializada para a renovação das licenças de uso de software antivírus com upgrade do Kaspersky Endpoint Security for Business ADVANCED, incluindo suporte técnico remoto em horário comercial, por um período de 36 (trinta e seis) meses nos termos dos requisitos listados no item 2.1 deste Estudo Técnico Preliminar.

2.3.2 ALINHAMENTO DA SOLUÇÃO (ART. 14, IV, B)

A presente contratação está em consonância com a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário - ENTIC-JUD (Resolução CNJ n° 370/2021 - alterada pela Resolução CNJ n° 396/2021):

· Art. 2°, I, c: Processos Internos: Objetivo 6 – Aprimorar as Aquisições e Contratações; e

· Art. 2°, I, c: Processos Internos: Objetivo 7 – Aprimorar a Segurança da Informação e a Gestão de Dados.

Além disso, com base nas diretrizes definidas na Estratégia Nacional do Poder Judiciário, vários investimentos em Tecnologia da Informação e Comunicação (TIC) estão sendo priorizados para modernizar a infraestrutura de TIC com a finalidade de alcançar os objetivos estratégicos estabelecidos, tais como: consolidar a Tecnologia da Informação e Comunicação do TJMA como instrumento viabilizador de execução de estratégias, aperfeiçoar a Gestão da Segurança da Informação e das Comunicações, impulsionar a implantação e o aperfeiçoamento contínuo dos sistemas judiciais e prover infraestrutura tecnológica apropriada às atividades judiciais e administrativas.

A contratação pretendida também encontra consonância com Política de Segurança da Informação (PSI) do TJMA (Resolução n. 13/217) que define as diretrizes gerais para Segurança da Informação no âmbito do Poder Judiciário do Estado do Maranhão.

Da mesma forma, com o objetivo de aprimorar o nível de maturidade em segurança cibernética, foram observados os ditames da Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ6), no tocante aos objetivos ali traçados, para tornar o Judiciário mais seguro e inclusivo no ambiente digital; aumentar a resiliência às ameaças cibernéticas; estabelecer governança de segurança cibernética e fortalecer a gestão e coordenação integrada de ações de segurança cibernética nos órgãos do Poder Judiciário; e permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível, visando minimizar danos e agilizar o pronto restabelecimento da condição de normalidade em caso de ocorrência de ataques cibernéticos.

2.3.3 BENEFÍCIOS ESPERADOS (ART. 14, IV, C)

a) Eliminação de gastos com manutenção de hardwares e softwares devido a danos causados por malwares e outros ataques virtuais;
b) Servidores e estações atendidos e protegidos;
c) Permanente atualização tecnológica;
d) Elevação e melhoria nos níveis de segurança nos ativos protegidos; e
e) Uso de software com tecnologia moderna e atualizada.

2.3.4 RELAÇÃO ENTRE A DEMANDA PREVISTA E A CONTRATADA (ART.14, IV, D)

A demanda contratada deverá fornecer a quantidade de licenças de uso de softwares e suas funcionalidades suficientes para atender aos requisitos determinados neste Estudo Técnico Preliminar. Além disso, o serviço suporte técnico do software a ser fornecido deverá ser prestado por demanda por um período de 36 (trinta e seis) meses, cobrindo todo o prazo de validade das licenças;

2.3.5 NECESSIDADE DE ADEQUAÇÃO DO AMBIENTE PARA A EXECUÇÃO CONTRATUAL (ART. 14, V, A, B, C, D, E, F)

Para a execução contratual desta demanda não há, a cargo do TJMA, qualquer necessidade de adequação do seu ambiente físico ou lógico. Sobre o aspecto de avaliação do ambiente do TJMA, convém ressaltar:

a) infraestrutura tecnológica: O TJMA dispõe de infraestrutura tecnológica para suportar o objeto a ser contratado, tais como: hardware (microcomputadores e servidores) e recursos de comunicação (acesso à internet);

b) infraestrutura elétrica: A infraestrutura elétrica do ambiente do TJMA é capaz de suportar o objeto a ser contratado;

c) logística de implantação: Será provido pelo TJMA o acesso lógico e os respectivos privilégios necessários e adequados à perfeita execução do objeto a ser

contratado, exclusivamente para os profissionais diretamente envolvidos em sua execução;

d) espaço físico: Não se aplica ao objeto a ser contratado;

e) mobiliário: Não se aplica ao objeto a ser contratado;

f) impacto ambiental: Os ambientes físico e tecnológico do TJMA estão aderentes a Resolução GP n. 37/2022, que institui o Plano de Logística Sustentável do PJMA para o período de 2021-2026, em conformidade com a Resolução CNJ n. 400/2021, que trata da Política de sustentabilidade do Poder Judiciário. Atendendo no que couber aos critérios de sustentabilidade ambiental contidos no Decreto n. 7746/2012 que regulamenta o art. 3º da Lei n. 8.666/93, que estabelece critérios e práticas para a promoção do desenvolvimento nacional sustentável nas contratações realizadas pela administração pública. Portanto, deverá ser privilegiada a otimização dos recursos materiais, o uso de inovações que reduzam a pressão sobre recursos naturais e a adoção de medidas para racionalização no consumo de energia.

Por se tratar de serviço de atualização de software (intangível), bem como serviço de suporte remoto não foram encontrados danos ambientais possíveis na contratação.

2.3.6 ORÇAMENTO ESTIMADO (ART. 14, II, G)

Como já apresentado anteriormente, o prazo de validade e a quantidade de licenças influencia no preço unitário, sendo que não foi identificada uma proporcionalidade em relação ao número de licenças ou ao prazo de validade, tipo o valor de um ano é proporcional ao valor de três anos de licenças, ou o valor unitário para adquirir sete mil é proporcional ao de dez mil, sendo por isso consideradas somente as propostas referentes ao prazo de três anos para dez mil licenças.

Com base na análise de custos totais da demanda, constante do item 2.2.7, chegou-se à estimativa de orçamento total:

Item	Descrição	Qtd	Valor unitário (R$)	Valor total (R$)
1	Kaspersky Endpoint Security for Business - ADVANCED – 3 anos	10.000	217,63	2.176.300,00
2	Kaspersky Endpoint Security for Business – ADVANCED – 3 anos	10.000	162,00	1.620.000,00
3	Kaspersky Endpoint Security for Business – ADVANCED – Base Plus – 3 anos	10.000	227,63	2.276.300,00
4	Solução de antivírus Kaspersky Endpoint Security For Business ADVANCED, prazo de licenciamento 36 meses, com serviços de instalação e suporte técnico, pelo período 03 anos	10.000	219,63	2.196.300,00
	VALOR TOTAL MÉDIO ESTIMADO	**10.000**	**206,72**	**2.067.200,00**

Tabela 4 – Valores de Antivírus Kaspersky – Estimativa de custo - período de 3 anos.

Considerando a média simples das 4 propostas baseadas no valor unitário acima tem-se o valor de R$2.067.200,00 (Dois milhões, sessenta e sete mil, duzentos reais).

3. SUSTENTAÇÃO DO CONTRATO (ART.15)

O plano de sustentação tem por finalidade garantir a continuidade da operação da Solução de TIC após o término do contrato, de forma prevista ou imprevista.

Como o fornecimento do objeto não caracteriza prestação de serviços continuados, não cabe elaborar plano de sustentação.

3.1 RECURSOS MATERIAIS E HUMANOS (ART.15, I)

Em relação aos recursos materiais, serão os já usados comumente pelos profissionais da TI, como servidor, microcomputador, acesso à rede corporativa do TJMA para acesso às consoles administrativas, bem como acesso à Internet. Todos esses materiais e recursos já estão disponíveis no ambiente atual do TJMA.

Quanto aos recursos humanos, o objeto a ser contratado não impõe necessidades especiais de pessoal, além dos já disponíveis no TJMA.

Para uso da solução a ser contratada, sob o enfoque do TJMA, além do acompanhamento da conformidade legal pelo Gestor do Contrato por um servidor efetivo da Diretoria de Informática e Automação, conforme a Resolução GP n. 21/2018, art 4º, será necessário o acompanhamento técnico pelos fiscais (um titular e um substituto), realizado por servidores efetivos da Coordenação de Infraestrutura e Telecomunicação, conforme a Resolução GP n. 21/2018, art 5º e 6º.

A empresa a ser contratada deverá dispor de profissionais qualificados e detentores de conhecimento técnico e experiência suficientes para o pleno atendimento da solução conforme este Estudo Técnico Preliminar.

3.2 ESTRATÉGIA DE CONTINUIDADE (ART.15, II)

No caso de eventual interrupção contratual, antes da entrega completa do objeto a ser contratado, a solução será a rescisão por inadimplência das obrigações, com aplicação das penalidades cabíveis. Nessa situação, será realizada uma nova contratação com fornecedor classificado em posição subsequente no certame ou, ainda, a realização de novo processo de contratação.

3.3 TRANSIÇÃO E ENCERRAMENTO CONTRATUAL (ART.15, III, A,B,C,D,E)

O processo de transição do contrato se dá quando a empresa a ser contratada entrega as novas licenças com o novo prazo de validade, que começará a contar após o término da validade das licenças atuais.

Para a transição final desta contratação, será importante que a nova contratação seja motivada com antecedência razoável, em relação ao término do contrato em vigor.

3.4 ESTRATÉGIA DE INDEPENDÊNCIA DO ÓRGÃO COM RELAÇÃO À CONTRATADA (ART.15, IV,A,B)

Os direitos autorais e os direitos de propriedade intelectual da Solução de Tecnologia da Informação sobre os diversos artefatos e produtos produzidos ao longo do

contrato, incluindo a documentação e as bases de dados pertencerão ao TJMA, devendo ser justificado os casos em que isso não ocorra. Portanto, a empresa contratada cederá os direitos de propriedade intelectual e direitos autorais da Solução de Tecnologia da Informação sobre os diversos artefatos e produtos produzidos ao longo do contrato, incluindo a documentação e as bases de dados do TJMA. Ressalte-se que os direitos autorais dos fabricantes dos softwares utilizados na solução são resguardados e garantidos por legislação nacional e internacional.

4. ESTRATÉGIA PARA A CONTRATAÇÃO (ART.16)

4.1 NATUREZA DO OBJETO (ART.16, I)

Como apontado no de Descrição da Solução, o arcabouço de atividades que integram o objeto da solução possuem características comuns e usuais encontradas atualmente no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos no Termo de Referência. Portanto, se enquadram como BENS COMUNS ou usuais de mercado. Conforme prevê o Parágrafo único do artigo 1º da Lei 10.520/2002:

“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”.

Hoje a Kaspersky oferece licenciamento desses produtos na modalidade de licença perpétua, onde o cliente compra a licença e junto com a aquisição adquire também o direito a suporte técnico da própria Kaspersky e manutenção das licenças (ex.: fazer o upgrade gratuito caso seja lançada uma nova versão do produto comprado). Este direito ao suporte e manutenção, também conhecido como "Termo" pode ser de 1, 2 ou 3 anos. Finalizado este prazo, o cliente deverá fazer a renovação deste "Termo", ou seja, pagará um valor menor do que a aquisição e continuará se beneficiando do acesso a suporte e manutenção das licenças.

Características Técnicas mínimas a serem atendidas:

1. Servidor de Administração e Console Administrativa

1.1. Compatibilidade:

1.1.1. Microsoft Windows Server 2012/R2 (Todas as edições);

1.1.2. Microsoft Windows Small Business Server 2008 (Todas as edições);

1.1.3. Microsoft Windows Small Business Server 2011 (Todas as edições);

1.1.4. Microsoft Windows Server 2016 x64;

1.1.5. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x86/x64;

1.1.6. Microsoft Windows 8 SP1 Professional / Enterprise x86/x64;

1.1.7. Microsoft Windows 8/8.1 Professional / Enterprise X86/x64;

1.1.8. Microsoft Windows 10 (Todas as edições);

1.1.9. Microsoft Windows 11;

1.2. Suporta as seguintes plataformas virtuais:

1.2.1. Vmware: Workstation 12.x Pro, vSphere 5.5, vSphere 6, vSphere 7;

1.2.2. Microsoft Hyper-V: 2008, 2008 R2, 2008 R2 SP1, 2012, 2012 R2;

1.2.3. Microsoft Virtual PC 6.0.156.0;

1.2.4. KVM integrado com: RHEL 5.4.;

1.2.5. Oracle VM VirtualBox 4.0.4-70112;

1.2.6. Citrix XenServer 6.2 e 6.5;

1.3. Características:

1.3.1. Console deve ser acessada via WEB (HTTPS) ou MMC;

1.3.2. Console deve ser baseada no modelo cliente/servidor;

1.3.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;

1.3.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;

1.3.5. Deve permitir incluir usuários do AD para logarem na console de administração;

1.3.6. Console deve ser totalmente integrada com as suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;

1.3.7. 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;

1.3.8. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;

1.3.9. 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;

1.3.10. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

1.3.11. Deve armazenar histórico das alterações feitas em políticas;

1.3.12. 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;

1.3.13. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;

1.3.14. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

1.3.15. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;

1.3.16. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS e Android;

1.3.17. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

1.3.18. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os parâmetros KB/s e horário;

1.3.19. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução;

1.3.20. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;

1.3.21. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;

1.3.22. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto;

1.3.23. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

1.3.24. 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;

1.3.25. A comunicação entre o cliente e o servidor de administração deve ser criptografada;

1.3.26. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

1.3.27. Capacidade de aplicar atualizações do Windows remotamente nas estações e servidores;

1.3.28. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

1.3.29. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;

1.3.30. Capacidade de monitorar diferentes subredes a fim de encontrar máquinas novas para serem adicionadas à proteção;

1.3.31. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas à proteção;

1.3.32. Capacidade de, assim que detectar máquinas novas no Active Directory, subredes ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

1.3.33. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos dois dias, etc.;

1.3.34. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

1.3.35. Deve fornecer as seguintes informações dos computadores: Se o antivírus está instalado; Se o antivírus está iniciado; Se o antivírus está atualizado; Minutos/horas desde a última conexão da máquina com o servidor administrativo; Minutos/horas desde a última atualização de vacinas; Data e horário da última verificação executada na máquina; Se é necessário reiniciar o computador para aplicar mudanças; Data e horário de quando a máquina foi ligada; Quantidade de vírus encontrados (contador) na máquina; Nome do computador; Domínio ou grupo de trabalho do computador; Data e horário da última atualização de vacinas; Sistema operacional com Service Pack; Quantidade de processadores; Quantidade de memória RAM; Usuário(s) logado(s) naquele momento, com informações de contato (caso disponível no Active Directory); Endereço IP; Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido; Atualizações do Windows Updates instaladas; Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD; Vulnerabilidades de aplicativos instalados na máquina;

1.3.36. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

1.3.37. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como: Alteração de Gateway Padrão; Alteração de subrede; Alteração de domínio; Alteração de servidor DHCP; Alteração de servidor DNS; Resolução de Nome; Disponibilidade de endereço de conexão SSL;

1.3.38. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

1.3.39. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

1.3.40. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;

1.3.41. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

1.3.42. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

1.3.43. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;

1.3.44. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;

1.3.45. Capacidade de gerar traps SNMP para monitoramento de eventos;

1.3.46. Capacidade de enviar e-mails para contas específicas em caso de algum evento;

1.3.47. Listar em um único local, todos os computadores não gerenciados na rede;

1.3.48. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;

1.3.49. Deve possuir compatibilidade com Cisco Network Admission Control (NAC);

1.3.50. Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).

1.3.51. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente;

1.3.52. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc.), inclusive de máquinas que estejam em subredes diferentes do servidor;

1.3.53. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

1.3.54. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo porém sem comprometer o desempenho do computador;

1.3.55. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex.: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);

1.3.56. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação;

1.3.57. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;

1.3.58. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

1.3.59. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo: Nome do vírus; Nome do arquivo infectado; Data e hora da detecção; Nome da máquina ou endereço IP; Ação realizada;

1.3.60. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

1.3.61. Capacidade de listar updates nas máquinas com o respectivo link para download

1.3.62. Deve criar um backup de todos os arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;

1.3.63. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;

1.3.64. Capacidade de realizar inventário de hardware de todas as máquinas clientes;

1.3.65. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;

1.3.66. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

2. Estações Windows

2.1. Compatibilidade:

2.1.1. Microsoft Windows 7 SP1 Professional/Enterprise/Ultimate x86/x64;

2.1.2. Microsoft Windows 8 Professional/Enterprise x86 /x64;

2.1.3. Microsoft Windows 8.1 Pro / Enterprise x86 /x64;

2.1.4. Microsoft Windows 10 Pro / Enterprise x86 /x64;

2.1.5. Microsoft Windows Server 2012 R2 Standard x64;

2.1.6. Microsoft Windows Server 2012 Foundation x64;

2.1.7. Microsoft Windows Server 2012 Standard x64;

2.1.8. Microsoft Small Business Server 2011 Standard x64;

2.1.9. Microsoft Windows Server 2016 x64.

2.2. Características:

2.2.1. Deve prover as seguintes proteções:

2.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;

2.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);

2.2.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);

2.2.1.4. Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc.);

2.2.1.5. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;

2.2.1.6. Firewall com IDS;

2.2.1.7. Autoproteção (contra-ataques aos serviços/processos do antivírus);

2.2.1.8. Controle de dispositivos externos;

2.2.1.9. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;

2.2.1.10. Controle de acesso a sites por horário;

2.2.1.11. Controle de acesso a sites por usuários;

2.2.1.12. Controle de acesso a websites por dados, ex.: Bloquear websites com conteúdos de vídeo e áudio;

2.2.1.13. Controle de execução de aplicativos;

2.2.1.14. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

2.2.2. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

2.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, **no máximo, uma em uma hora** independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

2.2.4. Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o Firewall da solução;

2.2.5. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

2.2.6. 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;

2.2.7. 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;

2.2.8. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

2.2.9. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

2.2.10. 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;

2.2.11. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;

2.2.12. Capacidade de verificar somente arquivos novos e alterados;

2.2.13. Capacidade de verificar objetos usando heurística utilizando no mínimo as seguintes opções de nível: Alta, Média, Baixa;

2.2.14. Capacidade de agendar uma pausa na verificação;

2.2.15. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;

2.2.16. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

2.2.17. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);

2.2.18. Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;

2.2.19. Capacidade de verificar links inseridos em e-mails contra phishings;

2.2.20. Capacidade de verificar tráfego SSL nos browsers: Internet Explorer, Firefox, Google Chrome e Opera;

2.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística;

2.2.22. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;

2.2.23. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;

2.2.24. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;

2.2.25. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas;

2.2.26. Deve ter suporte total ao protocolo Ipv6;

2.2.27. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;

2.2.28. Na verificação de tráfego web, caso encontrado código malicioso o programa deve: Perguntar o que fazer, ou Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou Permitir acesso ao objeto;

2.2.29. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador: Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo-real, ou Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação;

2.2.30. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;

2.2.31. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

2.2.32. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;

2.2.33. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;

2.2.34. Deve possuir módulo de bloqueio de *Phishing*, com atualizações incluídas nas vacinas, obtidas pelo *Anti-Phishing Working Group* (http://www.antiphishing.org/);

2.2.35. Capacidade de distinguir diferentes subredes e conceder opção de ativar ou não o firewall para uma subrede específica;

2.2.36. Deve possuir módulo IDS (*Intrusion Detection System*) para proteção contra *port scans* e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;

2.2.37. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras: Filtragem de pacotes onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; Filtragem por aplicativo onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados;

2.2.38. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo: Discos de armazenamento locais; Armazenamento removível; Impressoras; CD/DVD; Modems; Dispositivos de fita; Dispositivos multifuncionais; Leitores de smart card; Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc); Wi-Fi; Adaptadores de rede externos; Dispositivos MP3 ou smartphones; Dispositivos Bluetooth; Câmeras e Scanners.

2.2.39. Capacidade de liberar acesso a um dispositivo específico e usuários específico por um período de tempo específico, sem a necessidade de desabilitar a proteção, sem desabilitar o gerenciamento central ou de intervenção local do administrador na máquina do usuário;

2.2.40. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;

2.2.41. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;

2.2.42. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.

2.2.43. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

2.2.44. Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc), com possibilidade de configuração por usuário ou grupos de usuários e agendamento.

2.2.45. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);

2.2.46. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação: Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.2.47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

2.2.48. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;

2.2.49. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;

2.2.50. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

2.2.51. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

2.2.52. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

2.2.53. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

2.2.54. Capacidade de integração com o Windows Defender Security Center.

2.2.55. Capacidade de integração com a Antimalware Scan Interface (AMSI).

2.2.56. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).

2.2.57. Deve possuir módulo que monitora e bloqueia atividades potencialmente maliciosas, baseado no comportamento do usuário e Machine Learning.

3. Estações Mac OS X

3.1. Compatibilidade:

3.1.1. MasOS High Sierra 10.13

3.1.2. MacOS Sierra 10.12

3.1.3. Mac OS X 10.11 (El Capitan);

3.1.4. Mac OS X 10.10 (Yosemite);

3.1.5. Mac OS X 10.9 (Mavericks);

3.2. Características:

3.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

3.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https;

3.2.3. Possuir módulo de bloqueio á ataques na rede;

3.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;

3.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio a ataques na rede;

3.2.6. Possibilidade de importar uma chave no pacote de instalação;

3.2.7. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

3.2.8. Deve possuir suportes a notificações utilizando o Growl;

3.2.9. As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

3.2.10. Capacidade de voltar para a base de dados de vacina anterior;

3.2.11. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;

3.2.12. 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;

3.2.13. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

3.2.14. 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;

3.2.15. Capacidade de verificar somente arquivos novos e alterados;

3.2.16. Capacidade de verificar objetos usando heurística;

3.2.17. Capacidade de agendar uma pausa na verificação;

3.2.18. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve: Perguntar o que fazer ou Bloquear acesso ao objeto ou Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

3.2.18.1. Caso positivo de desinfecção restaurar o objeto para uso;

3.2.18.2. Caso negativo de desinfecção Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

3.2.19. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

3.2.20. Capacidade de verificar arquivos de formato de e-mail;

3.2.21. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;

3.2.22. Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

4. Estações de trabalho Linux 32-64 bits

4.1. Compatibilidade:

4.1.1. Ubuntu 14.04.5 LTS

4.1.2. Ubuntu 16.04.4 LTS

4.1.3. Ubuntu 17.10.1

4.1.4. Red Hat® Enterprise Linux® 6.9

4.1.5. CentOS-6.9

4.1.6. Debian GNU/Linux 8.10

4.1.7. Debian GNU/Linux 9.4

4.1.8. AltLinux 8.0.0

4.1.9. AltLinux 8.2*

4.1.10. GosLinux 6.6

4.1.11. Ubuntu 18.04

4.1.12. Red Hat® Enterprise Linux® 7.4

4.1.13. CentOS-7.4

4.1.14. OracleLinux 7.4

4.1.15. SUSE® Linux Enterprise Server 12 SP3

4.1.16. OpenSUSE® 42.3

4.1.17. AltLinux 8.0.0

4.2. Características:

4.2.1. Deve prover as seguintes proteções:

4.2.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

4.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, **no máximo, uma em uma hora** independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

4.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus;

4.2.5. Capacidade de criar exclusões por local, máscara e nome da ameaça;

4.2.6. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

4.2.7. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

4.2.8. Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers;

4.2.9. Capacidade de verificar objetos usando heurística utilizando no mínimo as seguintes opções de nível: Alta, Média, Baixa;

4.2.10. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

4.2.11. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

4.2.12. Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;

4.2.13. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

4.2.14. 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;

4.2.15. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

4.2.16. Administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

5. Servidores Windows 32 ou 64 bits

5.1. Compatibilidade:

5.1.1. Windows Server 2008 Standard/Enterprise/Datacenter SP1 e posterior;

5.1.2. Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 e posterior;

5.1.3. Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior);

5.1.4. Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior);

5.1.5. Microsoft Windows Storage Server 2008 R2;

5.1.6. Microsoft Windows Storage Server 2008 SP2 Standard Edition;

5.1.7. Microsoft Windows Storage Server SP2 Workgroup Edition;

5.1.8. Microsoft Windows Hyper-V Server 2008 R2 SP1 e posterior;

5.1.9. Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;

5.1.10. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;

5.1.11. Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;

5.1.12. Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;

5.1.13. Microsoft Windows Storage Server 2012 (Todas edições);

5.1.14. Microsoft Windows Storage Server 2012 R2 (Todas edições);

5.1.15. Microsoft Windows Hyper-V Server 2012;

5.1.16. Microsoft Windows Hyper-V Server 2012 R2;

5.1.17. Windows Server 2016 Essentials/Standard/Datacenter/MultiPoint Premium Server;

5.1.18. Windows Server 2016 Core Standard / Datacenter;

5.1.19. Windows Storage Server 2016;

5.1.20. Windows Hyper-V Server 2016.

5.2. Características:

5.2.1. Deve prover as seguintes proteções:

5.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;

5.2.1.2. Auto-proteção contra-ataques aos serviços/processos do antivírus;

5.2.1.3. Firewall com IDS;

5.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

5.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

5.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, **no máximo, uma em uma hora** independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

5.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções: Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas); Gerenciamento de tarefa (criar ou excluir tarefas de verificação); Leitura de configurações; Modificação de configurações; Gerenciamento de Backup e Quarentena; Visualização de relatórios; Gerenciamento de relatórios; Gerenciamento de chaves de licença; Gerenciamento de permissões (adicionar/excluir permissões acima);

5.2.5. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras: Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

5.2.6. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;

5.2.7. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede

5.2.8. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);

5.2.9. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja rodando com fonte ininterrupta de energia (*uninterruptible Power supply – UPS*);

5.2.10. Em caso de erros, deve ter capacidade de criar *logs* e *traces* automaticamente, sem necessidade de outros softwares;

5.2.11. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;

5.2.12. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

5.2.13. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;

5.2.14. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

5.2.15. 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;

5.2.16. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

5.2.17. 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;

5.2.18. Capacidade de verificar somente arquivos novos e alterados;

5.2.19. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);

5.2.20. Capacidade de verificar objetos usando heurística;

5.2.21. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

5.2.22. Capacidade de agendar uma pausa na verificação;

5.2.23. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

5.2.24. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve: Perguntar o que fazer ou Bloquear acesso ao objeto; Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

5.2.24.1. Caso positivo de desinfecção restaurar o objeto para uso;

5.2.24.2. Caso negativo de desinfecção mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

5.2.25. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

5.2.26. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

5.2.27. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

5.2.28. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa;

5.2.29. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros

5.2.30. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning);

5.2.31. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

6. Servidores Linux 32 ou 64 bits

6.1. Compatibilidade:

6.1.1. Red Hat® Enterprise Linux® 6.9 Server

6.1.2. CentOS-6.9

6.1.3. Ubuntu 14.04.5 LTS

6.1.4. Ubuntu 16.04.2 LTS

6.1.5. Ubuntu 17.10.1

6.1.6. Debian GNU / Linux 8.10

6.1.7. Debian GNU / Linux 9.4

6.1.8. AltLinux 8.0.0

6.1.9. AltLinux 8.2

6.1.10. Red Hat® Enterprise Linux® 7.4 Server

6.1.11. Red Hat® Enterprise Linux® 7.5 Server

6.1.12. CentOS-7.4

6.1.13. CentOS-7.5

6.1.14. Ubuntu 18.04

6.1.15. SUSE® Linux Enterprise Server 12 SP3

6.1.16. Oracle Linux 7.4

6.1.17. SUSE® Linux Enterprise Server 12 SP2

6.1.18. OpenSUSE® 42.3

6.1.19. EMIAS 1.0

6.1.20. Amazon Linux AMI

6.2. Características:

6.2.1. Deve prover as proteções de Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

6.2.2. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

6.2.2.1. Gerenciamento de status de tarefa (iniciar, pausar, parar tarefas);

6.2.2.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

6.2.2.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

6.2.2.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;

6.2.3. Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;

6.2.4. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

6.2.5. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção;

6.2.6. Capacidade de verificar objetos usando heurística;

6.2.7. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

6.2.8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

6.2.9. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

7. Smartphones e tablets

7.1. Compatibilidade:

7.1.1. Dispositivos com os sistemas operacionais:

7.1.1.1. Android 5.0 – 5.1.1 ou superior

7.1.1.2. iOS 9.0 – 9.3.5 ou superior

7.2. Características:

7.2.1. Deve prover as seguintes proteções:

7.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo;

7.2.1.2. Proteção contra adware e autodialers;

7.2.1.3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;

7.2.1.4. Arquivos abertos no smartphone;

7.2.1.5. Programas instalados usando a interface do smartphone

7.2.1.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;

7.2.2. Deverá isolar em área de quarentena os arquivos infectados;

7.2.3. Deverá atualizar as bases de vacinas de modo agendado;

7.2.4. Deverá bloquear spams de SMS através de Black lists;

7.2.5. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado com mensagem de aviso ao utilizador do dispositivo;

7.2.6. Capacidade de desativar por política: Wi-fi; Câmera; Bluetooth.

7.2.7. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;

7.2.8. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;

7.2.9. Deverá ter firewall pessoal (Android);

7.2.10. Capacidade de tirar fotos quando a senha for inserida incorretamente;

7.2.11. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;

7.2.12. Capacidade de enviar comandos remotamente de: Localizar; Bloquear.

7.2.13. Capacidade de detectar Jailbreak em dispositivos iOS;

7.2.14. Capacidade de bloquear o acesso a site por categoria em dispositivos;

7.2.15. Capacidade de bloquear o acesso a sites phishing ou malicioso;

7.2.16. Capacidade de bloquear o dispositivo quando o cartão “SIM” for substituído;

7.2.17. Capacidade de configurar White e blacklist de aplicativos;

7.2.18. Capacidade de localizar o dispositivo quando necessário;

7.2.19. Permitir atualização das definições quando estiver em “roaming”;

7.2.20. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

7.2.21. Deve permitir verificar somente arquivos executáveis;

7.2.22. Deve ter a capacidade de desinfectar o arquivo se possível;

7.2.23. Capacidade de agendar uma verificação;

7.2.24. Capacidade de enviar URL de instalação por e-mail;

7.2.25. Capacidade de fazer a instalação através de um link QRCode;

7.2.26. Capacidade de executar as seguintes ações caso a desinfecção falhe: Deletar; Ignorar; Quarentenar; Perguntar ao usuário.

8. Gerenciamento de dispositivos móveis (MDM)

8.1. Compatibilidade:

8.1.1. Dispositivos com os sistemas operacionais:

8.1.1.1. Android 5.0 – 5.1.1 ou superior

8.1.1.2. iOS 9.0 – 9.3.5 ou superior

8.1.2. Softwares de gerência de dispositivos:

8.1.2.1. Kaspersky Security Center 10 SP2 MR1 e superior;

8.1.2.2. Kaspersky Endpoint Security Cloud 3.0 e superior;

8.1.2.3. VMWare AirWatch 9.2 e superior;

8.1.2.4. MobileIron 9.6 e superior;

8.1.2.5. IBM Maas360 10.66 e superior;

8.1.2.6. SOTI MobiControl 14.1.0 (1152) e superior;

8.2. Características:

8.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

8.2.2. Capacidade de ajustar as configurações de: sincronização de e-mail; uso de aplicativos; senha do usuário; criptografia de dados; conexão de mídia removível.

8.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;

8.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS;

8.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;

8.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS;

8.2.7. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;

8.2.8. Permitir sincronização com perfil do “Touch Down”;

8.2.9. Capacidade de desinstalar remotamente o antivírus do dispositivo;

8.2.10. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;

8.2.11. Capacidade de sincronizar com Samsung Knox;

8.2.12. Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

9. Criptografia

9.1. Compatibilidade

9.1.1. Microsoft Windows 7 Ultimate/Enterprise/Professional SP1 ou superior x86/x64;

9.1.2. Microsoft Windows 8/8.1 Enterprise/Pro x86/x64;

9.1.3. Microsoft Windows 10 Enterprise x86/x64;

9.1.4. Microsoft Windows 10 Pro x86/x64;

9.1.5. Microsoft Windows 11;

9.2. Características

9.2.1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;

9.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

9.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;

9.2.4. Capacidade de utilizar *Single Sign-On* para a autenticação de pré-boot;

9.2.5. Permitir criar vários usuários de autenticação pré-boot;

9.2.6. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;

9.2.7. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

9.2.7.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

9.2.7.2. Criptografar todos os arquivos individualmente;

9.2.7.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

9.2.7.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

9.2.8. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;

9.2.9. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

9.2.10. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

9.2.11. Verificar compatibilidade de hardware antes de aplicar a criptografia;

9.2.12. Possibilita estabelecer parâmetros para a senha de criptografia;

9.2.13. Bloqueia o reuso de senhas;

9.2.14. Bloqueia a senha após um número de tentativas pré-estabelecidas;

9.2.15. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

9.2.16. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo

9.2.17. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;

9.2.18. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

9.2.19. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de áudio, etc;

9.2.20. Permite criar um grupo de extensões de arquivos a serem criptografados;

9.2.21. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;

9.2.22. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.

9.2.23. Capacidade de deletar arquivos de forma segura após a criptografia;

9.2.24. Capacidade de criptografar somente o espaço em disco utilizado;

9.2.25. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;

9.2.26. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;

9.2.27. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;

9.2.28. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;

9.2.29. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;

9.2.30. Capacidade de fazer “Hardware encryption”.

10. Gerenciamento de Sistemas

10.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores *bare-metal*;

10.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;

10.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;

10.4. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;

10.5. Capacidade de gerenciar licenças de softwares de terceiros;

10.6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;

10.7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, etc);

10.8. Possibilita fazer distribuição de software de forma manual e agendada;

10.9. Suporta modo de instalação silenciosa;

10.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;

10.11. Possibilita fazer a distribuição através de agentes de atualização;

10.12. Utiliza tecnologia multicast para evitar tráfego na rede;

10.13. Possibilita criar um inventário centralizado de imagens;

10.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;

10.15. Suporte a WakeOnLan para deploy de imagens;

10.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;

10.17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;

10.18. Capacidade de gerar relatórios de vulnerabilidades e patches;

10.19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;

10.20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;

10.21. Permite baixar atualizações para o computador sem efetuar a instalação;

10.22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;

10.23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;

10.24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;

10.25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;

10.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;

10.27. Capacidade de instalar atualizações ou correções somente em computadores definidos ou em grupos definidos conforme selecionado pelo administrador;

10.28. Capacidade de configurar o reinício do computador após a aplicação das atualizações e correções de vulnerabilidades;

10.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;

10.30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;

10.30.1. Capacidade de definir listas de tipos de objetos que não serão verificados;

10.30.2. Capacidade de definir listas de servidores que não terão o tráfego verificado;

10.30.3.Capacidade de definir grupos de usuários e aplicar regras de verificação por grupos.

4.2 PARCELAMENTO DO OBJETO (ART. 16, II)

No contexto da solução apontada pela equipe de planejamento da contratação e conforme as necessidades e os requisitos levantados nos itens 2.2 e 4.1 deste documento recomenda-se que o objeto seja dividido no item a seguir:

GRUPO	ITEM	DESCRIÇÃO
ÚNICO	1	Fornecimento da renovação de licenças de uso do software de antivírus Kaspersky Endpoint Security For Business com upgrade para ADVANCED, com suporte técnico, por 03 anos.

4.3 ADJUDICAÇÃO DO OBJETO (ART.16, III)

Uma vez que a solução é formada por um só item, para fins de licitação do objeto ensejador deste Estudo recomenda-se a adjudicação por item a um único fornecedor e em uma única parcela, o que simplifica a condução das atividades de gestão, fiscalização e controle do contrato, atendendo aos princípios da celeridade, economicidade e eficiência.

4.4 MODALIDADE E TIPO DE LICITAÇÃO (ART. 16, IV)

O artigo 1º da Lei 10.520 institui a modalidade denominada Pregão, para aquisição de bens e serviços comuns. Como já se demonstrou que o objeto a ser contratado é oferecido por diversos fornecedores no mercado de TIC e apresenta características padronizadas e usuais, conclui-se que o objeto é comum, portanto, sugere-se, como melhor opção, a utilização da modalidade “Pregão” sendo, preferencialmente, em sua forma eletrônica e do tipo “Menor Preço”, pelo Sistema de Registro de Preços.

4.5 CLASSIFICAÇÃO E INDICAÇÃO ORÇAMENTÁRIA (ART. 16, V)

Definição a ser realizada pela Diretoria Financeira.

4.6 VIGÊNCIA DA PRESTAÇÃO (ART. 16, VI)

Para o fiel cumprimento das obrigações será celebrado contrato de fornecimento com vigência de doze meses, de acordo com art. 57, caput, da Lei nº 8.666/1993.

4.7 EQUIPE DE APOIO À CONTRATAÇÃO (ART.16, VII)

Servidor 1		
Nome	**Matrícula**	**Telefone**
Marcos Aurélio Ferreira Nava	129023	98 3198-4540

Servidor 2		
Nome	**Matrícula**	**Telefone**
Leandro Cavalcante Mendonça Lima	164186	98 3198-4757

4.8 EQUIPE DE GESTÃO DA CONTRATAÇÃO (ART. 16, VIII)

A gestão do referido contrato ficará sob a responsabilidade da Diretoria de Informática e Automação, conforme Resolução GP 21/2018.

Gestor do Contrato		
Nome	**Matrícula**	**Telefone**
Cláudio Henrique Carneiro Sampaio	099176	98 3198-4581

Fiscal Técnico Titular		
Nome	**Matrícula**	**Telefone**
Marcos Aurélio Ferreira Nava	129023	98 3198-4540

Fiscal Técnico Substituto		
Nome	**Matrícula**	**Telefone**
Carlos Henrique Oliveira Silva	100941	98 3198-4743

Fiscal Administrativo		
Nome	**Matrícula**	**Telefone**
A definir	Nnnnnn	98 3198-nnnn

5. ANÁLISE DE RISCOS

Esta seção contém a descrição, a análise e o tratamento dos riscos e ameaças que possam vir a comprometer o sucesso em todas as fases da contratação.

Neste Estudo avaliou-se qualitativamente e quantitativamente cada risco identificado, bem como foram definidos a probabilidade de ocorrência de cada evento, os seus possíveis danos potenciais, as possíveis ações de prevenção e contingência, além da identificação dos responsáveis pela ação.

Usou-se a classificação escalar da probabilidade e do impacto na análise qualitativa dos riscos e estabeleceu-se a relação "probabilidade x impacto" na análise quantitativa, conforme tabelas a seguir:

Classificação	Valor
Baixo	1
Médio	2
Alto	3

Tabela da Escala qualitativa de classificação

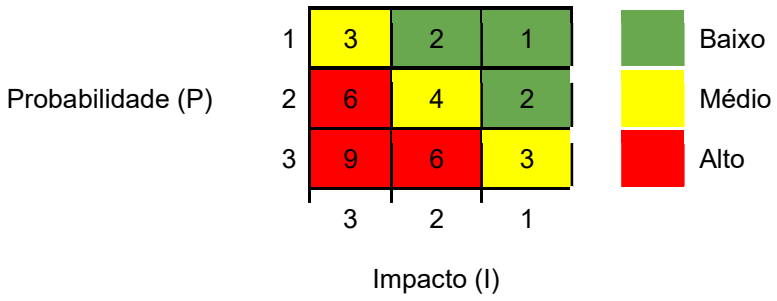


Tabela da Matriz de Probabilidade x Impacto

5.1 RISCOS DO PROCESSO DE CONTRATAÇÃO

Identificação dos Riscos

Id	Risco	Probabilidade (P)	Impacto (I)	Dano (PxI)	Fase
1	Licitação Deserta ou Fracassada	1	3	3	Contratação
2	Cotação incompatível com o objeto ou desatualizada	1	3	3	Contratação
3	Recursos Administrativos durante o Pregão	2	2	4	Contratação
4	Pedidos de Impugnação de Edital	1	3	3	Contratação
5	Indisponibilidade de orçamento para a contratação	1	3	3	Contratação
5	Objeto não atende as necessidades	1	3	3	Contratação
6	Atraso de Fornecimento	1	2	2	Execução
7	Serviços de garantia inoperante	1	3	3	Execução
8	Profissionais desqualificados ou insuficientes para prestar o suporte técnico no objeto	2	3	6	Execução
9	Quantidade do objeto contratado não atende a demanda	2	3	6	Execução

Planos de ação

Id	Ação Preventiva	Ação de Contingência	Responsável
1	Elaborar especificações técnicas compatíveis com produtos existentes no mercado	Atualizar as especificações técnicas da contratação	Equipe de planejamento da contratação
2	Realizar cotação de acordo com as características do objeto em fontes confiáveis para a pesquisa de preços	Realizar novas cotações revendo as características do objeto e as fontes da pesquisa de preços	Equipe de apoio à contratação
3	Redigir as especificações técnicas do objeto de forma clara e objetiva	Responder aos recursos administrativos	Equipe de planejamento da contratação e equipe de apoio à contratação

4	Redigir claramente as regras da contratação no Edital e seus anexos, atentando para as legislações vigente que impactam o objeto	Republicar o Edital com as correções necessárias	Equipe de planejamento da contratação e equipe de apoio à contratação
5	Consultar a administração quanto ao recursos disponíveis para a contratação	Realocação de recursos	Equipe de apoio à contratação
6	Consulta constante ao mercado sobre a disponibilidade do objeto e o tempo médio de fornecimento	Aplicar sanções contratuais	Equipes de fiscalização e gestão do contrato
7	Monitorar riscos	Aplicar sanções contratuais	Equipes de fiscalização e gestão do contrato
8	Exigir no edital a quantidade e qualificação mínima dos profissionais da contratada conforme objeto do contrato	Aplicar sanções contratuais	Equipes de fiscalização e gestão do contrato
9	Realizar estudo de quantitativo necessário para a demanda atual e de projeção futura	Realizar nova licitação ou adesão a ARP vigente que atenda a necessidade	Equipe de planejamento da contratação e equipe de apoio à contratação

6. DECLARAÇÃO DA VIABILIDADE DA CONTRATAÇÃO (IN04/2014, ART.12, VIII)

O presente ESTUDO TÉCNICO PRELIMINAR, elaborado pelos integrantes abaixo, considerando a análise das alternativas de atendimento das necessidades elencadas pela área requisitante e os demais aspectos normativos, conclui pela VIABILIDADE DA CONTRATAÇÃO da SOLUÇÃO para renovação dez mil novas licenças do software antivírus Kaspersky Endpoint Security for Business com upgrade para versão ADVANCED por um período de 3 (três) anos. A solução foi considerada a de melhor custo benefício, atendendo aos requisitos listados adequadamente e demandas formuladas, os custos previstos são compatíveis e os riscos identificados são administráveis, pelo que RECOMENDAMOS o prosseguimento da contratação.

Esta equipe de planejamento declara **VIÁVEL** esta contratação.

São Luís (MA), assinado e datado digitalmente.

Marcos Aurelio Ferreira Nava

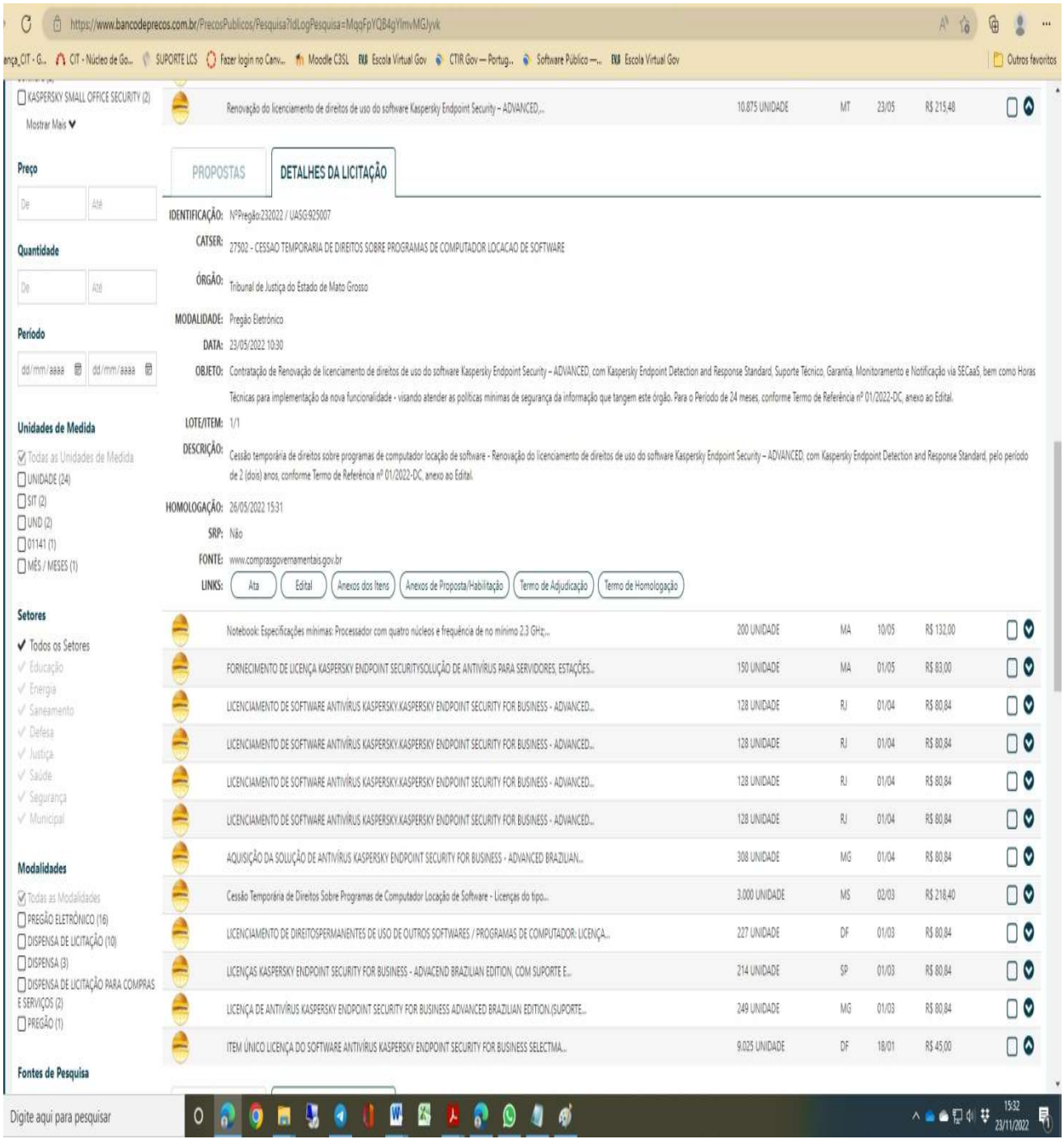
I

Leandro Cavalcante Mendonça Lima

ANEXO A – LISTA DE POTENCIAIS FORNECEDORES

Item	CNPJ	FORNECEDOR	TELEFONE	EMAIL
1	03.242.841/0001-01	E-SEC TECNOLOGIA EM SEGURANCA DE DADOS S/A	(61) 3323-4410	coelho@esec.com.br
2	30.738.505/0001-19	SS SERVICE & SOFTWARE LTDA	(11) 5112-9300	comercial@serviceti.inf.br
3	05.250.796/0001-54	NETWORK SECURE SEGURANCA DA INFORMACAO LTDA	(85) 3252-7020	andrea@networksecure.com.br
4	30.357.688/0001-22	4F SOLUCOES EM TECNOLOGIA LTDA	(61) 3037-2006	chrystian@4fti.com.br
5	12.007.998/0001-35	PISONTEC COMERCIO E SERVICOS EM TECNOLOGIA DA INFORMACAO EIRELI	(81) 3251-5110	licitacao@pisontec.com
6	10.685.932/0001-79	NOVA SERVICOS DE TECNOLOGIA DA INFORMACAO E NETWORKING EIRELI	(61) 3032-6602	jacob@grupoinovva.com.br
7	19.585.941/0001-62	SATURNO SOFTWARE E SISTEMAS LTDA	(71) 3506-8467	fiscal@jrsempresas.com.br
8	09.368.935/0001-08	ADVANCED RESELLER COMÉRCIO E SERVIÇOS DE TECNOLOGIA LTDA – EPP	(11) 2319-9898	raphael.meliti@arit.com.br
9	10.224.281/0001-10	QUALITEK TECNOLOGIA LTDA - EPP	(84) 4008-9454	jefferson.xavier@qualitek.com.br
10	22.122.370/0001-34	VTECH COMERCIO, SERVIÇOS E EQUIPAMENTOS DE INFORMÁTICA EIRELI	(71) 3289-0643	luciana@vtechti.com.br

ANEXO B – CONTRATAÇÕES SIMILARES REALIZADAS POR OUTROS ÓRGÃOS OU ENTIDADES DA ADMINISTRAÇÃO PÚBLICA



Renovação do licenciamento de direitos de uso do software Kaspersky Endpoint Security – ADVANCED,...	10.875 UNIDADE	MT	23/05	R$ 215,48

IDENTIFICAÇÃO: NºPregão:232022 / UASG:925007

CATSER: 27502 - CESSAO TEMPORARIA DE DIREITOS SOBRE PROGRAMAS DE COMPUTADOR LOCACAO DE SOFTWARE

ÓRGÃO: Tribunal de Justiça do Estado de Mato Grosso

MODALIDADE: Pregão Eletrônico

DATA: 23/05/2022 10:30

OBJETO: Contratação de Renovação de licenciamento de direitos de uso do software Kaspersky Endpoint Security – ADVANCED, com Kaspersky Endpoint Detection and Response Standard, Suporte Técnico, Garantia, Monitoramento e Notificação via SECaaS, bem como Horas Técnicas para implementação da nova funcionalidade - visando atender as políticas mínimas de segurança da informação que tangem este órgão. Para o Período de 24 meses, conforme Termo de Referência nº 01/2022-DC, anexo ao Edital.

LOTE/ITEM: 1/1

DESCRIÇÃO: Cessão temporária de direitos sobre programas de computador locação de software - Renovação do licenciamento de direitos de uso do software Kaspersky Endpoint Security – ADVANCED, com Kaspersky Endpoint Detection and Response Standard, pelo período de 2 (dois) anos, conforme Termo de Referência nº 01/2022-DC, anexo ao Edital.

HOMOLOGAÇÃO: 26/05/2022 15:31

SRP: Não

FONTE: www.comprasgovernamentais.gov.br

LINKS:

Notebook: Especificações mínimas: Processador com quatro núcleos e frequência de no mínimo 2.3 GHz;...	200 UNIDADE	MA	10/05	R$ 132,00
FORNECIMENTO DE LICENÇA KASPERSKY ENDPOINT SECURITYSOLUÇÃO DE ANTIVÍRUS PARA SERVIDORES, ESTAÇÕES...	150 UNIDADE	MA	01/05	R$ 83,00
LICENCIAMENTO DE SOFTWARE ANTIVÍRUS KASPERSKY.KASPERSKY ENDPOINT SECURITY FOR BUSINESS - ADVANCED...	128 UNIDADE	RJ	01/04	R$ 80,84
LICENCIAMENTO DE SOFTWARE ANTIVÍRUS KASPERSKY.KASPERSKY ENDPOINT SECURITY FOR BUSINESS - ADVANCED...	128 UNIDADE	RJ	01/04	R$ 80,84
LICENCIAMENTO DE SOFTWARE ANTIVÍRUS KASPERSKY.KASPERSKY ENDPOINT SECURITY FOR BUSINESS - ADVANCED...	128 UNIDADE	RJ	01/04	R$ 80,84
LICENCIAMENTO DE SOFTWARE ANTIVÍRUS KASPERSKY.KASPERSKY ENDPOINT SECURITY FOR BUSINESS - ADVANCED...	128 UNIDADE	RJ	01/04	R$ 80,84
AQUISIÇÃO DA SOLUÇÃO DE ANTIVÍRUS KASPERSKY ENDPOINT SECURITY FOR BUSINESS - ADVANCED BRAZILIAN...	308 UNIDADE	MG	01/04	R$ 80,84
Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software - Licenças do tipo...	3.000 UNIDADE	MS	02/03	R$ 218,40
LICENCIAMENTO DE DIREITOSPERMANENTES DE USO DE OUTROS SOFTWARES / PROGRAMAS DE COMPUTADOR: LICENÇA...	227 UNIDADE	DF	01/03	R$ 80,84
LICENÇAS KASPERSKY ENDPOINT SECURITY FOR BUSINESS - ADVACEND BRAZILIAN EDITION, COM SUPORTE E...	214 UNIDADE	SP	01/03	R$ 80,84
LICENÇA DE ANTIVÍRUS KASPERSKY ENDPOINT SECURITY FOR BUSINESS ADVANCED BRAZILIAN EDITION.(SUPORTE...	249 UNIDADE	MG	01/03	R$ 80,84
ITEM ÚNICO LICENÇA DO SOFTWARE ANTIVÍRUS KASPERSKY ENDPOINT SECURITY FOR BUSINESS SELECTMA...	9.025 UNIDADE	DF	18/01	R$ 45,00

ANEXO B-1. Banco de Preços – Licitação TJMG.

Pregão/Concorrência Eletrônica

Tribunal de Justiça do Estado de Mato Grosso

Termo de Adjudicação do Pregão Eletrônico

Pregão Nº 00023/2022 - (Decreto Nº 10.024/2019)

Às 15:51 horas do dia 24 de maio de 2022, após analisado o resultado do Pregão nº 00023/2022, referente ao Processo nº 0059400-30.2021, o Pregoeiro, Sr(a) ETELVINO ALVES DOS SANTOS NETO, ADJUDICA aos licitantes vencedores os respectivos itens, conforme indicado no quadro Resultado da Adjudicação.

**OBS: Itens com recursos serão adjudicados pela Autoridade competente e constarão no termo de julgamento.

Resultado da Adjudicação

Grupo 1
Tratamento Diferenciado: -
Aplicabilidade Margem de Preferência: Não
Critério de Valor: R$ 3.084.413,7600
Situação: Adjudicado

Adjudicado para: SOLO NETWORK BRASIL S.A. **, pelo melhor lance de** R$ 2.900.243,2800 **, com valor negociado a** R$ 2.890.022,0300 .

Itens do grupo:

- 1 - Cessão temporária de direitos sobre programas de computador locação de software
- 2 - Manutenção de Software (Corretiva, Preventiva, Adaptativa)
- 3 - Pagamento despesa com pessoal

Item: 1 - Grupo 1
Descrição: Cessão temporária de direitos sobre programas de computador locação de software
Descrição Complementar: Renovação do licenciamento de direitos de uso do software Kaspersky Endpoint Security – ADVANCED, com Kaspersky Endpoint Detection and Response Standard, pelo período de 2 (dois) anos, conforme Termo de Referência nº 01/2022-DC, anexo ao Edital.
Tratamento Diferenciado: -
Aplicabilidade Margem de Preferência: Não
Quantidade: 10.875 **Unidade de fornecimento:** UNIDADE
Valor Máximo Aceitável: R$ 2.343.290,6300 **Intervalo Mínimo entre Lances:** -
Situação: Adjudicado

Adjudicado para: SOLO NETWORK BRASIL S.A. **, pelo melhor lance de** R$ 2.177.500,0000 **, com valor negociado a** R$ 2.167.278,7500 .

Eventos do Item

Evento	Data	Observações
Adjudicado	24/05/2022 15:51:33	Adjudicação individual da proposta. Fornecedor:SOLO NETWORK BRASIL S.A., CNPJ/CPF:00.258.246/0001-68, Melhor lance : R$ 2.177.500,0000, Valor Negociado : R$ 2.167.278,7500

Item: 2 - Grupo 1
Descrição: Manutenção de Software (Corretiva, Preventiva, Adaptativa)
Descrição Complementar: Suporte Técnico, Monitoramento e Notificação via SECaaS, pelo período de 2 (dois) anos, conforme Termo de Referência nº 01/2022-DC, anexo ao Edital.
Tratamento Diferenciado: -
Aplicabilidade Margem de Preferência: Não
Quantidade: 1 **Unidade de fornecimento:** UND SERVIÇO TÉCNICO
Valor Máximo Aceitável: R$ 560.350,0000 **Intervalo Mínimo entre Lances:** -
Situação: Adjudicado

Adjudicado para: SOLO NETWORK BRASIL S.A. **, pelo melhor lance de** R$ 548.153,2800 .

ANEXO B-2. Banco de Preços – Adjudicação Licitação TJMG pág1.

Eventos do Item

Evento	Data	Observações
Adjudicado	24/05/2022 15:51:34	Adjudicação individual da proposta. Fornecedor:SOLO NETWORK BRASIL S.A., CNPJ/CPF:00.258.246/0001-68, Melhor lance : R$ 548.153,2800

Item: 3 - Grupo 1
Descrição: Pagamento despesa com pessoal
Descrição Complementar: Horas Técnicas para implementação da solução, conforme Termo de Referência nº 01/2022-DC, anexo ao Edital.
Tratamento Diferenciado: -
Aplicabilidade Margem de Preferência: Não
Quantidade: 650 **Unidade de fornecimento:** UNIDADE
Valor Máximo Aceitável: R$ 180.773,1300 **Intervalo Mínimo entre Lances:** -
Situação: Adjudicado

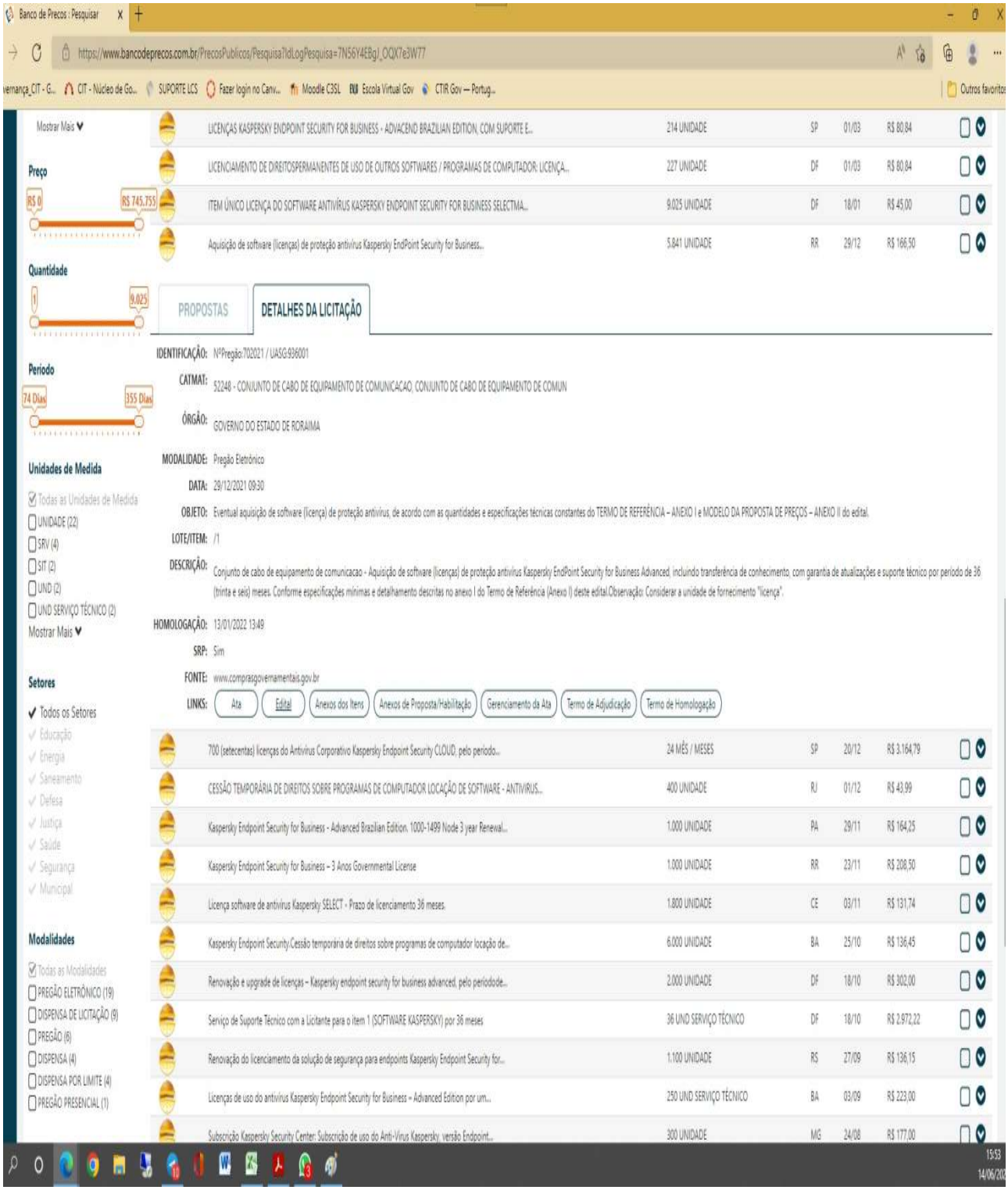
Adjudicado para: SOLO NETWORK BRASIL S.A. **, pelo melhor lance de** R$ 174.590,0000 .

Eventos do Item

Evento	Data	Observações
Adjudicado	24/05/2022 15:51:37	Adjudicação individual da proposta. Fornecedor:SOLO NETWORK BRASIL S.A., CNPJ/CPF:00.258.246/0001-68, Melhor lance : R$ 174.590,0000

Fim do documento

ANEXO B-3. Banco de Preços – Adjudicação Licitação TJMG pág2.



ANEXO B-4. Banco de Preços – Licitação Roraima.

Pregão/Concorrência Eletrônica

GOVERNO DO ESTADO DE RORAIMA

Termo de Adjudicação do Pregão Eletrônico

Pregão Nº 00070/2021 (SRP) - (Decreto Nº 10.024/2019)

Às 11:06 horas do dia 04 de janeiro de 2022, após analisado o resultado do Pregão nº 00070/2021, referente ao Processo nº 22101005846202173, o Pregoeiro, Sr(a) PAULO SERGIO DA SILVA MAIA, ADJUDICA aos licitantes vencedores os respectivos itens, conforme indicado no quadro Resultado da Adjudicação.

**OBS: Itens com recursos serão adjudicados pela Autoridade competente e constarão no termo de julgamento.

Resultado da Adjudicação

Item: 1
Descrição: Conjunto de cabo de equipamento de comunicacao
Descrição Complementar: Aquisição de software (licenças) de proteção antivírus Kaspersky EndPoint Security for Business Advanced, incluindo transferência de conhecimento, com garantia de atualizações e suporte técnico por período de 36 (trinta e seis) meses. Conforme especificações mínimas e detalhamento descritas no anexo I do Termo de Referência (Anexo I) deste edital. Observação: Considerar a unidade de fornecimento "licença".
Tratamento Diferenciado: -
Aplicabilidade Decreto 7174: Não
Aplicabilidade Margem de Preferência: Não
Quantidade: 5.841
Unidade de fornecimento: Unidade
Valor Máximo Aceitável: R$ 170,0000
Intervalo Mínimo entre Lances: R$ 1,00
Situação: Adjudicado

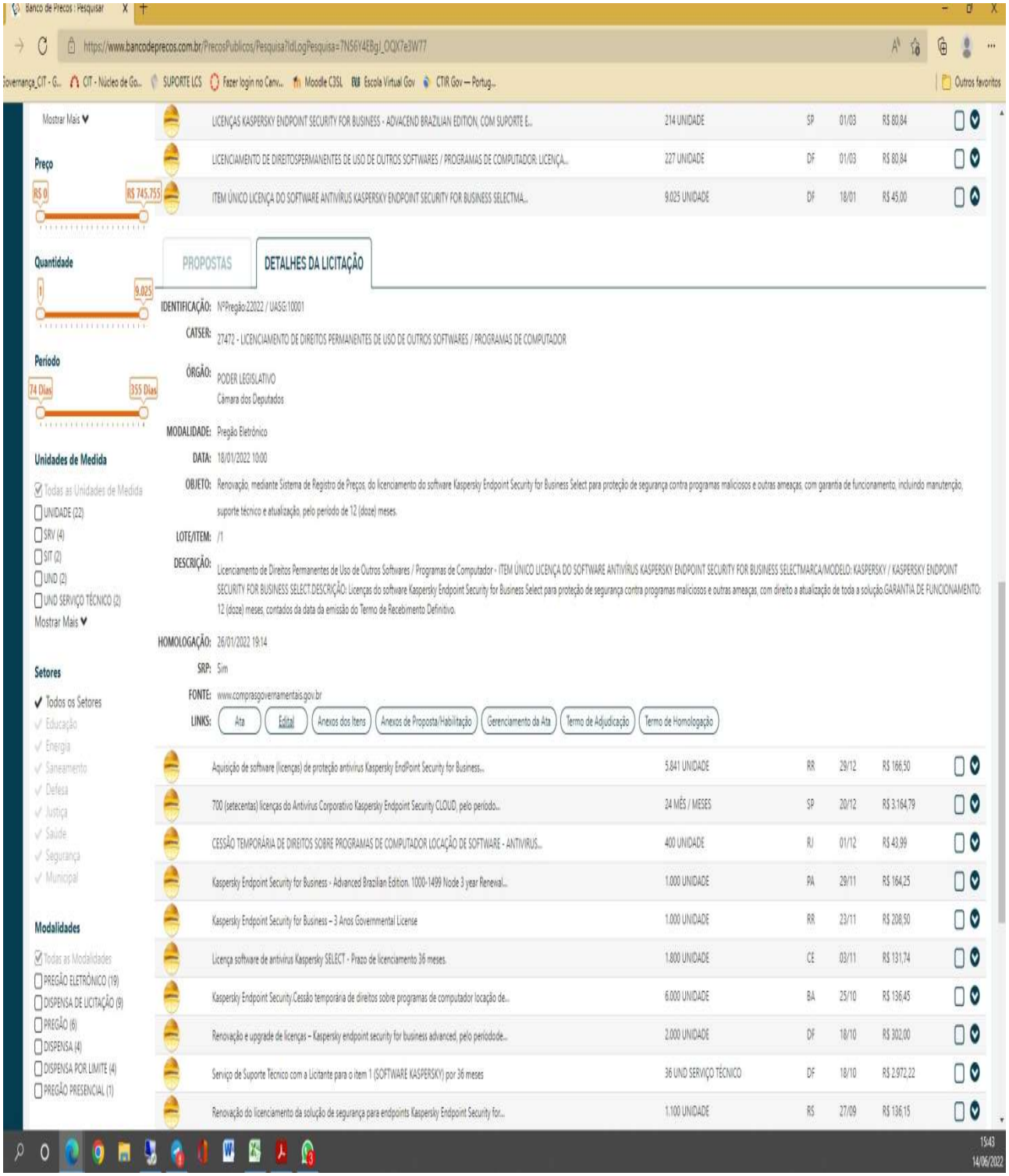
Adjudicado para: VTECH COMERCIO, SERVICOS E EQUIPAMENTOS DE INFORMATICA **, pelo melhor lance de** R$ 163,0000 **, com valor negociado a** R$ 160,0000 **e a quantidade de** 5.841 **Unidade** .

Eventos do Item

Evento	Data	Observações
Adjudicado	04/01/2022 11:06:22	Adjudicação em grupo da proposta. Fornecedor: VTECH COMERCIO, SERVICOS E EQUIPAMENTOS DE INFORMATICA, CNPJ/CPF: 22.122.370/0001-34, Melhor lance: R$ 163,0000, Valor Negociado: R$ 160,0000

Fim do documento

ANEXO B-5. Banco de Preços – Adjudicação Licitação Roraima.



ANEXO B-6. Banco de Preços – Licitação Câmara dos Deputados.

Pregão/Concorrência Eletrônica

PODER LEGISLATIVO
Câmara dos Deputados

Termo de Adjudicação do Pregão Eletrônico

Pregão Nº 00002/2022 (SRP) - (Decreto Nº 10.024/2019)

Às 11:34 horas do dia 20 de janeiro de 2022, após analisado o resultado do Pregão nº 00002/2022, referente ao Processo nº 256.615/2021, o Pregoeiro, Sr(a) VANDERLEI ALMEIDA VELOSO, ADJUDICA aos licitantes vencedores os respectivos itens, conforme indicado no quadro Resultado da Adjudicação.

**OBS: Itens com recursos serão adjudicados pela Autoridade competente e constarão no termo de julgamento.

Resultado da Adjudicação

Item: 1
Descrição: Licenciamento de Direitos Permanentes de Uso de Outros Softwares / Programas de Computador
Descrição Complementar: ITEM ÚNICO LICENÇA DO SOFTWARE ANTIVÍRUS KASPERSKY ENDPOINT SECURITY FOR BUSINESS SELECT MARCA/MODELO: KASPERSKY / KASPERSKY ENDPOINT SECURITY FOR BUSINESS SELECT. DESCRIÇÃO: Licenças do software Kaspersky Endpoint Security for Business Select para proteção de segurança contra programas maliciosos e outras ameaças, com direito a atualização de toda a solução. GARANTIA DE FUNCIONAMENTO: 12 (doze) meses, contados da data da emissão do Termo de Recebimento Definitivo.
Tratamento Diferenciado: -
Aplicabilidade Decreto 7174: Não
Aplicabilidade Margem de Preferência: Não
Quantidade: 9.025
Unidade de fornecimento: UNIDADE
Valor Estimado: R$ 39,5200
Intervalo Mínimo entre Lances: 0,50 %
Situação: Adjudicado

Adjudicado para: E-SEC TECNOLOGIA EM SEGURANCA DE DADOS S/A **, pelo melhor lance de** R$ 30,8300 **, com valor negociado a** R$ 30,0000 **e a quantidade de** 9.025 **UNIDADE** .

Eventos do Item

Evento	Data	Observações
Adjudicado	20/01/2022 11:34:42	Adjudicação individual da proposta. Fornecedor: E-SEC TECNOLOGIA EM SEGURANCA DE DADOS S/A, CNPJ/CPF: 03.242.841/0001-01, Melhor lance: R$ 30,8300, Valor Negociado: R$ 30,0000

Fim do documento

ANEXO B-7. Banco de Preços – Adjudicação Licitação Câmara Deputados.

3. Escopo do Projeto.

Propostas comercial para aquisição de novas licenças kaspersky endpoint security for business advanced para o TJMA

4. Proposta Comercial:

Produto	Período	Part Number	Quantidade	Valor Usuário R$
Kaspersky Endpoint Security for Business - Advanced	1 year	KL4867KA*F8	7000	114,26
Kaspersky Endpoint Security for Business - Advanced	1 year	KL4867KA*F8	10000	108,81

5. Forma de Pagamento

Boleto à vista

Frete: já incluso para todo o estado de São Paulo

Os impostos já estão incluídos nos preços apresentados nesta proposta, qualquer alteração ocorrida entre a da validade da proposta e a do faturamento dos produtos, que importe em aumento ou redução das atuais alíquotas dos tributos neles incidentes, será repassada ao valor acima indicado.

6. Prazo de Entrega

Até 45 dias úteis.

7. Validade da Proposta

Esta proposta é válida por 20 dias.

A AR IT agradece a oportunidade.

09.368.935/0001-08
ADVANCED RESELLER COMÉRCIO E SERVIÇOS DE TECNOLOGIA LTDA-EPP
RUA DO GRITO, 387 13° ANDAR CJ 134
IPIRANGA - CEP 04217-000
SÃO PAULO - SP

Raphael Meliti
Account Manager
E-mail: raphael.meliti@arit.com.br
Phone: (11) 2319-9898

ANEXO B-8. Proposta 1 AR IT -TJMA.

Intelligence for Technology

3. Escopo do Projeto.

Propostas comercial para aquisição de novas licenças kaspersky endpoint security for business advanced para o TJMA

4. Proposta Comercial:

Produto	Período	Part Number	Quantidade	Valor Usuário R$
Kaspersky Endpoint Security for Business - Advanced	3 year	KL4867KA*T8	7000	228,51
Kaspersky Endpoint Security for Business - Advanced	3 year	KL4867KA*T8	10000	217,63

5. Forma de Pagamento

Boleto à vista

Frete: já incluso para todo o estado de São Paulo

Os impostos já estão incluídos nos preços apresentados nesta proposta, qualquer alteração ocorrida entre a da validade da proposta e a do faturamento dos produtos, que importe em aumento ou redução das atuais alíquotas dos tributos neles incidentes, será repassada ao valor acima indicado.

6. Prazo de Entrega

Até 45 dias úteis.

7. Validade da Proposta

Esta proposta é válida por 20 dias.

A AR IT agradece a oportunidade.

09.368.935/0001-08
ADVANCED RESELLER COMÉRCIO E SERVIÇOS DE TECNOLOGIA LTDA-EPP
RUA DO GRITO, 387 13° ANDAR CJ 134
IPIRANGA - CEP 04217-000
SÃO PAULO - SP

Raphael Meliti
Account Manager
E-mail: raphael.meliti@arit.com.br
Phone: (11) 2319-9898

DELL Technologies TITANIUM PARTNER · KASPERSKY SILVER PARTNER · vmware professional PARTNER · Quest Partner Circle · SONICWALL

ANEXO B-9. Proposta 2 AR IT -TJMA.

NETWORK SECURE

PROPOSTA COMERCIAL:

	Produto	Qde.	Valor unit. (R$)	Total (R$)
( )	Kaspersky Endpoint Security for Business – ADVANCED – 3 anos	10.000	162,00	1.620.000,00

CONDIÇÕES GERAIS

- Incluso serviço de implantação, configuração e suporte técnico durante 36 meses
- Preço das licenças em Reais (R$)
- Faturamento Network Secure
- **Condições de pagamento licenças:** Empenho
- Prazo de entrega licenças: até 10 dias
- Validade da proposta: 60 dias

Recife-PE, 04 de Outubro de 2022

Atenciosamente,

NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

ANEXO B-10. Proposta 1 Networksecure -TJMA.

NETWORK SECURE

PROPOSTA COMERCIAL:

	Produto	Qde.	Valor unit. (R$)	Total (R$)
( )	Kaspersky Endpoint Security for Business – ADVANCED – 3 anos	7000	198,00	1.386.000,00

CONDIÇÕES GERAIS

- Incluso serviço de implantação, configuração e suporte técnico durante 36 meses
- Preço das licenças em Reais (R$)
- Faturamento Network Secure
- **Condições de pagamento licenças:** Empenho
- Prazo de entrega licenças: até 10 dias
- Validade da proposta: 60 dias

Recife-PE, 04 de Outubro de 2022

Atenciosamente,

_____

NETWORK SECURE SEGURANCA DA INFORMACAO LTDA

ANEXO B-11. Proposta 2 Networksecure -TJMA.

Qualitek

I. Proposta Comercial

Natal, 04 de Outubro de 2022.

TRIBUNAL DE JUSTIÇA DO MARANHÃO
Proposta Comercial

Prezado Sr. Marcos Aurélio,

Apresento abaixo a proposta comercial para aquisição de solução de segurança.

Item 1 – Licenciamento Kaspersky Endpoint Security for Business – 1 ano

Descrição	Qnt	Preço Und R$	Total R$
Kaspersky Endpoint Security for Business – Advanced – Base Plus – 1 ano.	10000	R$ 109,81	**R$ 1.098.100,00**

Item 2 – Licenciamento Kaspersky Endpoint Security for Business – 3 anos

Descrição	Qnt	Preço Und R$	Total R$
Kaspersky Endpoint Security for Business – Advanced – Base Plus – 3 anos.	10000	R$ 227,63	**R$ 2.276.300,00**

Observações:

- **A reinstalação do software devido à formatação da máquina, não está incluso nos serviços de suporte;**
- **Faturamento:** Qualitek Tecnologia Ltda (CNPJ: 10.224.281/0001-10);
- **Prazo para pagamento:** 30 dias após o faturamento
- **Previsão de entrega:** Em até 10 dias;
- **Impostos:** Inclusos;
- **Validade da Proposta**: 60 dias.

Autorizo o faturamento dos serviços acima, e estou de acordo com as condições comerciais acima citadas.

Data	Nome e Função do Responsável pela Aprovação	Assinatura

Atenciosamente,

Jefferson Xavier
jefferson.xavier@qualitek.com.br

ANEXO B-12. Proposta Qualitec -TJMA.

VTECH SEGURANÇA DE INFORMAÇÃO
PROPOSTA DE PREÇOS
07/10/2022

produtos de segurança em todo o mundo) à frente da concorrência. A missão da empresa é sempre estar um passo à frente da concorrência ao fornecer excelência: a melhor proteção possível e garantir que o portfólio de produtos da empresa permaneça na vanguarda do mercado.

DOS PREÇOS

ESPECIFICAÇÕES /MARCA	Qtd Licenças	Valor Unitário (R$	Valor Total (R$)
Solução de antivírus Kaspersky Endpoint Security For Business **ADVANCED**, prazo de licenciamento 36 meses, com serviços de instalação e suporte técnico, pelo período 03 anos	**7.000**	**R$ 238,51**	**R$ 1.668.170,00**
Solução de antivírus Kaspersky Endpoint Security For Business **ADVANCED**, prazo de licenciamento 36 meses, com serviços de instalação e suporte técnico, pelo período 03 anos	**10.000**	**R$ 219,63**	**R$ 2.196.300,00**

A validade desta proposta é de 60 (Sessenta dias).

O prazo de entrega é de 15 (quinze) dias corridos, contatos do aviso de empenho.

Prazo de Garantia: O prazo de garantia técnica, manutenção e suporte remoto é de 36 meses.

Luciana Santos da Silva | luciana@vtechti.com.br
Gerente Comercial
CNPJ: 22.122.370/0001-34
Endereço: AV SANTOS DUMONT, 4487, KM: 3-5, LOJA: 157; SHOPPING; PASSEIO NORTE; CEP: 42.702-400, Estrada do Coco, Lauro de Freitas, Bahia.
Tel: (71)3289-0643 | 9 9625-5980
Insc. Municipal: 001.001.7482 | Insc. Estadual: 123.555.216 ME

Luciana Santos da Silva
CPF: 790.641.595-72

ANEXO B-13. Proposta VTECH -TJMA.