Estudos Preliminares

CONTRATAÇÃO DE SOLUÇÃO DE ANTIVÍRUS ENDPOINT

Sumário

[1 ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO (Art. 14) 4](#_Toc99538559)

[1.1 Contextualização 4](#_Toc99538560)

[1.2 Definição e Especificação dos Requisitos da Demanda (Art. 14, I) 6](#_Toc99538561)

[1.3 Soluções Disponíveis no Mercado de TIC (Art. 14, I, a) 7](#_Toc99538562)

[1.4 Contratações Públicas Similares (Art. 14, I, b) 9](#_Toc99538563)

[1.5 Outras Soluções Disponíveis (Art. 14, II, a) 11](#_Toc99538564)

[1.6 Portal do Software Público Brasileiro (Art. 14, II, b) 11](#_Toc99538565)

[1.7 Alternativas no Mercado de TIC (Art. 14, II, c) 11](#_Toc99538566)

[1.8 Modelo Nacional de Interoperabilidade – MNI (Art. 14, II, d) 11](#_Toc99538567)

[1.9 Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (Art. 14, II, e) 11](#_Toc99538568)

[1.10 Modelo de Requisitos Moreq-Jus (Art. 14, II, f) 12](#_Toc99538569)

[1.11 Análise dos Custos Totais da Demanda (Art. 14, III) 12](#_Toc99538570)

[1.12 Escolha e Justificativa da Solução (Art. 14, IV) 13](#_Toc99538571)

[1.13 Descrição da Solução (Art. 14, IV, a) 19](#_Toc99538572)

[1.14 Alinhamento da Solução (Art. 14, IV, b) 21](#_Toc99538573)

[1.15 Benefícios Esperados (Art. 14, IV, c) 22](#_Toc99538574)

[1.16 Relação entre a Demanda Prevista e a Contratada (Art. 14, IV, d) 22](#_Toc99538575)

[1.17 Requisitos Temporais (Art.3,V) 23](#_Toc99538576)

[1.18 Adequação do Ambiente (Art. 14, V, a, b, c, d, e, f) 24](#_Toc99538577)

[1.19 Orçamento Estimado (Art. 14, II, g) 24](#_Toc99538578)

[2 SUSTENTAÇÃO DO CONTRATO (Art. 15) 26](#_Toc99538579)

[2.1 Recursos Materiais e Humanos (Art. 15, I) 26](#_Toc99538580)

[2.2 Qualificação técnica dos Profissionais (Art. 18, §3º, III, a, 10) 26](#_Toc99538581)

[2.3 Descontinuidade do Fornecimento (Art. 15, II) 27](#_Toc99538582)

[2.4 Transição Contratual (Art. 15, III, a, b, c, d, e) 27](#_Toc99538583)

[2.5 Estratégia de Independência Tecnológica (Art. 15, IV, a, b) 28](#_Toc99538584)

[2.6 Direitos de Propriedade Intelectual e Autorais 28](#_Toc99538585)

[3 ESTRATÉGIA PARA A CONTRATAÇÃO (Art. 16) 28](#_Toc99538586)

[3.1 Natureza do Objeto (Art. 16, I) 28](#_Toc99538587)

[3.2 Parcelamento e Adjudicação do Objeto (Art. 16, II) 29](#_Toc99538588)

[3.2.1 Subcontratação 32](#_Toc99538589)

[3.2.2 Do consórcio 32](#_Toc99538590)

[3.2.3 Da amostra 33](#_Toc99538591)

[3.3 Modalidade e Tipo de Licitação (Art. 16, IV) 33](#_Toc99538592)

[3.3.1 Não aplicação da Lei Complementar 123/2006, alterada pela Lei Complementar n. 147/2014 33](#_Toc99538593)

[3.4 Classificação e Indicação Orçamentária (Art. 16, V) 34](#_Toc99538594)

[3.5 Vigência do Contrato (Art. 16, VI) 35](#_Toc99538595)

[3.6 Equipe de Apoio e Gestão à Contratação (Art. 16, VII) 36](#_Toc99538596)

[4 ANÁLISE DE RISCOS 38](#_Toc99538597)

[Anexo A 43](#_Toc99538598)

[LISTA DOS PRINCIPAIS FORNECEDORES 43](#_Toc99538599)

[Anexo B 45](#_Toc99538600)

[Contratações Públicas Similares 45](#_Toc99538601)

[Anexo C 51](#_Toc99538602)

[ORÇAMENTOS 51](#_Toc99538603)

[Anexo d 54](#_Toc99538604)

[DESCRITIVO TÉCNICO DA SOLUÇÃO 54](#_Toc99538605)

[Anexo e 57](#_Toc99538606)

[EVIDÊNCIA DE SOLICITAÇÃO DE PROPOSTA 57](#_Toc99538607)

# ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO (Art. 14)

## Contextualização

Conforme contextualização apresentada no Documento de Oficialização da Demanda, visando a proteção de dados mais próxima ao usuário final, o Poder Judiciário de Mato Grosso se utiliza de solução de antivírus da marca Kaspersky, cuja última atualização de requisitos técnicos ocorrera em março de 2019.

A opção pela marca Kaspersky foi adotada, inicialmente, em 2016 e vem sendo atualizada desde então pela eficácia técnica das soluções contratadas, sempre alinhadas com o mercado de TIC, garantindo também o melhor aproveitamento de investimento prévio.

A solução utilizada atualmente para suprir esta demanda, qual seja Kaspersky Endpoint Security – ADVANCED, com suporte, monitoramento e notificação via SECaaS vem atendendo as expectativas, detectando mais de 70 mil ameaças nos últimos 11 meses, como pode ser verificado na tabela abaixo:

Tabela

Descrição gerada automaticamente

Tabela 1: Gestão de Antivírus do Relatório de Indicadores de Segurança / Dezembro 2021

Com o fim da vigência do Contrato nº 15/2019, assim como da vigência do direito de atualização das licenças de antivírus endpoint, março e maio respectivamente, se faz necessária nova contratação para dar continuidade ao atendimento da demanda hoje suprida pela solução contratada da Karspersky, além da possibilidade de aprimoramento nos serviços prestados.

Apesar da qualidade já demonstrada da solução contratada em 2019, através de estudos de mercado, a equipe técnica de segurança da informação deste Poder Judiciário identificou possibilidade de melhoria com relação aos níveis de detalhamento das informações que disponíveis na solução em funcionamento que podem ser sanadas através de ferramentas de Detecção e Respostas.

Em suma, os serviços de proteção de endpoint mais atuais dispõe de funcionalidades que vão além da simples proteção contra ocorrências pontuais de malwares ou ransonwares nos dispositivos, mas também munem a equipe técnica com informações mais aprofundadas, que podem ser cruciais para identificação de ataques cibernéticos de maior magnitude contra o ecossistema tecnológico, dentre outras possibilidades.

Cabe frisar que em levantamento realizado quanto ao Status da Segurança 2021, apresentado no Plano de Trabalho Segurança 2022 / 2023, fica evidente que dos incidentes de segurança ocorridos no último ano, aproximadamente 47% se tratavam de infecção por ransomware ou vírus, como pode ser visto nas figuras abaixo.

Gráfico, Gráfico de barras

Descrição gerada automaticamente

Figura 1 – Incidentes de Segurança – Linha do Tempo 2021

Gráfico, Gráfico de pizza

Descrição gerada automaticamente

Figura 2 – Incidentes de Segurança – Linha do Tempo 2021

Portanto, fica evidente que o investimento em soluções que aprimorem a linha de defesa contra este tipo de incidente está totalmente alinhado com a estratégia de melhoria efetiva dos processos de segurança da instituição.

Desta forma, cabe reforçar a necessidade de que, para a contratação que se pretende formalizar, sejam atendidos todos os requisitos de segurança mais aderentes à realidade deste Poder Judiciário e de seus usuários internos.

## Definição e Especificação dos Requisitos da Demanda (Art. 14, I)

A contratação pretendida, qual seja “Contratação de software de antivírus” consiste na aquisição de licenças com suporte técnico e garantia, visando atender as políticas mínimas de segurança da informação que tangem este órgão.

Os principais requisitos para o presente projeto são:

* Suporte técnico e garantia do fabricante ou empresa devidamente credenciada e autorizada por aquele;
* Suporte técnico baseado por indicadores de medição de resultados, para tratamento de incidentes e resolução de problemas 24x7.
* Suporte especializado a ser prestado na modalidade on-site (quando necessário), nas dependências do respectivo órgão Contratante, sem prejuízo ao atendimento via remoto/telefone.
* Proteção de todos os equipamentos, atuais e novos a serem adquiridos, contra softwares indesejados;
* Impedir a disseminação e proliferação de ameaças virtuais;
* Monitoramento da infraestrutura lógica do PJMT, por conta da Contratada, em disposição 24x7;
* Aprimoramento nos mecanismos de SECaaS com recurso da solução avançada de Detecção e Resposta de incidentes;
* O sistema de Detecção e Resposta deve:
  + Detectar elevação de privilégios;
  + Permitir coleta de dados do sistema;
  + Criar regras de notificações por e-mail;
  + Executar tarefas de deleção de objeto, quarentena ou recuperação de arquivos, execução de scripts, isolamento de hosts, dentre outras.
* O sistema de Detecção de Resposta deve permitir integração com as seguintes ferramentas de SIEM: ArchSight, Wazuh.

## Soluções Disponíveis no Mercado de TIC (Art. 14, I, a)

O mercado de tecnologia apresenta diversos fabricantes para atender a Solução de Antivírus de endpoint (estação de trabalho/ notebooks / smartphones/servidores, entre outros) realizando a proteção e detecção de atividades maliciosas na infraestrutura de TIC do PJMT.

Para nos auxiliar na identificação das principais empresas que atuam em uma determinada área fornecendo soluções de Tecnologia da Informação (TI), muitas vezes o Departamento de Conectividade recorre ao Quadrante Mágico do Gartner. Esse Quadrante Mágico é um relatório gráfico muito importante para contribuir na tomada de decisões em negócios tecnológicos. Ele possibilita aos órgãos uma visão mais ampla sobre os produtos disponíveis no mercado, podendo analisar vantagens ao adquirir alguma solução em TI.

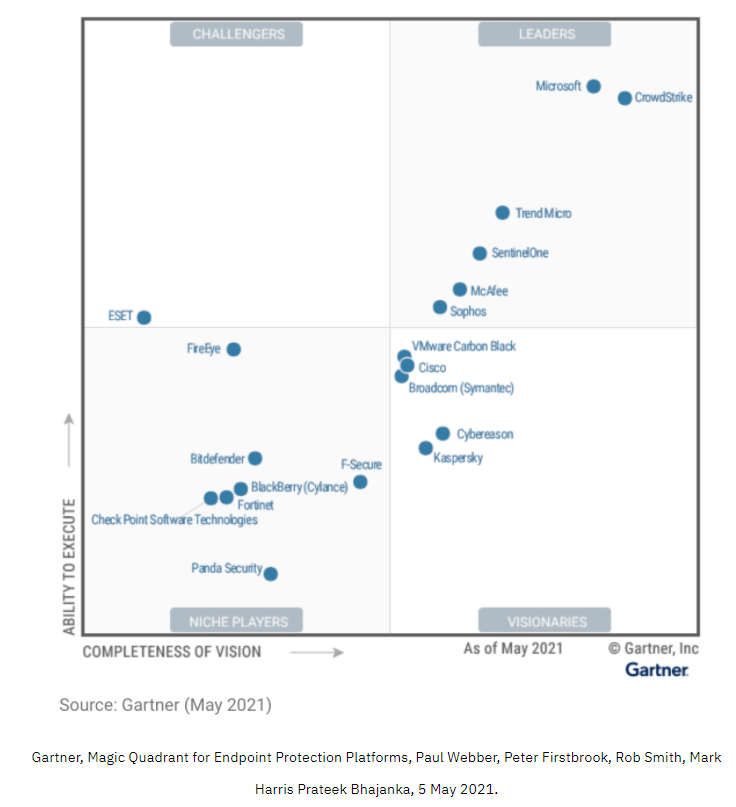
Para a solução de antivírus, utilizamos o Quadrante Mágico para *Endpoint Protection Plataforms*, conforme mostrado na figura a seguir. 

Figura 3 - Quadrante Mágico Solução de Antivírus

Ainda que a característica principal dos antivírus comercializados no mercado de TIC seja a proteção de endpoints contra malwares, ransonwares e demais ameaças cibernéticas, existe uma variação de funcionalidades que podem ser ofertadas em cada solução, de acordo com a necessidade da demanda.

Tal variação envolve desde a ampliação da proteção para servidores de terminal, dispositivos móveis, gateways da Web, gerenciamento de criptografia, SIEM, soluções de inteligência artificial, detecção e resposta, dentre tantas outras funcionalidades.

Por este motivo, é de extrema importância considerar o cenário de cada instituição, como a arquitetura de infraestrutura de TIC para se obter a definição mais adequada para análise e escolha dos requisitos de segurança, suporte, monitoramento da solução a ser contratada, concomitante com os requisitos técnicos propostos pelas diversas fabricantes que atuam nesta solução.

Outro fator a ser considerado é pela forma de contratação, tendo as opções de aquisição de licenças perpétuas com direito de atualização e suporte técnico, ou ainda pela utilização do software como serviço (SaaS).

## Contratações Públicas Similares (Art. 14, I, b)

Após pesquisa na internet, foram encontrados os seguintes Pregões Eletrônicos similares, constantes do Anexo B deste Estudo Preliminar:

* **Justiça Federal de Primeiro Grau no Ceará – Pregão Eletrônico nº 29/2021** - Registro de preços para eventual serviços de renovação, suporte técnico e garantia da SOLUÇÃO ANTIVIRUS KASPERSKY ENDPOINT SECURITY FOR BUSINESS - SELECT BRAZILIAN, conforme especificações e demais condições detalhadas no termo de referência

**Contrato 41/2021 – Com vigência a partir de 03/12/2021**.

* **Superior Tribunal Militar – Pregão Eletrônico nº 49/2021 –**Contratação de empresa especializada para renovação das licenças do Antivírus para solução Kaspersky Endpoint Security for Business Advanced, com direito a atualizações e treinamento, por 36 meses.

**Contrato 31/2021 – Com vigência a partir de 20/12/2021**;

* **Prefeitura de Manaus – Pregão Eletrônico nº 100/2021–** Contratação de licenças da solução de segurança de Endpoint Kaspersky Security for Business Advanced, para atender a Manausprev.

**ARP 08/2022 – Registrada em 15 de fevereiro de 2022**;

* **Tribunal de Justiça Militar do Estado de Minas Gerais – Pregão Eletrônico nº 05/2021–** Aquisição de 325 (trezentas e vinte e cinco) licenças do antivírus Kaspersky Endpoint Security Corporativo, incluindo atualizações, garantia e suporte técnico pelo período de 36 (trinta e seis) meses para continuar cobrindo com a presente solução a demanda de segurança da informação da Justiça Militar de Minas Gerais.

**Contrato 10/2021 – Com vigência a partir de 14/07/2021**;

* **Secretaria da Fazenda do Governo do Estado do Ceará – Pregão Eletrônico nº 20210007–** Aquisição de Licenças Perpetua do Software Kaspersky Endpoint Security For Business Select, com o objetivo de atender às demandas relacionadas a proteção de dados em endpoint e servidores contra malwares e ransomware, visando a continuidade dos serviços de TI e integridade das informações da Secretaria da Fazenda do Ceará.

**Contrato 38/2021 – Com vigência a partir de 11/06/2021**;

* **Universidade Federal do Rio Grande do Sul – Pregão Eletrônico nº 07/2021–** Renovação do licenciamento da solução de segurança para dispositivos fins (computadores, servidores e dispositivos móveis) Kaspersky Endpoint Security for Business Advanced, já instalado e em produção na UFRGS, bem como suas renovações anuais, por um prazo de 48 meses.

**Contrato 13/2021 – Com vigência a partir de 23/03/2021**;

Cada órgão possui peculiaridades acerca de tamanho e de forma de infraestrutura computacional, de demandas internas atuais e de projetos futuros, de crescimento do parque, de desenvolvimento de sistemas, de servidores efetivos, de colaboradores terceirizados e etc., de modo que não há como se ter conhecimento da estratégia presente e futura de cada um deles, tornando, portanto, a comparação entre os órgãos, algo totalmente inviável.

Importante salientar que as licitações informadas foram realizadas em 2021. Importante salientar, ainda, que os ambientes computacionais possuem diferentes características em sua estrutura e nem todos os certames levantados atendem a todos os requisitos da contratação ora pretendida.

## Outras Soluções Disponíveis (Art. 14, II, a)

Não foram encontradas outras soluções disponíveis além das já apresentadas no item 1.3 deste Estudo Preliminar.

## Portal do Software Público Brasileiro (Art. 14, II, b)

Não se aplica ao contexto deste Estudo Preliminar, por não se tratar de aquisição de software, e sim de aquisição de licenças e contratação de serviços de atualização e suporte técnico.

## Alternativas no Mercado de TIC (Art. 14, II, c)

Não há alternativa no mercado de TIC que não as que já explicitadas neste Estudo Preliminar.

## Modelo Nacional de Interoperabilidade – MNI (Art. 14, II, d)

É cediço que o Modelo Nacional de Interoperabilidade definido pelas equipes técnicas dos órgãos (STF - CNJ - STJ - CJF - TST - CSJT - AGU e PGR), de acordo com as metas do Termo de Cooperação Técnica nº 58/2009-CNJ, visa estabelecer os padrões para o intercâmbio de informações de processos judiciais e assemelhados, entre os diversos órgãos de administração de justiça, além de servir de base para a implementação das funcionalidades pertinentes no âmbito do sistema processual.

Nesse contexto, não se aplica a este Estudo, uma vez que a demanda está relacionada à aquisição de licenças e contratação de serviços de atualização e suporte técnico.

## Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (Art. 14, II, e)

Inicialmente, salutar a explanação da conceituação da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil: É uma cadeia hierárquica de confiança, que enseja a emissão de certificados digitais para a identificação virtual do cidadão.

Inaplicável ao caso em comento, pois a demanda está relacionada à aquisição de licenças e contratação de serviços de atualização e suporte técnico e garantia.

## Modelo de Requisitos Moreq-Jus (Art. 14, II, f)

Tal modelo, instituído pela Resolução nº 91/2009-CNJ, apresenta os requisitos que os documentos digitais produzidos pelo Judiciário e os sistemas informatizados de gestão documental deverão cumprir no intuito de garantir a segurança e a preservação das informações, assim como a comunicação com outros sistemas.

Não se aplica ao contexto deste Estudo Preliminar, já que não se relaciona à Gestão de Processos e Documentos do Poder Judiciário, mas sim de demanda à aquisição de licenças e contratação de serviços de atualização e suporte técnico e garantia.

## Análise dos Custos Totais da Demanda (Art. 14, III)

Os custos da contratação que se pretende abrangem a Solução de Antivírus, contemplando licenciamento, além de serviço de suporte técnico e garantia. Esta premissa é válida para todas as opções de mercado, como pode ser confirmado nas contratações públicas apresentadas no item 1.4 deste Estudo Preliminar.

Para o licenciamento do serviço de Antivírus, existem as possibilidades de aquisição de licenças, em caráter perpétuo, incluindo o serviço de atualização das mesmas, ou da contratação como serviço, seja por subscrição (uso das licenças atualizadas por um período pré-definido) ou pela modalidade de uso de software como serviço na nuvem.

Em caso de aquisição de licenças, o pagamento é realizado em parcela única, de forma antecipada (por via de regra), além da possibilidade de atualização de versão, que usualmente é negociado como um serviço complementar. Já nos casos dos serviços de subscrição ou software como serviço, o dispêndio financeiro ocorre de forma periódica, de acordo com a negociação.

Já o suporte técnico geralmente é contratado em forma de serviço, podendo ou não contemplar serviços especializados complementares, com pagamento periódico, sob demanda, ou até mesmo antecipado.

## Escolha e Justificativa da Solução (Art. 14, IV)

Considerando as opções de mercado apresentadas no item 1.3 deste Estudo Preliminar, a escolha da solução deve estar alinhada ao atendimento dos requisitos da demanda, restando a definição da fabricante com o melhor custo-benefício para o Poder Judiciário de Mato Grosso.

Conforme contextualização apresentada neste artefato, o PJMT é detentor de 10.750 licenças Kaspersky Endpoint Protection – ADVANCED, resultado de investimentos prévios realizados nas 2 (duas) últimas contratações (aquisição, upgrade e renovação).

O quadrante mágico apresentado na figura 3 do item 1.3 deste Estudo Preliminar, faz uma avaliação macro, considerando todos os aspectos / funcionalidades possíveis das plataformas de proteção a endpoints. Contudo, é importante ressaltar que cada instituição possui necessidades especificas e, portanto, deve se avaliar os requisitos de cada demanda para identificar qual solução / fabricante seria a mais adequada.

Neste contexto, cabe destacar também outro estudo do Gartner denominado “Gartner Peer Insights ‘Voice of the Customer’: Endpoint Protection Platforms”, publicado em novembro de 2021, que aborda a avaliação dos usuários das principais plataformas de proteção de endpoints.

Neste documento são apresentadas além de uma avaliação geral das fabricantes, diversas avaliações categorizadas por tamanho das empresas / corporações, setor público, segmento de finanças, serviços, dentre outras.

A figura abaixo, por exemplo, ilustra a classificação dos clientes do setor público, na qual as empresas são categorizadas entre 4 grupos: *Aspiring* – Aspirante, *Established* – Estabelecido, *Strong Performer* - Forte Participante e *Customer’s Choice* – Escolha do Cliente.

Diagrama

Descrição gerada automaticamente com confiança média

Figura 4 - Quadrante “*Voice of the Customer”* para Plataformas de Proteção de Endpoint

Ao avaliar as opções disponíveis dos principais fabricantes do mercado nacional, fica evidente que para cada solução apresentada, são disponibilizados alguns recursos comuns entre eles, além de recursos adicionais para situações e requisitos específicos. Esta premissa é válida, inclusive, dentro das opções disponibilizadas por uma mesma fabricante, variando nível de proteção dos Endpoints.

Tendo em vista que a solução atual vem suprindo as necessidades deste Poder Judiciário, além de apresentar-se como forte participante no mercado em questão, é correto afirmar que a sua manutenção seria a opção mais alinhada aos requisitos técnicos da demanda, assim como pelo aproveitamento de *know-how* e investimento prévio.

Contudo, é preciso considerar também a inclusão de um novo requisito para esta contratação, qual seja da possibilidade de aprimoramento da solução no quesito de detecção e resposta de incidentes de segurança da informação, que não se faz presente na solução atual.

Para suprir esta nova demanda, a solução já utilizada pelo Poder Judiciário de Mato Grosso pode ser aprimorada com a inclusão do serviço *Kaspersk*y *Endpoint Detection and Response Standard,* garantindo um mecanismo de detecção e resposta automatizado, com acesso às informações oficiais da fabricante para aplicação das melhores práticas de segurança da informação a nível de desktops de usuários, juntamente com recursos de análise forense.

A implementação desta nova funcionalidade requer o envolvimento de equipe especializada que detenha conhecimento específico para configuração da solução tanto no gerenciamento, quanto nos endpoints que compõe a estrutura computacional do Poder Judiciário de Mato Grosso.

Novamente, as principais fabricantes apresentadas no quadro do item 1.3 deste artefato possuem soluções que atendem todos os requisitos desta nova demanda, mas ao considerar as soluções da Kaspersky, é possível consolidar a aquisição mais ajustada aos requisitos tanto técnico quanto de negócios ora apresentados nesta contratação.

Somado a isso, o aproveitamento de investimento prévio, na aquisição das licenças de endpoint security traz uma vantagem competitiva para esta fabricante, uma vez que não seria necessário aquisição de novas licenças para proteção dos ativos (computadores, notebooks, celulares, dentre outros) já utilizados no PJMT, mas somente o direito de atualização das 10.875 licenças já utilizadas.

Portanto, considerando o fino alinhamento entre os requisitos da demanda com a solução da fabricante Kaspersky, somado ao aproveitamento financeiro na opção de renovação de licenças já adquiridas, a escolha mais adequada para este projeto consiste na Contratação de Renovação de licenciamento de direitos de uso do software *Kaspersky Endpoint Security – ADVANCED* com *Kaspersky Endpoint Detection and Response STANDARD,* Suporte Técnico, Monitoramento e Notificação via SECaaS e Horas Técnicas para implementação da nova funcionalidade.

**1.12.1 Indicação de Marca**

Como cediço, através da inteligência do artigo 7º, §5º da Lei 8.666/93 c/c com o artigo 15, §7º, inciso I, desta mesma norma, há expressa vedação quanto a imputação específica de marca, em atenção a lisura, imparcialidade, isonomia e eticidade que os instrumentos convocatórios requerem.

Nesta seara, o Tribunal de Contas da União, no Acórdão nº 1553/2008 – Plenária, aborda sobre a temática. Vejamos:

***“A vedação imposta por esse dispositivo é um dos mecanismos utilizados pelo legislador no sentido de conferir efetividade aos princípios informativos da licitação, entre esses o da livre concorrência, o do julgamento objetivo e o da igualdade entre os licitantes”* (Acórdão 1553/2008 – Plenário.)**

Todavia, não se pode olvidar a expressa ressalva na norma supracitada, qual seja: a possibilidade de indicação de marca, nos casos em que tecnicamente justificável fazê-lo, com espeque na ausência de similaridade de objeto correlato, de forma que a vedação à indicação de marca em certames licitatórios não é absoluta. E, intrínseca a essa situação excepcional, este Estudo Preliminar se ampara. Veja que, conforme já delineado anteriormente, não existe outra solução no mercado que seja capaz de garantir a continuidade do atendimento da demanda com as melhorias pontuais pretendidas, com aproveitamento de investimento já realizado. As opções no mercado são de troca da solução, não havendo espaço, assim, para outras formas de contratação. Aliado a isso, tem-se a questão da criticidade do projeto, que por si só é deveras sensível. O tempo de implantação de nova solução excederia, sem sombra de dúvidas, o prazo de vigência do contrato atual, comprometendo diretamente a segurança de informação deste Poder Judiciário.

Há casos em que a restrição por determinadas marcas é lícita e até recomendável, como é o caso do presente projeto, que, se contrário fosse, perder-se-ia todo um investimento feito desde os idos de 2016 na solução hora defendida.

Com o fito de embasar este cenário, salutar a análise do enunciado nº 270 da Súmula da Jurisprudência do TCU:

**Súmula nº 270, TCU: *Em licitações referentes a compras, inclusive de softwares, é possível a indicação de marca, desde que seja estritamente necessária para atender exigências de padronização e que haja prévia justificação.***

Este entendimento, que resguarda, além do parâmetro de qualidade, a facilitação na descrição do objeto almejado, se alinha perfeitamente ao caso em comento, tornando efetivo o princípio da padronização contido no artigo 15, inciso I da Lei 8.666/93:

***Art.15. As compras, sempre que possível, deverão***

***I - atender ao princípio da padronização, que imponha compatibilidade de especificações técnicas e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas; (***Grifo nosso***)***

Nesta baila, segue entendimento doutrinário do jurista Marçal Justen Filho**[[1]](#footnote-2)**:

***É possível a contratação de fornecedores exclusivos ou a preferência por certas marcas desde que essa seja a solução mais adequada para satisfazer as necessidades coletivas. Não se admite a opção arbitrária, destinada a beneficiar determinado fornecedor ou fabricante. (***Grifo nosso***)***

Quanto a justificativa técnica para fundamentar a estrita necessidade da indicação, em observância ao princípio da impessoalidade, arrazoamos que a solução já utilizada pelo Poder Judiciário de Mato Grosso será mantida, havendo somente a necessidade de renovação dos direitos de atualização, assim como o incremento de funcionalidade de detecção e resposta (KEDR). Trata-se, portanto, de um *“upgrade”* da solução atual, para atender o crescimento natural da demanda se segurança da informação.

Do ponto de vista da economicidade, a renovação das licenças do software de segurança endpoint Kaspersky implica não ser necessário o custo adicional para a contratação de treinamento especializado para capacitar os servidores e técnicos envolvidos.

É importante esclarecer que a opção pela continuidade da solução já adotada da marca Kaspersky não se dá somente por aproveitamento de investimento prévio, mas principalmente pela qualidade do serviço e dos resultados até então alcançados, conforme evidências apresentadas na contextualização deste Estudo Preliminar.

Do ponto de vista administrativo, o Departamento de Conectividade desenvolveu experiência prática em lidar com incidentes e problemas durante os 6 (seis) anos em que a solução de segurança Kaspersky para estações de trabalho se encontra em operação no órgão. Dispor desta experiência na solução atual assegura melhores condições na identificação, efetividade e celeridade na resolução de problemas que se apresentem no decorrer do tempo.

O desempenho da solução já utilizada por este Poder Judiciário é condizente, inclusive, com a realidade do mercado internacional de Antivírus, que apresenta a fabricante Checkpoint entre as principais fabricantes no Quadrante Magico do Gartner apresentado no item 1.3 deste Estudo Preliminar.

De outro norte, o TCU, em diversos julgados, tem se manifestado pela possibilidade excepcional de indicação de marca em licitações, desde que fundadas em razões de ordem técnica ou econômica, devidamente justificadas, como feito in casu, hipóteses nas quais não há ofensa ao princípio da isonomia, nem tampouco restrições ao caráter competitivo do certame (Decisão n. 664/2001 - Plenário; Acórdão n. 1.010/2005 - Plenário e Acórdão n. 1.685/2004 - 2ªCâmara). (TCU, Acórdão 1.122/2010, Primeira Câmara, Rel. Min. Marcos Bemquerer Costa, DOU 12/03/2010).

Uma eventual substituição de marca resultaria não somente no descarte precoce de licenças em plenas condições de uso, mas também na perda da expertise adquirida pela equipe técnica do Departamento de Conectividade na utilização da solução da fabricante Kaspersky.

Corroborando o exposto, tem-se que a numerosa existência de empresas no ramo, como demonstrado no ANEXO A, fornecedoras dos produtos / serviços abordados e autorizadas à comercialização dos mesmos, tornam exígua a tese de restrição a competitividade.

Ademais disso, a indicação recai sobre marca consolidada no mercado, cujas características são imprescindíveis para satisfação do interesse público, consoante às evidências apresentadas no item 1.3 deste Estudo Preliminar.

Assim, aclarado qualquer questionamento atinente a eventual cláusula restritiva ao caráter competitivo do certamente em questão, já que, como esmiuçado, há correspondência à justificativa técnica para se fazer uso da indicação emanada.

Veja que não se está a limitar a competitividade e ferir a isonomia. Trata-se, na verdade, de uma alternativa da Administração para selecionar um objeto que atenda de modo escorreito às suas necessidades, ensejando continuidade da utilização de marca já adotada.

## Descrição da Solução (Art. 14, IV, a)

A solução escolhida, qual seja “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 e Horas Técnicas para implementação da nova funcionalidade” visa dar continuidade ao licenciamento e suporte apropriado para este porte crítico de software, bem como, melhorar a segurança digital e antecipar possíveis ameaças à infraestrutura lógica de arquivos e dados do PJMT.

A solução escolhida contempla licenciamento e serviços, para atender o Poder Judiciário de Mato Grosso.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lote** | **Item** | **Descrição** | **Qtde** | **Tipo** |
| 1 | 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. | 10.875 | Serviço |
| 2 | Suporte Técnico, Monitoramento e Notificação via SECaaS, pelo período de 2 (dois) anos. | 1 | Serviço |
| 3 | Horas Técnicas para implementação da solução. | 650 | Horas |

**ITEM 1**

Renovação do licenciamento de direitos de uso do software *Kaspersky Endpoint Security - ADVANCED*, com upgrade *Kaspersky Endpoint Detection and Response STANDARD*, pelo período de 2 (dois) anos.

**ITEM 2**

Suporte Técnico com garantia, monitoramento e Notificação via SECaaS, pelo período de 2 (dois) anos.

Este serviço deve contemplar tanto as funcionalidades adquiridas junto à fabricante para o pleno funcionamento da solução, quanto o serviço de suporte técnico da própria contratada, que será responsável direta pelo atendimento à equipe técnica do PJMT.

Para este documento, a definição de SECaaS é uma solução de serviço que alerta proativamente quando ocorrem incidentes de segurança. Essa solução SECURITY-as-a-Service deverá oferecer um método para detectar invasores em um estágio inicial e evitar que criminosos cibernéticos tenham acesso à rede ou aplicativos/softwares mal-intencionados, utilizando, mas não limitando a procura por comportamento suspeito durante as várias fases de um ataque.

O SECaaS deverá prover, minimamente:

1. Atualizações constantes de definições de malware que não dependem da conformidade do usuário;
2. Maior perícia em análises de segurança do parque tecnológico do Tribunal de Justiça de Mato Grosso;
3. Subsidiar com documentos/relatórios/análises a equipe técnica de forma a auxiliar na tomada de decisão;
4. O gerenciamento de logs;
5. Uma interface Web que permita a administração interna de tarefas, bem como visão do ambiente de segurança e das atividades em andamento.
6. A Manutenção e o suporte técnico remoto e/ou presencial (help desk) por parte da Proponente às dúvidas de utilização do software por parte do TJMT.
7. A Proponente junto com a equipe técnica do TJMT deverá montar um cronograma de implantação de todas as funcionalidades que a ferramenta oferece:
   1. A implantação das funcionalidades de gerenciamento de licenças, controle de admissão na rede, ferramenta de gestão de instalação de softwares, ferramenta de gestão de imagens/provisionamento, gerenciamento de correções e atualizações e a verificação de vulnerabilidades serão feitas, gradualmente pela equipe da Proponente, com acompanhamento do TJMT, devendo ao final de cada funcionalidade implementada ocorrer a transferência de conhecimento desta nova ferramenta.

**ITEM 3**

Apesar da solução Kaspersky Endpoint Security já estar instalada e configurada neste Poder Judiciário, se faz necessário a implementação da funcionalidade Kaspersky Endpoint Detection and Response Standard advinda do upgrade previsto no item 1 do objeto desta contratação.

Esta implementação deve ser realizada pelos profissionais da empresa contratada, podendo ter o apoio técnico da fabricante da solução.

Dentre as atividades, deve se prever desde o planejamento da implementação, o desenvolvimento – atualização, importação, instalação, update, customização, criação de alertas e configuração – tanto do security center quanto dos 10875 endpoints, estabilização, testes e repasse de conhecimento.

## Alinhamento da Solução (Art. 14, IV, b)

Atender as metas do Planejamento Estratégico Participativo (PEP) 2021-2026 do PJMT:

**PEP 4.1:**

**Tema:** Programa de Transformação Digital.

**Nome do Projeto:** Modernização de TIC do PJMT.

**Objetivo Estratégico:** Fortalecer a estratégia e infraestrutura de TIC, assegurando a transformação necessária ao negócio.

**Iniciativa Estratégica:** Contratação de empresa para fornecimento de software de antivírus para atender o PJMT.

**Justificativa:** A contratação de software de antivírus justifica-se pelo fato de os ataques às estações de trabalho e servidores de dados serem cada vez mais frequentes e sofisticados. Além disso, as melhorias dos sistemas de segurança contribuem com a redução de incidentes e, assim, minimizam o vazamento indevido de informação sensível.

**Plano Anual de Contratações de TIC - 2021:** Esta ação está prevista no Plano Anual de Contratações de TIC 2021, item E.12 / Essencial.

## Benefícios Esperados (Art. 14, IV, c)

A motivação para a contratação que ora se pretende se dá em face da necessidade de se garantir maior segurança da informação para os usuários do PJMT, através da proteção das estações de trabalho (microcomputadores), notebooks e servidores de rede, dispositivos móveis, como base na utilização de software antivírus.

Os benefícios diretos que se almejam com a contratação são:

* Impedir o acesso, disseminação e proliferação de ameaças virtuais;
* Tornar mais eficaz o gerenciamento de incidentes, beneficiando a rotina de trabalho dos usuários do PJMT;
* Manter o parque tecnológico em nível de segurança adequado;
* Melhoria na gestão e suporte técnico dos equipamentos endpoints (equipamento de uso final seja ele um computador, celular smartphone ou servidor, onde se instala o antivírus);
* Proteção de dados e da continuidade dos processos de negócios das ameaças sofisticadas e de ataques cibernéticos.

## Relação entre a Demanda Prevista e a Contratada (Art. 14, IV, d)

Esta contratação visa dar continuidade ao licenciamento e suporte apropriado para este porte crítico de segurança da informação de software, com seus devidos aprimoramentos, de acordo com os requisitos da demanda.

Desde a implantação da solução de antivírus da marca Kaspersky, em 2016, o PJMT atingiu um quantitativo de 10.875 licenças para proteção de endpoints de forma a atender o quantitativo de equipamentos passíveis de gerenciamento.

O direito de atualização dessas licenças garante a atualização de vacinas e filtragens contra ataques maléficos, seguindo as variações tecnológicas das formas de intrusão desenvolvidas pelos diversos agentes maliciosos existentes no mundo cibernético.

Para a contratação ora pretendida, ter-se-á os seguintes respectivos quantitativos e a previsão de distribuição dos serviços para este PJMT se dará conforme explanação abaixo:

**Item 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**, com quantitativo suficiente para manter a proteção de todos os dispositivos eletrônicos gerenciados pela solução Kaspersky atualmente, aprimorados com o serviço de Detecção e Resposta STANDARD, pelo período da vigência contratual de 2 (dois) anos.

**Item 2: Suporte Técnico, Monitoramento e Notificação via SECaaS,** pelo período suficiente para garantir o suporte técnico adequado à solução contratada, acompanhando a vigência contratual de 2 (dois) anos.

**Item 3: Horas Técnicas para implementação da nova funcionalidade**, com quantitativo suficiente para configurar a ferramenta de detecção e resposta tanto no security center, quanto nos 10.875 endpoints do parque tecnológico do PJMT – quantidade de licenças Kaspersky em uso pelo PJMT, estimando-se um total de 650 (seiscentos e cinquenta) horas para execução de todos os serviços descritos.

## Requisitos Temporais (Art.3,V)

Com o fim da vigência do Contrato nº 15/2019, em 18/03/2022, a renovação de software antivírus Kaspersky Endpoint Advanced, a contratação do serviço de suporte técnico, monitoramento e notificação via SECaaS- Security, além de horas técnicas para implantação / configuração da solução, deverão ter início imediato após a assinatura do Contrato.

O contrato que ora se pretende firmar terá vigência de 24 (vinte e quatro) meses, podendo ser prorrogado.

## Adequação do Ambiente (Art. 14, V, a, b, c, d, e, f)

**Infraestrutura tecnológica**: A solução prevista nessa contratação utilizará a rede lógica corporativa existente do TJMT.

**Infraestrutura elétrica**: A disponibilização de energia elétrica ficará por conta deste TJMT.

**Logística de execução/implantação**: A instalação e configuração das novas soluções de software, serão instalados e configurados pela equipe técnica da Contratada, como devido acompanhamento da equipe técnica do Departamento de Conectividade do PJMT. Todo serviço de suporte técnico será executado por profissionais da Contratada.

**Espaço físico e mobiliário**: A disponibilização de espaço físico e mobiliário para o serviço especializado ficará por conta deste TJMT.

**Impacto Ambiental**: Não haverá impacto ambiental na implantação da solução objeto deste Estudo Preliminar.

## Orçamento Estimado (Art. 14, II, g)

Os valores referentes à solução constam da tabela abaixo, e seu pagamento será realizado após o aceite definitivo dos itens, mediante apresentação das respectivas notas fiscais das licenças / serviços e demais documentos habilitatórios. Desta forma, garante-se o pleno funcionamento integral da solução, pelo período de 24 (vinte e quatro) meses.

Os pagamentos dos serviços de licenciamento e suporte técnico com garantia serão realizados da seguinte maneira:

O pagamento para os itens 1 e 2 será realizado em parcela única, após o recebimento definitivo.

A comercialização do serviço de atualização de licenças de antivírus Endpoint Kaspersky é feita através de pagamento antecipado pelo período pretendido. Como a pretensão desta contratação é de uma vigência contratual de 24 meses, a fabricante comercializa o serviço unitário de 2 anos para cada licença contratada.

A mesma premissa é válida para o serviço de monitoramento e suporte técnico, pois ainda que este seja prestado pela representante, também envolve funcionalidades técnicas adquiridas junto à fabricante da solução, também comercializada de forma antecipada pela Kaspersky.

Esta modalidade vem sendo adotada, inclusive, nos contratos do próprio Poder Judiciário da solução desta fabricante (Contratos 15/2019 e 59/2015 TJMT).

Já para o item 3, o pagamento será efetuado mediante consumo mensal das horas técnicas necessárias para implantação / configuração da solução, com apresentação das respectivas notas fiscais e relatório técnico da execução dos serviços.

Os itens da demanda possuem variações quanto ao custo e a forma de execução, conforme clarificado abaixo.

A estimativa dos custos totais da demanda foi baseada em valores registrados em orçamentos privados, levando-se em consideração o quantitativo necessário para atender a demanda deste Poder Judiciário.

Em pesquisas realizadas no Radar de Preço do TCE/MT, assim como demais ferramentas de pesquisas de contratações públicas, não foram identificadas aquisições com as mesmas especificações elencadas para a contratação que se pretende firmar nestes autos (Anexo C).

O próprio Contrato 15/2019 TJMT não pode ser utilizado como parâmetro de preço público para a contratação que se pretende, tendo em vista a inclusão de nova funcionalidade na solução.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Lote** | **Item** | **Descrição** | **Qtde** | **Tipo** | **Valor**  **Unit. (R$)** | **Valor**  **Total (R$)** |
| 1 | 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. | 10.875 | Serviço | R$ 215,48 | R$ 2.343.290,63 |
| 2 | Suporte Técnico, Monitoramento e Notificação via SECaaS, pelo período de 2 (dois) anos. | 1 | Serviço | R$ 560.350,00 | R$ 560.350,00 |
| 3 | Horas Técnicas para implementação da solução. | 650 | Horas | R$ 278,11 | R$ 180.773,13 |

Durante a vigência do Contrato de Manutenção e Suporte, o TJMT terá direito à atualização de versões do software feita sem custo adicional. Em caso de necessidade de treinamento de usuários para novas versões, esse deverá ser feito sem custos adicionais e, para tanto, será admitida a modalidade a distância.

O valor estimado para a aquisição da solução objeto deste Estudo Preliminar é de **R$ 3.084.413,75**.

# SUSTENTAÇÃO DO CONTRATO (Art. 15)

## Recursos Materiais e Humanos (Art. 15, I)

**Recursos materiais:** Todos os recursos materiais necessários para a execução dos serviços deverão ser fornecidos pela empresa, sem necessidade de aquisição de nenhum objeto ou suprimento adicional por parte deste PJMT.

**Recursos humanos:** A execução dos serviços a serem prestados pelos profissionais da Contratada desta contratação presume, além do acompanhamento de sua conformidade legal pelo Fiscal Técnico do Contrato, também dos demais profissionais da diretoria de Conectividade, da Coordenadoria de Tecnologia da Informação.

## Qualificação técnica dos Profissionais (Art. 18, §3º, III, a, 10)

Para os itens 2 e 3, serviço de suporte técnico, monitoramento e notificação via SECaaS e Implantação e Configuração do serviço de Detecção e Resposta STANDARD, a empresa deverá apresentar na reunião de kick-off comprovação de que consta em sua equipe de atendimento, profissionais com as seguintes certificações da fabricante da solução, sem custos adicionais para o Poder Judiciário de Mato Grosso:

* Kaspersky Endpoint Security and Management.
* Protecting Windows Servers and Embedded Systems.
* Kaspersky Anti Targeted Attack Platform.

As certificações acima listadas estão diretamente relacionadas ao escopo do serviço previsto nesta contratação. Desde o gerenciamento da solução de segurança de endpoint, sistemas, até a plataforma contra ataques direcionados, visando a entrega de um serviço de suporte técnico e implementação / configuração de maior agilidade e eficácia, junto à empresa Contratada.

Será indispensável a apresentação de documentação original do emissor responsável que comprove a validade das certificações acima enquanto durar o contrato. Eventual indício de fraude ensejará na abertura de diligência por parte do Poder Judiciário de Mato Grosso.

## Descontinuidade do Fornecimento (Art. 15, II)

Se, por qualquer eventualidade, a empresa Contratada frustrar total ou parcialmente o objeto da avença, será necessária aplicação de penalidades, e ser observado o cadastro de reserva para convocação da empresa subsequente na ordem de classificação, acaso tenha, ou elaboração de novo processo de licitação. Inobstante isso, comunicação à Procuradoria Geral do Estado com vistas a início de processo em face da Contratada.

Entretanto, a garantia deverá ser fornecida pelo Fabricante, independente de termo firmado com a Contratada, para aqueles produtos já entregues e recebidos definitivamente~~.~~

## Transição Contratual (Art. 15, III, a, b, c, d, e)

Ao decorrer da vigência contratual de 24 (vinte e quatro) meses os fiscais técnicos da solução deverão realizar acompanhamento de mercado para definição se o modelo de contratação ora proposto se mantém atualizado e adequado às necessidades do Poder Judiciário de Mato Grosso ou não.

Visto a possibilidade de renovação dos itens 1 e 2 do contrato até o limite de 48 (quarenta e oito) meses, caberá às equipes técnicas, previamente ao final da vigência, elaborar estudos que permitam seguir com o modelo ora adotado ou reavaliá-lo para novo processo de contratação.

A revogação dos perfis de acesso à rede e sistemas deste Tribunal, concedidos para a execução contratual, bem como a eliminação de caixas postais (e-mail corporativo) porventura criados para os profissionais externos alocados, será realizada em até 10 (dez) dias após o encerramento contratual, pela equipe técnica dos Departamentos de Suporte e Informações e de Conectividade.

## Estratégia de Independência Tecnológica (Art. 15, IV, a, b)

Não se aplica ao contexto desta contratação, já que não versa sobre desenvolvimento de softwares sob encomenda no mercado de TIC.

## Direitos de Propriedade Intelectual e Autorais

São do Contratante todos os direitos de propriedade intelectual e direitos autorais associados ao material produzido em suas dependências.

# ESTRATÉGIA PARA A CONTRATAÇÃO (Art. 16)

## Natureza do Objeto (Art. 16, I)

A contratação objeto deste Estudo Preliminar constitui solução de Tecnologia da Informação e Comunicação, composta por licenciamentos e serviço de suporte técnico, de necessidade contínua, para garantir a integridade, confidencialidade e segurança das informações da Rede de Dados que trafegam dentro do Poder Judiciário de Mato Grosso.

Justifica-se como contínua a demanda já que perene e essencial, visto que abrange os serviços de Segurança da Informação, podendo interferir diretamente na prevenção contra ações de softwares mal intencionados à rede de dados do PJMT, colocando em risco a integridade dos dados por ela trafegados, afetando diretamente a produtividade dos serviços jurisdicionais, além de possíveis danos materiais, morais.

## Parcelamento e Adjudicação do Objeto (Art. 16, II)

O objeto desse Estudo Preliminar constitui lote único composto por 03 (três) itens. Tal agrupamento dos itens em lote se dá em face da indivisibilidade técnica da solução, de modo que os itens se interconectam entre si, conforme delineado abaixo.

Cumpre ponderar que, ao decidir pelo procedimento do julgamento das propostas em licitações, cujos objetos constituem-se bens divisíveis, que podem ser apartados em itens, bem como diversos itens podem ser agrupados em lotes, a Administração lançando-se do poder discricionário que tem, definiu que para o certame objetivado houvessem vencedores ao lote contendo itens agrupados, não descurando do interesse público, que demanda ser otimizado.

Portanto, ao se licitar por lote, deve o administrador analisar a viabilidade técnica e econômica de dividir-se o objeto licitatório, pois segundo Justen Filho: "*a obrigatoriedade do fracionamento respeita limites de ordem técnica e econômica. Não se admite o fracionamento quando tecnicamente isso não for viável ou, mesmo, recomendável. O fracionamento em lotes deve respeitar a integridade qualitativa do* *objeto a ser executado. (...) a unidade do objeto a ser executado não pode ser destruída através do fracionamento*".

Esclarece-nos Carvalho Carneiro acerca do conceito de viabilidade técnica e econômica, informando que: "*a viabilidade técnica diz respeito à integridade do objeto, não se admitindo o parcelamento quando tal medida implicar na sua desnaturação, onde tem risco a satisfação do interesse público em questão. Já a viabilidade econômica significa que o parcelamento deve trazer benefícios para a Administração licitante, proporcionando um aumento da competitividade e uma consequente diminuição dos custos para a execução do objeto. No entanto, para uma real noção da viabilidade econômica do parcelamento, é preciso ter em mente a redução de custos proporcionada pela economia de escala*".

Sobre o tema, vale ainda citar a obra “Temas Polêmicos sobre Licitações e Contratos”, vários autores, da editora Malheiros, na página 74, o seguinte trecho: *“(...) em geral, a economia de escala é instrumento fundamental para diminuição de custos. Quanto maior a quantidade a ser negociada, menor o custo unitário, que em decorrência do barateamento do custo da produção (economia de escala na indústria), quer porque há diminuição da margem de lucro (economia de escala geralmente encontrada no comércio)*”.

O agrupamento em questão, software de antivírus endpoint com serviço de detecção e resposta de incidentes (item 1), suporte técnico com garantia (item 2) e horas técnicas para configuração da solução (item 3) é tecnicamente indispensável para se manter a uniformidade do fornecimento, pois todos os elementos do lote possuem correlação técnica entre si, uma vez que cada item é complemento dos demais.

Tal premissa encontra guarita ainda em deliberações do TCU sobre a matéria, tais como a decisão que: "*A aquisição de itens diversos em lotes deve estar respaldada em critérios justificantes*", adotando o entendimento do Acórdão 5260/2011, de 06/07/2011, que decidiu que "*Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si* ".

No presente caso, os itens são de mesma natureza, já que se tratam de solução de antivírus endpoint, guardando correlação entre si, pois tem-se o suporte de tais licenças, assim como o serviço de configuração da nova funcionalidade.

Assim posto, o agrupamento dos itens em lote levou em consideração questões técnicas, bem como o ganho de economia em escala, sem prejuízo a ampla competividade, uma vez que existe no mercado várias empresas com capacidade de fornecer os produtos e serviços na forma em que estão agrupados neste estudo - Anexo A. No que toca a tecnologia empregada nos itens do lote, todos guardam correlação entre si quando aplicados neste projeto.

Aliado a isso, deriva do não parcelamento da solução a sua forma de adjudicação, a qual deverá se dar a uma empresa, devido ao fato da contratação versar sobre a renovação de licenças da marca Kaspersky já existentes e instaladas no parque computacional do PJMT, com seu devido aprimoramento (item 1).

Entende-se que o serviço de suporte técnico Kaspesky, monitoramento e notificação do serviço (item 2), assim como a configuração da nova funcionalidade (item 3) deve ser feito pela mesma empresa que fornece as licenças, visto que não existe possibilidade comercial de uma empresa fornecer os softwares e licenças necessárias, e outra empresa fazer o serviço de manutenção e monitoramento ou configuração destas licenças e do ambiente computacional.

Caso o objeto fosse parcelado, empresas distintas poderiam ser responsáveis pela prestação dos mesmos serviços supracitados, ou seja, fornecimento de licenças, suporte técnico e configuração, e isso poderia acarretar em grandes dificuldades a Administração, pois, mais de uma empresa prestaria serviços correlatos simultaneamente, o que poderia causar conflitos de procedimentos e responsabilidades. Isso dificultaria a aplicação de penalidades aos contratados devido a extrema dificuldade em separar as responsabilidades de cada empresa Contratada, caso fosse necessário, acarretando queda na qualidade dos serviços prestados e em consequentes prejuízos na segurança da informação para o TJMT.

Outro empecilho técnico está na possibilidade da não adjudicação de um dos itens licitados, ou até mesmo de atraso da entrega dos serviços descritos no item 1, por exemplo. A empresa sagrada vencedora do item 2 (suporte técnico) ficaria impossibilitada de prestar seus serviços adequadamente, não podendo ser penalizada pela incapacidade de outra. Isto prejudicaria o Poder Judiciário de Mato Grosso que não teria nenhum dos serviços prestados, sem a possibilidade de sanar os impedimentos através dos procedimentos administrativos adequados.

Some-se a isso a possibilidade de estabelecimento de um padrão de qualidade e eficiência que pode ser acompanhado ao longo da garantia, o que fica sobremaneira dificultado quando se trata de diversos fornecedores.

Assim posto, resta claro que o agrupamento destes itens em lote, na forma como foram expressos nesta presente demanda, não é opcional, mas sim, estritamente necessário, não cabendo, assim, o fornecimento de outra forma, que a apresentada neste documento.

Diante de objetos complexos, distintos ou divisíveis cabe, como regra e conforme o caso concreto justificar, a realização de licitação por itens ou lotes, que está prevista no art. 23, §1º, da Lei n.º 8.666/931, de modo a majorar a competitividade do certame.

Portanto, a adjudicação se dará por menor preço global do lote, previamente ao menor preço individual de cada item, e modo de disputa aberto e fechado.

### Subcontratação

Não será permitida a subcontratação.

Deve-se reconhecer que, em uma abordagem conceitual rigorosa, dificilmente existiria uma situação em que a totalidade absoluta da prestação de serviços / fornecimento de produtos possa ser executada por uma única empresa sem recorrer a terceiros em nenhuma de suas etapas: transporte, fabricação de componentes etc.

Cabe frisar que o serviço de garantia técnica deverá ser prestado por profissionais da própria Contratada ou da Fabricante da solução, com atendimento aos requisitos constantes neste instrumento.

Para efeito deste projeto, não será adotada esta abordagem conceitual rigorosa, bastando a prestação de serviços direta ao PJMT (instalação, configuração, manutenção e demais suportes técnicos), ainda que necessite recorrer a terceiros para obter os insumos necessários. Além disso, não há como permitir a transferência da obrigação contratual à terceiro, pois se assim fosse, estar-se-ia, in casu, admitindo a execução do núcleo do objeto contratado, culminando na subcontratação total, vedada pelo TCU.

### Do consórcio

A divisão da solução não é tecnicamente viável e existem fornecedores para toda ela, não sendo necessário, portanto, a aceitação da participação de consórcios.

### Da amostra

Para a contratação ora pretendida, não será necessária amostra da solução.

## Modalidade e Tipo de Licitação (Art. 16, IV)

A contratação da solução ora pretendida é oferecida por diversos fornecedores no mercado de TIC, vez que apresenta características padronizadas e usuais. Assim, trata-se de serviço comum e, portanto, licitação via Pregão, em sua forma eletrônica, pelo tipo menor preço global do lote - previamente ao menor preço individual de cada item - e modo de disputa aberto e fechado.

### Não aplicação da Lei Complementar 123/2006, alterada pela Lei Complementar n. 147/2014

Nos termos do art. 48, III da Lei Complementar n. 123, de 2006 (atualizada pela LC n. 147/2014), a Administração deverá estabelecer, em certames para aquisição de bens de natureza divisível, cota de até 25% (vinte e cinco por cento) do objeto para a contratação de microempresas e empresas de pequeno porte. Por essa razão, parcela de até 25% (vinte e cinco por cento) dos quantitativos divisíveis deverão ser destinados exclusivamente a ME/EPP/COOP beneficiadas pela LC n. 123/2006. Essas “cotas reservadas” deverão ser definidas em função de cada item separadamente ou, nas licitações por preço global, em função do valor estimado para o grupo ou o lote da licitação que deve ser considerado como um único item (art. 9º, inciso I do Decreto n. 8.538, de 2015).

In casu, a licitação que se pretende deverá ocorrer pelo menor preço individual de cada item do lote. Contudo, todos os itens se tratam de licenciamento e serviços em sua totalidade, sendo 03 (três) itens, não havendo, desta forma, como fazê-lo divisível sem desnaturá-lo.

Para tanto, o art. 10, incisos I, II e IV do Decreto nº 8.538, de 2015 excepciona algumas hipóteses, quais sejam: I - não houver o mínimo de três fornecedores competitivos enquadrados como microempresas [...] capazes de cumprir as exigências estabelecidas no instrumento convocatório; II - o tratamento diferenciado e simplificado para as microempresas e as empresas de pequeno porte não for vantajoso para a administração pública ou representar prejuízo ao conjunto ou complexo do objeto a ser contratado, justificadamente; (...) IV - o tratamento diferenciado e simplificado não for capaz de alcançar, justificadamente, pelo menos um dos objetivos previstos no art. 1º. (grifo nosso).

No caso aqui exposto, com toda a contextualização elaborada até então, fica evidente de que o inciso II se amolda à situação ora posta, já que se trata de serviços não divisíveis, pela necessidade de gerenciamento unificado de todas as licenças que compõe a solução uma, não caberia particionar a entrega de seus itens entre fornecedores distintos.

Considera-se “não vantajosa a contratação” quando: II - a natureza do bem, serviço ou obra for incompatível com a aplicação do benefício (Decreto nº 8.538, de 2015, art. 10, parágrafo único). (grifo nosso)

A mesma premissa apresentada no grifo anterior justifica a incompatibilidade com a aplicação do benefício aqui tratado.

Diante do explanado, conclui-se que não há óbice quanto à aplicação da Lei Complementar 123/2006. Entretanto não é possível a divisão ou fragmentação dos itens em partes e nem aplicação do benefício da exclusividade para que ocorra a participação para ME/EPP, ante a impossibilidade da divisão técnica, conforme explanação apresentada no item 3.2 deste Estudo Preliminar.

## Classificação e Indicação Orçamentária (Art. 16, V)

* Unidade Orçamentária – UO: 03. 601 – Funajuris
* Programa: 036/ Apoio Administrativo
* Ação (P/A/OE) 2009 – Manutenção de Ações Informática
* Unidade Gestora – UG: 0002
* Fonte: 240/640
* Natureza 3.3.90.40/4.4.90.40.

## Vigência do Contrato (Art. 16, VI)

A vigência do Contrato será de 24 (vinte e quatro) meses para os itens 1 a 3, podendo ser prorrogado até o limite dos 48 (quarenta e oito) meses, nos termos do art. 57, inc. II, da Lei 8.666/93.

A prestação dos serviços se dará da seguinte maneira:

* Será necessária lavratura de contrato, com indicação dos *part numbers* dos produtos.
* A data de início do Contrato ocorrerá quando da assinatura de ambas as partes, a qual será objeto de Certidão aposta pela Coordenadoria Administrativa – Departamento Administrativo nos autos.
* A vigência do contrato referente aos serviços dos Itens 1 e 2 poderão ser prorrogados/renovados.
* A escolha do prazo de 24 (vinte e quatro) meses de vigência baseia-se na continuidade do licenciamento e serviços em execução, sendo contínuos e essenciais, garantindo a integridade, confidencialidade e segurança das informações institucionais contra as ações de softwares mal intencionados que ponham em risco a segurança e a continuidade das atividades organizacionais
* Além disso, no custo administrativo de um processo licitatório, já que quanto maior o número de procedimentos, maior o gasto da administração, considerando contratações de serviços continuados, como o que aqui se trata.
* O prazo dilatado permitirá obtenção de ganho de escala e consequentemente melhores preços para a Administração;
* Ademais, é maior a atratividade do certame pelo mercado, por meio de uma maior diluição dos custos por durante o lapso temporal do contrato, favorecendo a Administração em termos de economicidade e ampliação da competitividade;
* Seguindo esta lógica, a jurisprudência do Tribunal de Contas da União sustenta a possibilidade da fixação do prazo de vigência estendido com a finalidade de obter preços e condições mais vantajosos para a Administração, (Acórdão 3.320/2013-Segunda Câmara):

*“O prazo de vigência de contratos de serviços contínuos deve ser estabelecido considerando-se as circunstâncias de forma objetiva, fazendo-se registrar no processo próprio o modo como interferem na decisão e quais suas consequências. Tal registro é especialmente importante quando se fizer necessário prazo inicial superior aos doze meses entendidos como regra pelo TCU. Há necessidade de se demonstrar o benefício decorrente do prazo estabelecido (Acórdão 3320/2013-Segunda Câmara).”*

* Um prazo contratual exíguo implicaria na constante dedicação de recursos humanos especificamente para processos de Planejamento da Contratação, considerando que os trabalhos de renovação/prorrogação são deflagrados com pelo menos 180 dias de antecedência (em atendimento à recomendação do Tribunal de Contas da União esposada no Acórdão nº 728/2008 – 1ª Câmara).

## Equipe de Apoio e Gestão à Contratação (Art. 16, VII)

Para a composição da Equipe de Apoio e Gestão da Contratação, foram feitas as seguintes indicações:

**Indicação do Fiscal / Integrante demandante (art. 12, §5º, inciso III da Resolução 182/CNJ)**

|  |  |
| --- | --- |
| Nome | Benedito Pedro da Cunha Alexandre |
| Matrícula | 6590 |
| E-Mail | [benedito.alexandre@tjmt.jus.br](mailto:benedito.alexandre@tjmt.jus.br) |
| Área (Departamento/Setor) | Departamento de Conectividade |

**Indicação do Fiscal / Integrante demandante substituto (art. 12, §5º, inciso III da Resolução 182/CNJ)**

|  |  |
| --- | --- |
| Nome | Danyllo Carvalho Lopes Barrozo |
| Matrícula | 25926 |
| E-Mail | [danyllo.carvalho@tjmt.jus.br](mailto:danyllo.carvalho@tjmt.jus.br) |
| Área (Departamento/Setor) | Departamento de Conectividade |

**Indicação do Fiscal / Integrante técnico (art. 12, §6º, da Resolução 182/CNJ)**

|  |  |
| --- | --- |
| Nome | Danyllo Carvalho Lopes Barrozo |
| Matrícula | 25926 |
| E-Mail | [danyllo.carvalho@tjmt.jus.br](mailto:danyllo.carvalho@tjmt.jus.br) |
| Área (Departamento/Setor) | Departamento de Conectividade |

**Indicação do Fiscal / Integrante técnico substituto (art. 12, §6º, da Resolução 182/CNJ)**

|  |  |
| --- | --- |
| Nome | Marcelo Monteiro de Moraes |
| Matrícula | 9838 |
| E-Mail | [marcelo.moraes@tjmt.jus.br](mailto:marcelo.moraes@tjmt.jus.br) |
| Área (Departamento/Setor) | Departamento de Conectividade |

**Indicação do Fiscal / Integrante administrativo (art. 12, §7º, da Resolução 182/CNJ)**

|  |  |
| --- | --- |
| Nome | Marco Antonio Molina Parada |
| Matrícula | 5548 |
| E-Mail | [marco.parada@tjmt.jus.br](mailto:marco.parada@tjmt.jus.br) |
| Área (Departamento/Setor) | Coordenadoria Administrativa |

**Indicação do Fiscal / Integrante administrativo substituto (art. 12, §7º, da Resolução 182/CNJ)**

|  |  |
| --- | --- |
| Nome | Evandro Trindade do Amaral |
| Matrícula | 43642 |
| E-Mail | Evandro.amaral@tjmt.jus.br |
| Área (Departamento/Setor) | Coordenadoria Administrativa |

# ANÁLISE DE RISCOS

Considerando especialmente a situação atual do projeto de Contratação de Solução de Antivírus já detalhado neste documento, os seguintes riscos foram identificados:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **REFERENTE À FASE**  **( x ) Planejamento de Contratação e Seleção do fornecedor ( ) Execução contratual** | | | | |
| **Risco 01** | | Definição do objeto da contratação sem o devido aprofundamento técnico nos Estudos Preliminares | | Grau do risco  (MÉDIO) |
| Probabilidade | | ( x ) Baixa ( ) média ( ) alta | | |
| Impacto | | ( ) Baixo ( ) médio ( x ) alto | | |
| **Id.** | **Dano** | | | |
| 1 | Contratação de solução aquém das necessidades do PJMT; | | | |
| 2 | Possível impugnação do processo licitatório; | | | |
|  | **Ação Preventiva** | | **Responsável** | |
| 1 | Fazer análise de todas as possíveis soluções técnicas com possibilidade de atender a demanda do PJMT. | | Fiscal / Integrante Técnico. | |
| 2 | Fazer estudo com base em contratações públicas similares e os requisitos de negócio do PJMT. | | Equipe de Planejamento. | |
| 3 | Definir objeto da contratação com o máximo de informações disponíveis, alinhado às necessidades da área demandante. | | Equipe de Planejamento. | |
| 4 | Embasar o estudo técnico da definição do objeto em manuais e consultoria de empresa especializada (Gartner). | | Equipe de Planejamento. | |
|  | **Ação de Contingência** | | **Responsável** | |
| 1 | Rever análise técnica do objeto da contratação, considerando apontamentos de impugnações. | | Fiscal / Integrante Técnico. | |
| 2 | Em caso de solução insuficiente, iniciar processo de nova contratação. | | Fiscal / Integrante Demandante. | |
| 3 | Medidas administrativas cabíveis quanto à contratação já efetivada. | | Fiscal / Integrante Administrativo. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **REFERENTE À FASE**  **( x) Planejamento de Contratação e Seleção do Fornecedor ( ) Gestão do Contrato** | | | | |
| **Risco 02** | | Impugnação em virtude de apontamento de marca. | | Grau do risco  (MÉDIO) |
| Probabilidade | | ( x ) Baixa ( ) Média ( ) Alta | | |
| Impacto | | ( ) Baixo ( ) Média ( x ) Alta | | |
| **Id.** | **Dano** | | | |
| 1 | Não cumprimento dos prazos estabelecidos inicialmente no projeto, podendo afetar o pleno funcionamento dos serviços aqui elencados. | | | |
|  | **Ação Preventiva** | | **Responsável** | |
| 1 | Realizar extensa pesquisa de mercado em busca das opções disponíveis, principalmente em virtude de se tratar de solução composta por serviços interdependentes. | | Equipe de Planejamento. | |
| 2 | Utilizar consultoria especializada para fundamentação da escolha (Gartner). | | Equipe de Planejamento. | |
| 3 | Justificar apontamento de marca com base em condições financeiras (investimento prévio na solução atual, além do impacto funcional à prestação dos serviços jurisdicionais em eventual troca de solução). | | Equipe de Planejamento. | |
|  | **Ação de Contingência** | | **Responsável** | |
| 1 | Alocar integralmente os servidores responsáveis e que confeccionaram o TR, para dar respostas e, consequentemente, mitigar as causas que originaram a suspensão do processo licitatório. | | Fiscais / Integrantes Demandantes e Técnicos. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **REFERENTE À FASE**  **( x) Planejamento de Contratação e Seleção do Fornecedor ( ) Gestão do Contrato** | | | | |
| **Risco 03** | | Atraso ou suspensão do processo licitatório em face de impugnações. | | Grau do risco  (MÉDIO) |
| Probabilidade | | ( x ) Baixa ( ) Média ( ) Alta | | |
| Impacto | | ( ) Baixo ( ) Média ( x ) Alta | | |
| **Id.** | **Dano** | | | |
| 1 | Não cumprimento dos prazos estabelecidos inicialmente no projeto, podendo afetar o pleno funcionamento dos serviços aqui elencados. | | | |
|  | **Ação Preventiva** | | **Responsável** | |
| 1 | Elaborar o planejamento da contratação considerando soluções similares em outros órgãos. | | Equipe de Planejamento. | |
| 2 | Estabelecer contato prévio com o fabricante da solução de modo a alinhar os requisitos de negócio do PJMT com as especificações técnicas mais aderentes no mercado. | | Equipe de Planejamento. | |
| 3 | Justificar indicação de marca da solução, com todo embasamento técnico e econômico do projeto de contratação. | | Fiscal / Integrante Técnico. | |
|  | **Ação de Contingência** | | **Responsável** | |
| 1 | Alocar integralmente os servidores responsáveis e que elaboraram o planejamento da contratação, para dar respostas e, consequentemente, mitigar as causas que originaram a suspensão do processo licitatório. | | Fiscais / Integrantes Demandantes e Técnicos. | |
| **REFERENTE À FASE**  **( x) Planejamento de Contratação e Seleção do Fornecedor ( ) Gestão do Contrato** | | | | |
| **Risco 04** | | Orçamento da contratação mal estimado | | Grau do risco  (MÉDIO) |
| Probabilidade | | ( x ) Baixa ( ) Média ( ) Alta | | |
| Impacto | | ( ) Baixo ( ) Média ( x ) Alta | | |
| **Id.** | **Dano** | | | |
| 1 | Encerrar a licitação com valores inexequíveis, impedindo a adjudicação do processo. | | | |
| 2 | Licitação Deserta. | | | |
| 3 | Contratação de solução com valores acima do mercado / Sofrer sanções por parte de órgãos fiscalizadores. | | | |
|  | **Ação Preventiva** | | **Responsável** | |
| 1 | Realizar pesquisa de preço envolvendo todos os participantes de mercado. | | Equipe de Planejamento. | |
| 2 | Utilizar ferramentas de pesquisa de preço público (painel de preços). | | Equipe de Planejamento. | |
| 3 | Especificar o objeto na pesquisa de preço de forma adequada, conforme especificação da solução pretendida na contratação. | | Equipe de Planejamento. | |
|  | **Ação de Contingência** | | **Responsável** | |
| 1 | Em caso de suspensão por preço inexequível, realizar pesquisa de preço adequada, para nova publicação de edital. | | Equipe de Planejamento | |
| 2 | Em caso de valores acima do mercado, negociar com a empresa. | | Pregoeiro | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **REFERENTE À FASE**  **( x) Planejamento de Contratação e Seleção do Fornecedor ( ) Gestão do Contrato** | | | | |
| **Risco 05** | | Redução ou corte no orçamento. | | Grau do risco  (MÉDIO) |
| Probabilidade | | ( ) Baixa ( x ) Média ( ) Alta | | |
| Impacto | | ( ) Baixo ( ) Média ( x ) Alta | | |
| **Id.** | **Dano** | | | |
| 1 | Exposição dos ativos computacionais aos riscos de segurança de informação, afetando diretamente a prestação de serviços por falta de atualização e suporte técnico da solução. | | | |
| 2 | O volume orçamentário sofrer redução e a contratação ser executada num patamar financeiro inferior ao necessário para atender todas as demandas do PJMT ou, na pior das hipóteses, não ocorrer a contratação. | | | |
|  | **Ação Preventiva** | | **Responsável** | |
| 1 | Negociação do Comitê Gestor de TIC com a Presidência no tocante a defesa da aprovação integral do orçamento proposto pela CTI para a nova contratação. | | Equipe de Planejamento e Comitê Gestor de TIC. | |
|  | **Ação de Contingência** | | **Responsável** | |
| 1 | Priorização da demanda junto aos gestores das áreas de negócio, para tentar intermediar a não redução. | | Fiscais / Integrantes Demandantes e Técnicos. | |
| 2 | Necessidade de replanejamento da contratação e sua respectiva readequação frente ao serviço que não será contratado. | | Fiscais / Integrantes Demandantes e Técnicos e Comitê Gestor de TIC. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **REFERENTE À FASE**  **( ) Planejamento de Contratação e Seleção do Fornecedor ( x ) Gestão do Contrato** | | | | |
| **Risco 06** | | Contratada ficar impossibilitada de prestar os serviços contratados devido a não manutenção das condições habilitatórias. | | Grau do risco  (MÉDIO) |
| Probabilidade | | ( x ) Baixa ( ) Média ( ) Alta | | |
| Impacto | | ( ) Baixa ( ) Média ( x) Alto | | |
| **Id.** | **Dano** | | | |
| 1 | Os serviços elencados neste projeto ficarem sem atualizações e suporte técnico. | | | |
| 2 | Alto risco de sistemas críticos do PJMT cessarem funcionamento, em caso de intrusões não defendidas. | | | |
|  | **Ação Preventiva** | | **Responsável** | |
| 1 | Estudo de mercado quanto à qualificação da empresa a ser contratada. | | Equipe de Planejamento | |
| 2 | Exigir documentação fiscal e econômica que respalde a saúde financeira da empresa a ser contratada. | | Equipe de Planejamento. | |
|  | **Ação de Contingência** | | **Responsável** | |
| 1 | Sugerir aplicação de todas as sanções previstas em contrato. | | Fiscal / Integrante  Técnico. | |
| 2 | Iniciar processo de contratação emergencial para contratação de nova empresa para prestação dos serviços. | | Fiscal / Integrante Demandante. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **REFERENTE À FASE**  **( ) Planejamento de Contratação e Seleção do Fornecedor ( x ) Gestão do Contrato** | | | | |
| **Risco 07** | | Necessidade de ajustes no quantitativo de licenças durante a vigência do contrato. | | Grau do risco  (BAIXO) |
| Probabilidade | | ( x ) Baixa ( ) Média ( ) Alta | | |
| Impacto | | ( ) Baixa ( x) Média ( ) Alta | | |
| **Id.** | **Dano** | | | |
| 1 | Capacidade de atendimento às demandas impactando, afetando qualidade do serviço prestado. | | | |
|  | **Ação Preventiva** | | **Responsável** | |
| 1 | Avaliação criteriosa no quantitativo da demanda apresentada, com base na previsão de acréscimo ou decréscimo de pessoal, infraestrutura ou aplicações de TIC. | | Equipe de Planejamento | |
|  | **Ação de Contingência** | | **Responsável** | |
| 1 | Aditivo contratual limitado a 25%, conforme art. 65 § 1º da Lei 8.666/93, para os itens que permitam tal procedimento. | | Fiscal / Integrante Técnico. | |
| 2 | Priorizar utilização de licenças na missão crítica, de modo a minimizar o impacto, até que se realize nova contratação. | | Fiscal / Integrante Técnico. | |
| 3 | Iniciar estudos para nova contratação. | | Fiscais / Integrantes Demandantes e Técnicos | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **REFERENTE À FASE**  **( ) Planejamento de Contratação e Seleção do Fornecedor ( x ) Gestão do Contrato** | | | | |
| **Risco 08** | | Serviço de suporte técnico não satisfatório com relação ao Nível Mínimo de Serviço estabelecido. | | Grau do risco  (MÉDIO) |
| Probabilidade | | ( ) Baixa ( x ) Média ( ) Alta | | |
| Impacto | | ( ) Baixa ( ) Média ( x) Alta | | |
| **Id.** | **Dano** | | | |
| 1 | Degradação da qualidade dos serviços de suporte de antivírus por falta de suporte técnico adequado. | | | |
|  | **Ação Preventiva** | | **Responsável** | |
| 1 | Estipular cláusulas de acordo de nível mínimo de serviço com respectivas glosas, no caso de descumprimento. | | Equipe de Planejamento. | |
| 2 | Exigência de qualificação técnica dos profissionais através de certificação junto à fabricante e demais emissores responsáveis. | | Equipe de Planejamento | |
| 3 | Não permitir o fechamento de chamados sem a verificação de que o atendimento foi devidamente realizado. | | Integrante técnico. | |
|  | **Ação de Contingência** | | **Responsável** | |
| 1 | Conferência mensal dos serviços que estão sendo prestados, e, em caso de descumprimento, encaminhar o envio da ocorrência à contratada, permitindo as respectivas justificativas e correções. | | Fiscal / Integrante técnico. | |
| 2 | Aplicar os descontos definidos no nível mínimo de serviço. | | Fiscal / Integrante técnico. | |
| 3 | Sugerir aplicação de sanções e penalidades previstas no contrato. | | Fiscal / Integrante técnico. | |
| 4 | Verificar o interesse e conveniência na rescisão contratual. | | Equipe de Planejamento/ Área Demandante. | |

# Anexo A

LISTA DOS PRINCIPAIS FORNECEDORES

CONTRATAÇÃO DE SOLUÇÃO DE ANTIVÍRUS ENDPOINT

|  | **Fornecedor** |
| --- | --- |
| **1** | **Nome: NLIT**  **Sítio:** https://www.n1it.com.br/  **Telefone: (11) 2921-9100**  **E-mail: comercial@n1it.com.br**  **Contato:**  **Cidade:** São Paulo, SP |
| **2** | **Nome: Partner One**  **Sítio:** https://www.partnerone.com.br/  **Telefone: (11)5694-2200**  **E-mail: contato@partnerone.com.br**  **Contato:**  **Cidade:** São Paulo, SP |
| **3** | **Nome: Solo Network**  **Sítio:** https://www.solonetwork.com.br/  **Telefone: (61) 4062-6971**  **E-mail: adriana.lima@solonetwork.com.br**  **Contato: Adriana de Paula Lima**  **Cidade:** Brasília - DF |
| **4** | **Nome: Focal Data**  **Sítio:** https://www.focaldata.com.br/  **Telefone: (61) 98407-7673**  **E-mail: claudio.henrique@focaldata.com.br**  **Contato: Claudio Henrique Castelo Branco**  **Cidade:** Brasília - DF |
| **5** | **Nome: Alus**  **Sítio:** https://alus.com.br/  **Telefone: 11 3256-4433**  **E-mail: alus@alus.com.br**  **Contato: Daniele Mariano**  **Cidade:** São Paulo, SP |
| **6** | **Nome: DMK3**  **Sítio:** https://dmk3.com.br/  **Telefone: (11) 4117-0046**  **E-mail: contato@dmk3.com.br**  **Contato:**  **Cidade:** São Paulo, SP |
| **7** | **Nome: Brasoftware**  **Sítio:** https://www.brasoftware.com.br/  **Telefone: 11 3179 6900**  **E-mail: brasoftware@brasoftware.com.br**  **Contato:**  **Cidade:** São Paulo, SP |
| **8** | **Nome: Fortsecure**  **Sítio:** https://www.fortsecure.com.br/  **Telefone: (11) 3230-0106**  **E-mail: comercial@fortsecure.com.br**  **Contato:**  **Cidade:** Ribeirão Preto, SP |
| **9** | **Nome:**  **Sítio:** https://ish.com.br/  **Telefone: (61) 3029-8666**  **E-mail: comercial.df@ish.com.br**  **Contato:**  **Cidade:** Brasília, DF |
| **10** | **Nome:**  **Sítio:** http://kscorp.com.br/  **Telefone: (51) 3024-3131**  **E-mail: contato@kscorp.com.br**  **Contato:**  **Cidade:** Porto Alegre, RS |
| **11** | **Nome: Fast Help**  **Sítio:** https://www.fasthelp.com.br/  **Telefone: (61) 3363-8636**  **E-mail: Priscila.machado@fasthelp.com.br**  **Contato: Priscila Machado**  **Cidade:** Brasília - DF |
| **12** | **Nome: Microhard**  **Sítio:** https://microhard.com.br/  **Telefone: (31) 32815522**  **E-mail: vendas@microhard.com.br**  **Contato: Edillon Pinheiro**  **Cidade:** Belo Horizonte, MG |
| **13** | **Nome:**  **Sítio:** https://www.4fti.com.br/  **Telefone: (61) 3037-2006**  **E-mail: comercial@4fti.com.br**  **Contato:**  **Cidade:** Brasília, DF |
| **14** | **Nome:**  **Sítio:** https://www.softwareone.com/  **Telefone: (11) 3796-5020**  **E-mail: marketing.br@softwareone.com**  **Contato:**  **Cidade:** São Paulo, SP |
| **15** | **Nome:**  **Sítio:** https://www.grupoimagetech.com.br/  **Telefone: (67) 3357-0700**  **E-mail: relacionamento@grupoimagetech.com.br**  **Contato:**  **Cidade:** Campo Grande, MS |

Ressalta-se que a listagem de fornecedores é meramente exemplificativa.

# Anexo B

Contratações Públicas Similares

CONTRATAÇÃO DE SOLUÇÃO DE ANTIVÍRUS ENDPOINT

1. **JUSTIÇA FEDERAL DE PRIMEIRO GRAU NO CEARÁ**

Texto, Carta

Descrição gerada automaticamenteTexto, Carta

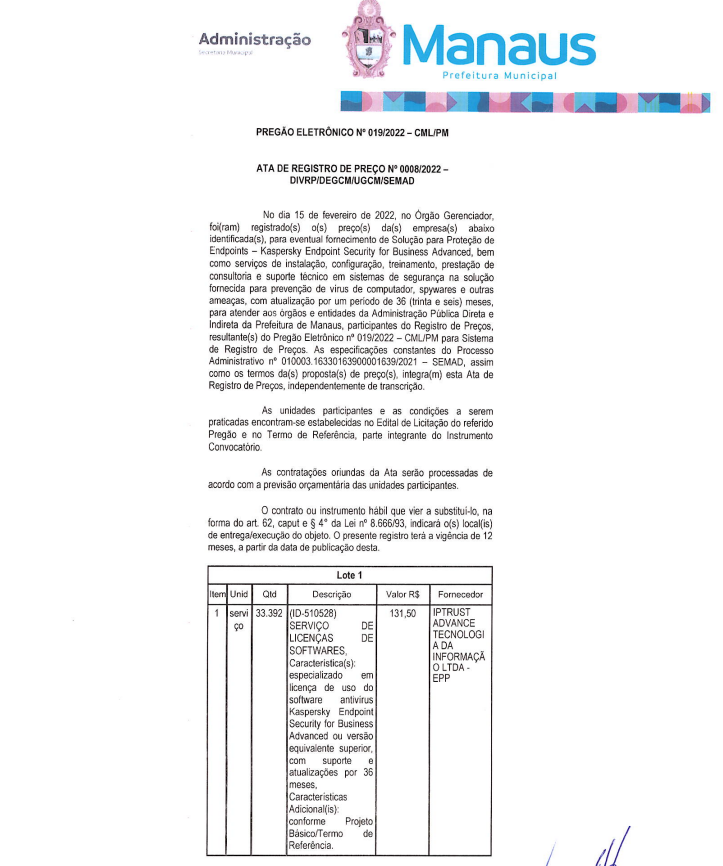
Descrição gerada automaticamente

1. **SUPERIOR TRIBUNAL MILITAR**

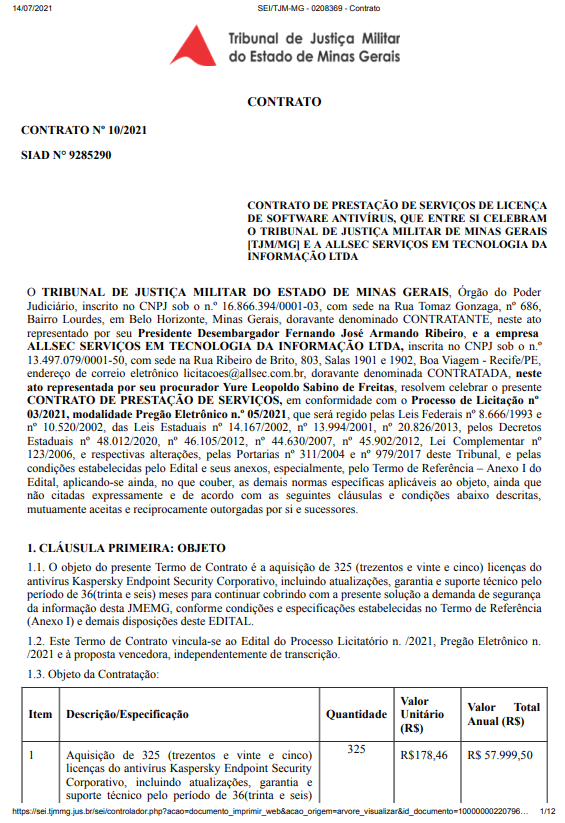
Texto, Carta

Descrição gerada automaticamente

1. **PREFEITURA DE MANAUS**



1. **TRIBUNAL DE JUSTIÇA MILITAR DO ESTADO DE MINAS GERAIS**



1. **SECRETARIA DE FAZENDA DO ESTADO DO CEARÁ**

**Texto

Descrição gerada automaticamente**

1. **UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL**

**Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente**

# Anexo C

ORÇAMENTOS

CONTRATAÇÃO DE SOLUÇÃO DE ANTIVÍRUS ENDPOINT

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Lote** | | **1** | | | | |
| **Item** | | **1** | **2** | | **3** | |
| **Descrição** | | **Renov. do licenc. de Kaspersky Endpoint Security – ADVANCED + Kaspersky Endpoint Detection and Response Optimun, 2 (dois) anos.** | **Manutenção, Suporte Técnico, Monitoramento e Notificação via SECaaS, pelo período de 2 (dois) anos.** | | **Horas Técnicas para implantação da solução.** | |
| **Quantidade** | | **10875** | **1** | | **650** | |
| **Tipo** | | **Serviço** | **Serviço** | | **Horas** | |
| **SOLO NETWORK** | Valor Unit. (R$) | R$ 182,22 | R$ 482.400,00 | | R$ 237,00 | |
| Valor Total (R$) | R$ 1.981.642,50 | R$ 482.400,00 | | R$ 154.050,00 | |
| PROPOSTA TOTAL | R$ 2.618.092,50 | | | | |
| **MICROHARD** | Valor Unit. (R$) | R$ 219,68 | R$ 579.000,00 | | R$ 285,45 | |
| Valor Total (R$) | R$ 2.389.020,00 | R$ 579.000,00 | | R$ 185.542,50 | |
| PROPOSTA TOTAL | R$ 3.153.562,50 | | | | |
| **FAST HELP** | Valor Unit. (R$) | R$ 225,00 | R$ 600.000,00 | | R$ 300,00 | |
| Valor Total (R$) | R$ 2.446.875,00 | R$ 600.000,00 | | R$ 195.000,00 | |
| PROPOSTA TOTAL | R$ 3.241.875,00 | | | | |
| **FOCAL DATA** | Valor Unit. (R$) | R$ 235,00 | | R$ 580.000,00 | | R$ 290,00 |
| Valor Total (R$) | R$ 2.555.625,00 | | R$ 580.000,00 | | R$ 188.500,00 |
| PROPOSTA TOTAL | R$ 3.324.125,00 | | | | |
| **MÉDIA** | Valor Unit. (R$) | R$ 215,48 | | R$ 560.350,00 | | R$ 278,11 |
| Valor Total (R$) | R$ 2.343.290,63 | | R$ 560.350,00 | | R$ 180.773,13 |
| PROPOSTA TOTAL | R$ 3.084.413,75 | | | | |
| **MEDIANA** | Valor Unit. (R$) | R$ 222,34 | | R$ 579.500,00 | | R$ 287,73 |
| Valor Total (R$) | R$ 2.417.947,50 | | R$ 579.500,00 | | R$ 187.021,25 |
| PROPOSTA TOTAL | R$ 3.184.468,75 | | | | |
| **MENOR PREÇO** | Valor Unit. (R$) | R$ 182,22 | | R$ 482.400,00 | | R$ 237,00 |
| Valor Total (R$) | R$ 1.981.642,50 | | R$ 482.400,00 | | R$ 154.050,00 |
| PROPOSTA TOTAL | R$ 2.618.092,50 | | | | |

|  |
| --- |
| **RADAR ELETRÔNICO TCE / MT:** Em pesquisa realizada no portal Radar Eletrônico do Tribunal de Contas do Estado de Mato Grosso, não foram identificadas contratações com objeto condizente aos itens aqui relacionados. Apesar da existência de 10 (dez) registros com a marca Kaspersky (conforme imagem abaixo), não se trata de serviço similar à especificação técnica da demanda deste Poder Judiciário (utilização da ferramenta Kaspersky Endpoint Detection and Response). Deste modo, não foi possível correlacionar valores públicos para comparação de preços nesta fonte. |
| **CATÁLOGO DE PREÇOS DA SECRETARIA DE GOVERNO DIGITAL:** Em pesquisa realizada no catálogo de Preços da Secretaria de Governo Digital, não foram identificadas contratações com objeto condizente aos itens aqui relacionados. Deste modo, não foi possível correlacionar valores públicos para comparação de preços nesta fonte. |
| **PREÇOS PÚBLICOS:** Em pesquisa realizada em ferramentas de pesquisa de preços públicos e na internet, não foram identificadas outras contratações com objeto condizente aos itens aqui relacionados, basicamente pela inclusão da solução Kaspersky Endpoint Detection and Response Standard. A mesma premissa é válida para comparação com o atual contrato deste Poder Judiciário (Contrato 15/2019). Portanto, não foi possível balizar o preço estimado desta contratação com outros preços públicos. |
| **ORÇAMENTOS PRIVADOS:** Inicialmente, foi encaminhada a primeira versão do pedido de orçamento para uma lista de empresas parceiras da fabricante Kaspersky, no dia 11/0/2022. Deste pedido, mediante considerações de fornecedores e da própria fabricante, foram feitos ajustes às especificações técnicas da solução, de modo a garantir uma contratação que suprisse, da melhor forma possível, a demanda e os requisitos técnicos do PJMT.  Desta forma, foi encaminhado no dia 15/03/2022 a versão final do pedido de orçamento para as empresas listadas no anexo A deste Estudo Preliminar, ação esta que resultou nas propostas das 4 (quatro) empresas listadas na tabela de orçamento acima. |
| **OUTROS ORÇAMENTOS:** Não foram encontrados outros orçamentos além dos já mencionados. |
| **METODOLOGIA MATEMÁTICA ADOTADA E JUSTIFICATIVA:** A metodologia adotada para composição de preço estimado da contratação foi o de **PREÇO MÉDIO**, tendo em vista que a variação é mínima quando comparado com valor mediano. Por outro lado, a metodologia de menor preço destoa em mais de 10% de redução, podendo colocar em risco a exequibilidade da solução, aumentando o risco de licitação fracassada. |

**Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente**

# Anexo d

DESCRITIVO TÉCNICO DA SOLUÇÃO

CONTRATAÇÃO DE SOLUÇÃO DE ANTIVÍRUS ENDPOINT

**ITEM 1**

Renovação do licenciamento de direitos de uso do software *Kaspersky Endpoint Security - ADVANCED*, com upgrade *Kaspersky Endpoint Detection and Response STANDARD*, pelo período de 2 (dois) anos.

A funcionalidade Kaspersky Endpoint Detection and Response STANDARD deverá:

* Prover a possibilidade de assinalar um evento para determinado usuário para verificação;
* Suportar arquivos no formato CEF para integração com SIEM;
* Mostrar alertas por importância;
* Mostrar alertas por vetor de ataques;
* Prover informações detalhadas mostradas nos alertas e eventos como, Host onde ocorreu, origem do ataque, destino do ataque, tamanho e hash do objeto, URL do ataque, nome da tecnologia responsável por identificar o ataque, informar se o ataque possui características baseado no YARA (Ferramenta Open Source) para uso no projeto do Plano de Trabalho 2022/2023;
* Possuir capacidade de disponibilizar facilmente as amostras dos arquivos suspeitos detectados e do arquivo PCAP do contexto de captura;
* Ser compatível com Windows Client, Windows Server e Linux;
* Garantir que as detecções por indicadores de ataque (IoA’s) façam referência ao framework MITRE ATT&CK e Capacidade de correlacionar os eventos recebidos com indicadores de ataque (IoA’s), através de modelos criados pelo fabricante;
* Detectar elevação de privilégio;
* Permitir coletar informações forenses do endpoint como: dados, dumps de memória, estado do sistema operacional, processos iniciados, conexões estabelecidas, arquivos criados, registro modificado, tentativas de conexão com um host remoto, tentativa de login com sucesso, tentativa de login com falha;
* Utilizar um certificado para garantir segurança entre a comunicação entre o EDR e a Console de gerenciamento;
* Permitir criar regras de notificações para envio por e-mail quando novos eventos são identificados pela ferramenta;
* Ser capaz de executar tarefas para todo o ambiente e para dispositivos específicos, contendo no mínimo as capacidades, como: parar um processo, deletar um objeto, quarentenar um arquivo, recuperar um arquivo, prevenir a execução de um arquivo, executar um script, isolar o host completamente e de forma granular;
* Permitir integrar a solução com pelo menos as seguintes ferramentas de SIEM: ArchSight, Splunk e IBM Qradar.

**ITEM 2**

Suporte Técnico com garantia, monitoramento e Notificação via SECaaS, pelo período de 2 (dois) anos.

Este serviço deve contemplar tanto as funcionalidades adquiridas junto à fabricante para o pleno funcionamento da solução, quanto o serviço de suporte técnico da própria contratada, que será responsável direta pelo atendimento à equipe técnica do PJMT.

Para este documento, a definição de SECaaS é uma solução de serviço que alerta proativamente quando ocorrem incidentes de segurança. Essa solução SECURITY-as-a-Service deverá oferecer um método para detectar invasores em um estágio inicial e evitar que criminosos cibernéticos tenham acesso à rede ou aplicativos/softwares mal-intencionados, utilizando, mas não limitando a procura por comportamento suspeito durante as várias fases de um ataque.

O SECaaS deverá prover, minimamente:

1. Atualizações constantes de definições de malware que não dependem da conformidade do usuário;
2. Maior perícia em análises de segurança do parque tecnológico do Tribunal de Justiça de Mato Grosso;
3. Subsidiar com documentos/relatórios/análises a equipe técnica de forma a auxiliar na tomada de decisão;
4. O gerenciamento de logs;
5. Uma interface Web que permita a administração interna de tarefas, bem como visão do ambiente de segurança e das atividades em andamento.
6. A Manutenção e o suporte técnico remoto e/ou presencial (help desk) por parte da Proponente às dúvidas de utilização do software por parte do TJMT.
7. A Proponente junto com a equipe técnica do TJMT deverá montar um cronograma de implantação de todas as funcionalidades que a ferramenta oferece:
   1. A implantação das funcionalidades de gerenciamento de licenças, controle de admissão na rede, ferramenta de gestão de instalação de softwares, ferramenta de gestão de imagens/provisionamento, gerenciamento de correções e atualizações e a verificação de vulnerabilidades serão feitas, gradualmente pela equipe da Proponente, com acompanhamento do TJMT, devendo ao final de cada funcionalidade implementada ocorrer a transferência de conhecimento desta nova ferramenta.

**ITEM 3**

Apesar da solução Kaspersky Endpoint Security já estar instalada e configurada neste Poder Judiciário, se faz necessário a implementação da funcionalidade Kaspersky Endpoint Detection and Response Standard advinda do upgrade previsto no item 1 do objeto desta contratação.

Esta implementação deve ser realizada pelos profissionais da empresa contratada, podendo ter o apoio técnico da fabricante da solução.

Dentre as atividades, deve se prever desde o planejamento da implementação, o desenvolvimento – atualização, importação, instalação, update, customização, criação de alertas e configuração – tanto do security center quanto dos 10875 endpoints, estabilização, testes e repasse de conhecimento

# Anexo e

EVIDÊNCIA DE SOLICITAÇÃO DE PROPOSTA

CONTRATAÇÃO DE SOLUÇÃO DE ANTIVÍRUS ENDPOINT

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Interface gráfica do usuário, Aplicativo, Word

Descrição gerada automaticamente

Uma imagem contendo Texto

Descrição gerada automaticamente

1. JUSTEN FILHO, Marçal. Comentários a lei de licitações e contratos administrativos. 12a ed. São Paulo: Dialética, 2008, p. 146 [↑](#footnote-ref-2)