



**ESTADO DO RIO GRANDE DO SUL
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA MILITAR**

**EDITAL DE PREGÃO ELETRÔNICO Nº 002/2025
PROCESSO ADMINISTRATIVO Nº 9.2024.0700.000618-7
MENOR PREÇO**

CONTRATAÇÃO DE EMPRESA DO RAMO DE PRESTAÇÃO DE SERVIÇOS CONTÍNUOS SEM DEDICAÇÃO EXCLUSIVA DE MÃO DE OBRA REFERENTE A LICENÇAS DA SOLUÇÃO DE ANTIVÍRUS KASPERSKY ENDPOINT SECURITY COM UPGRADE DO LICENCIAMENTO KASPERSKY SELECT PARA A VERSÃO KASPERSKY ENDPOINT DETECTION AND RESPONSE OPTIMUM (EDR).

CRITÉRIO DE JULGAMENTO: MENOR PREÇO
VALOR ESTIMADO TOTAL DO LOTE : R\$ 89.881,21
Modo de disputa: Aberto

CONDIÇÕES GERAIS DE LICITAÇÃO - ÍNDICE

- 1. DO OBJETO**
- 2. DA DISPONIBILIZAÇÃO DO EDITAL**
- 3. DA DATA E DO HORÁRIO DA LICITAÇÃO**
- 4. DA PARTICIPAÇÃO**
- 5. DA PARTICIPAÇÃO DE MICROEMPRESAS E DE EMPRESAS DE PEQUENO PORTE**
- 6. DO CREDENCIAMENTO**
- 7. DA PROPOSTA DE PREÇOS**
- 8. DA SESSÃO PÚBLICA DE LICITAÇÃO**
- 9. DA REFERÊNCIA DE TEMPO**
- 10. DA ABERTURA DA PROPOSTA E DA ETAPA COMPETITIVA**
- 11. DA NEGOCIAÇÃO**
- 12. DA ACEITABILIDADE E DO JULGAMENTO DAS PROPOSTAS**
- 13. DA HABILITAÇÃO**
- 14. DOS PEDIDOS DE ESCLARECIMENTOS, IMPUGNAÇÕES E RECURSOS**
- 15. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO**
- 16. DO TERMO DE CONTRATO**
- 17. DO ACORDO DE NÍVEL DE SERVIÇO**
- 18. DO PAGAMENTO**
- 19. DO REAJUSTE**
- 20. DA FONTE DE RECURSOS**
- 21. DAS OBRIGAÇÕES DO ADJUDICATÁRIO**

22. DA GARANTIA DE EXECUÇÃO

23. DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

24. DAS DISPOSIÇÕES FINAIS

ANEXO I – MINUTA DE CONTRATO

ANEXO II – MODELO DE PROPOSTAS DE PREÇOS (preenchida pelo licitante vencedor)

ANEXO III – MODELO DE DECLARAÇÃO PARA HABILITAÇÃO

ANEXO IV – MODELO DE DECLARAÇÃO DE COMPOSIÇÃO SOCIETÁRIA E DE NEPOTISMO

ANEXO V – TERMO DE REFERÊNCIA

ANEXO VI - MODELO ANÁLISE CONTÁBIL DA CAPACIDADE FINANCEIRA DE LICITANTE

CONDIÇÕES GERAIS DE LICITAÇÃO – CGL SERVIÇOS CONTÍNUOS SEM DEDICAÇÃO EXCLUSIVA DE MÃO DE OBRA PREGÃO ELETRÔNICO 002/2025 - SEAORÇ-TJM/RS

O Tribunal de Justiça Militar do Estado do Rio Grande do Sul, torna público que realizará licitação, por meio da utilização de recursos de tecnologia da informática – INTERNET, na modalidade de PREGÃO ELETRÔNICO Nº 002/2025 - SEAORÇ-TJM/RS, do tipo **menor preço**, a Pregoeira designada pela Portaria nº 77/2024, publicado no Diário da Justiça Eletrônica – RS do dia 15 de Abril de 2024. A presente licitação reger-se-á pela Lei Federal nº 14.133, de 01 de abril de 2021; Lei Complementar Federal nº 123, de 14 de dezembro de 2006; Decreto-Lei nº 2.848, de 7 de dezembro de 1940; Lei nº 11.389, de 25 de novembro de 1999; Lei nº 13.706, de 6 de abril de 2011; Decreto nº 42.250, de 19 de maio de 2003; Decreto 48.160, de 14 de julho de 2011; Decreto nº 52.768, de 15 de dezembro de 2015; Decreto nº 55.717, de 12 de janeiro de 2021; Decreto Estadual nº 57.033, de 23 de maio de 2023, Decreto Estadual nº 57.037, de 23 de maio de 2023, Decreto Estadual nº 57.154 de 22 de agosto de 2023 e pelas condições previstas neste Edital e seus Anexos.

1. DO OBJETO

Lote 01- Contratação de prestação de serviços **contínuos sem dedicação exclusiva de mão de obra referente a** Contratação de empresa(s) especializada(s) para a renovação de licenças da solução de **antivírus Kaspersky Endpoint Security** com upgrade do licenciamento Kaspersky Select para a versão Kaspersky endpoint Detection and Response Optimun (EDR), conforme **prazo de vigência da contratação que será de 36 (trinta e seis) meses, contados a partir da emissão da ordem de fornecimento, podendo ser prorrogado sucessivamente, conforme os limites legais estabelecidos nos artigos 106 e 107 da Lei nº 14.133/2021.** Esta contratação inclui a atualização de versões e suporte técnico, visando atender às necessidades do Tribunal de Justiça Militar do Estado do Rio Grande do Sul (TJM/RS), da 1ª Auditoria Militar, da 2ª Auditoria Militar, da Auditoria Militar de Santa Maria/RS e da Auditoria Militar de Passo Fundo/RS e de acordo com as condições contidas no Termo de Referência (Anexo V) e Minuta de Contrato (Anexo I), partes deste Edital.

2. DA DISPONIBILIZAÇÃO DO EDITAL

2.1. O Edital poderá ser obtido no *site*:

Site: <https://pregaobanrisul.com.br/>

Pedidos de esclarecimentos e informações: servico-licitacao@tjmrs.jus.br

Impugnações e recursos: exclusivamente no sistema eletrônico www.pregaobanrisul.com.br

2.2. A licitação será realizada na forma eletrônica, por meio do endereço indicado no **subitem 2.1**, mediante condições de segurança, criptografia e autenticação.

3. DA DATA E DO HORÁRIO DA LICITAÇÃO

3.1. Na data e horário designados, será aberta sessão pública pelo pregoeiro:

Data: 26/03/2025

Horário: 14h00min

3.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação do pregoeiro em sentido contrário.

4. DA PARTICIPAÇÃO

4.1. Respeitadas as condições normativas próprias e as constantes deste Edital, poderá participar desta licitação:

4.1.1. qualquer pessoa jurídica legalmente estabelecida no País que esteja devidamente credenciada nos termos do **item 6** deste Edital, cujo objeto social seja compatível com o objeto da licitação e que atenda a todas as exigências estabelecidas neste Edital e seus Anexos, **observado a participação preferencial de microempresa e empresa de pequeno porte.**

4.1.2. pessoa física que esteja devidamente credenciada nos termos do **item 6** deste Edital.

4.1.3. não será permitida participação de Consórcio haja vista a baixa complexidade do objetivo que será fornecido em única vez no momento da sua contratação ou renovação, decisão pautada conforme orientação Acórdão 1946/2006 - TCU

4.1.4. Será permitida a participação de Cooperativa de Trabalho.

4.1.4.1. Para fins de habilitação, as Cooperativas de Trabalho deverão apresentar os seguintes documentos, em conjunto com aqueles previstos no subitem 13 deste Edital, no que couber:

a) ata de fundação;

b) estatuto social com a ata da assembleia que o aprovou devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede;

c) registro previsto no art. 107 da Lei 5.764/1971.

4.1.5. empresa estrangeira, desde que apresente Decreto de Autorização para funcionamento no país, e ato de registro ou autorização para funcionamento expedida pelo órgão competente, quando a atividade assim o exigir e, ainda, atenda às exigências de habilitação mediante documentos equivalentes, autenticados pelos respectivos consulados e traduzidos por Tradutor Público e Intérprete Comercial, devendo ter representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente.

4.2. Não poderão disputar licitação ou participar da execução de contrato, direta ou indiretamente:

4.2.1. a pessoa física ou jurídica que se encontre impossibilitada de contratar com o Poder Público em decorrência de sanção que lhe foi imposta;

4.2.2. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função no procedimento ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

4.2.3. as empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

4.2.4. a pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista.

4.3 O impedimento de que trata o **subitem 4.2.1** será também aplicado ao participante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

4.4 Em procedimentos e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei Federal nº 14.133/2021.

4.5. Não poderá haver nesta licitação participante com mais de uma proposta por lote.

5. DA PARTICIPAÇÃO DE MICROEMPRESAS E DE EMPRESAS DE PEQUENO PORTE

5.1. Para fins de obtenção do tratamento diferenciado de que tratam os artigos 42 a 49 da Lei Complementar federal nº 123/2006, quando do envio da proposta inicial, o participante deve declarar eletronicamente em campo próprio do sistema:

5.1.1. que possui enquadramento como Microempresa ou Empresa de Pequeno Porte;

5.1.2 que, no ano-calendário de realização desta licitação, ainda não tenha celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

5.2. A ausência dessas declarações, no momento do envio da proposta, significará a renúncia da microempresa ou da empresa de pequeno porte de utilizar-se das prerrogativas a ela concedida pela Lei Complementar federal nº 123/2006.

5.3. Consideram-se empatadas as propostas apresentadas pelas microempresas e empresas de pequeno porte que estiverem no limite de até 5% (cinco por cento) superiores à proposta mais bem classificada, desde que esta não seja de microempresa ou de empresa de pequeno porte.

5.4. Ocorrendo o empate, nos termos da Lei Complementar federal nº 123/2006, a microempresa ou a empresa de pequeno porte melhor classificada poderá apresentar proposta inferior à proposta de menor preço apurada no certame, no prazo máximo de 5 (cinco) minutos após o encerramento dos lances, sob pena de preclusão.

5.5. No caso de não contratação à microempresa ou à empresa de pequeno porte, serão convocadas as empresas remanescentes que se encontrem na situação de empate, de mesmo enquadramento empresarial, na ordem classificatória, para o exercício do direito aqui previsto.

5.5.1. Na hipótese de não haver mais empresas de mesmo enquadramento empresarial, o objeto da licitação será adjudicado para a empresa que originalmente apresentou o melhor lance.

5.6. As microempresas e empresas de pequeno porte deverão apresentar os documentos de habilitação, mesmo que estes apresentem alguma restrição relativa à regularidade fiscal e trabalhista, sob pena de inabilitação.

5.7. A microempresa ou empresa de pequeno porte que apresentar documentos com restrições quanto à regularidade fiscal e trabalhista tem assegurado o prazo de 5 (cinco) dias úteis, a partir da declaração de vencedor da licitação, prorrogável por igual período, a critério da Administração, para apresentar as respectivas certidões de regularidade.

5.8. A não regularização da documentação implicará decadência do direito à contratação, sem prejuízo da aplicação da multa de 2% (dois por cento) sobre o valor total da proposta inicial, sendo facultado à Administração convocar as licitantes remanescentes, na ordem de classificação.

5.9. Não se aplicam os critérios de desempate previstos nos **subitens 5.3 e 5.4**, caso a licitação se destine exclusivamente a participação de microempresas e empresas de pequeno porte.

5.10 Não haverá tratamento preferencial para microempresas e empresas de pequeno porte na hipótese do art. 4º, § 1º, I da Lei Federal nº 14.133/2021, conforme previsto no **subitem 4.1.1**.

6. DO CREDENCIAMENTO

6.1. Os interessados em participar da presente licitação deverão estar regularmente credenciados no Portal do Fornecedor RS (www.portaldofornecedor.rs.gov.br).

6.2. O credenciamento será encaminhado através do Portal do Fornecedor RS (www.portaldofornecedor.rs.gov.br).

7. DA PROPOSTA DE PREÇOS

7.1. Os licitantes deverão encaminhar proposta inicial até a data e hora marcadas para a abertura da sessão, exclusivamente no sistema eletrônico referido no **subitem 2.2**, quando se encerrará a fase de recebimento de propostas.

7.2. As propostas deverão ter prazo de validade não inferior a **60 dias**, a contar da data da abertura da licitação.

7.2.1. Se não constar o prazo de validade, entende-se o **subitem 7.2**.

7.3. A proposta de preços inicial deverá conter as características técnicas do produto ofertado, indicando obrigatória e expressamente, a sua marca e, se for o caso, o modelo.

7.4. Os licitantes deverão consignar o valor da proposta, já consideradas inclusas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

7.5. As propostas encaminhadas por Cooperativas de Trabalho não terão qualquer tipo de acréscimo para fins de julgamento.

7.6. No momento do envio da proposta, o licitante deverá prestar, por meio do sistema eletrônico, as seguintes declarações:

7.6.1. que tem conhecimento e atende a todas as exigências de habilitação e especificações técnicas previstas no Edital;

7.6.2. que assume o compromisso de guardar todos os documentos originais/autenticados, anexados eletronicamente, pelo prazo de 10 (dez) anos, e apresentá-los quando requeridos pela Administração Pública;

7.6.3. que os documentos anexados eletronicamente são fiéis aos originais e válidos para todos os efeitos legais, incorrendo nas sanções previstas na Lei Federal nº 14.133/2021, em caso de declaração falsa, sem prejuízo da responsabilização civil e criminal;

7.6.4. que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos, salvo na condição de aprendiz, a partir de quatorze anos, conforme previsto no inciso VI do art. 68 da Lei Federal nº 14.133/2021 (inciso XXXIII do art. 7º da Constituição Federal);

7.6.5. que tem conhecimento das condutas passíveis de penalidades, elencadas no **item 23** deste Edital, e previstas no art. 156 da Lei Federal nº 14.133/2021;

7.6.6. que até a presente data inexistem fatos impeditivos à sua participação, conforme **itens 4 e 5** deste Edital, salvo disposição extraordinária prevista em lei específica;

7.6.7. que possui ou não enquadramento empresarial como ME/EPP; para fins de obtenção do tratamento diferenciado e favorecido nos termos da Lei Complementar Federal nº 123/2006, se for o caso;

7.6.8. que, em sendo ME/EPP, possui ou não possui contratos celebrados com a Administração Pública cujos, valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, no ano-calendário de realização desta licitação;

7.6.9. que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

7.6.10 que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

7.7. As declarações mencionadas nos subitens anteriores são condicionantes para a participação no Pregão.

7.8. Nos casos de declaração falsa, o licitante estará sujeito à tipificação no crime de falsidade ideológica,

previsto no art. 299 do Código Penal Brasileiro, nos crimes previstos nos arts. 337-F e 337-I do Capítulo II-B, do Título XI da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e no art. 5º da Lei Federal nº 12.846/2013, sem prejuízo da aplicação das sanções administrativas previstas no presente Edital.

7.9. Até data e hora marcadas como fim do recebimento de propostas, o licitante poderá retirar ou substituir a proposta anteriormente apresentada.

7.10. Após a abertura da sessão, não cabe desistência da proposta, salvo por motivo resultante de fato superveniente e aceito pelo pregoeiro, sujeitando-se o licitante às sanções previstas na Lei Federal nº 14.133/2021.

7.11. Serão desclassificadas as propostas que não atenderem às exigências do presente Edital, forem omissas ou apresentarem irregularidades.

7.12. O preço proposto será de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração sob a alegação de erro, omissão ou qualquer outro pretexto.

7.13. Não será permitida a subcontratação por não se mostrar viável, sob a ótica técnico-econômica, a subcontratação parcial do objeto.

7.14. A omissão de qualquer despesa necessária ao perfeito cumprimento do objeto deste certame será interpretada como não existente ou já incluída no preço, não podendo o licitante pleitear acréscimo após a abertura da sessão pública.

7.15. O licitante deverá utilizar, sempre que possível, na elaboração da proposta, mão de obra, materiais, tecnologias e matérias-primas existentes no local da execução dos serviços, desde que não se produzam prejuízos à eficiência na execução do objeto da licitação.

7.16. É de inteira responsabilidade do licitante obter dos órgãos competentes informações sobre a incidência ou não de tributos de qualquer natureza relativos ao objeto desta licitação, nos mercados interno e/ou externo, não se admitindo alegação de desconhecimento de incidência tributária, ou outras correlatas.

7.17. As propostas ficarão disponíveis no sistema eletrônico.

8. DA SESSÃO PÚBLICA DE LICITAÇÃO

8.1. Os trabalhos serão conduzidos pelo pregoeiro, mediante a inserção e monitoramento de dados gerados ou transferidos no endereço eletrônico mencionado no **subitem 2.2**.

8.2. A participação no certame dar-se-á por meio da digitação da senha pessoal e intransferível do licitante credenciado e subsequente encaminhamento da proposta, exclusivamente por meio do sistema eletrônico, observados data e horário estabelecidos neste Edital.

8.3. O encaminhamento da proposta pressupõe o pleno conhecimento e atendimento das exigências de habilitação previstas neste Edital.

8.4. Caberá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública da licitação, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem emitida pelo sistema ou de sua desconexão.

8.5. Se ocorrer a desconexão do pregoeiro durante a etapa de lances e o sistema eletrônico permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

8.5.1. Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão pública da licitação será suspensa e terá reinício, com o aproveitamento dos atos anteriormente praticados, somente após comunicação expressa do pregoeiro aos participantes.

8.6. No caso de desconexão do licitante, ele deverá de imediato, sob sua inteira responsabilidade, providenciar sua conexão ao sistema.

9. DA REFERÊNCIA DE TEMPO

9.1. Todas as referências de tempo citadas no aviso da licitação, neste Edital, e durante a sessão pública,

observarão obrigatoriamente o horário de Brasília/DF e serão registradas no sistema eletrônico e na documentação relativa ao certame.

10. DA ABERTURA DA PROPOSTA E DA ETAPA COMPETITIVA

10.1. A abertura da sessão pública ocorrerá na data e na hora indicadas no **subitem 3.1**.

10.2. Durante a sessão pública, a comunicação entre o pregoeiro e os licitantes ocorrerá exclusivamente pelo sistema eletrônico.

10.2.1. Não será aceito nenhum outro tipo de contato, como meio telefônico ou *e-mail*.

10.3. O Critério de Julgamento será **MENOR PREÇO**.

10.4. A partir da abertura das propostas, as empresas participantes terão conhecimento dos valores ofertados.

10.5. A partir do momento de início da etapa de lances, as empresas participantes poderão formular lances de menor valor, sendo informados sobre seu recebimento, com indicação de horário e valor.

10.5.1. Só serão aceitos novos lances cujos valores forem inferiores em relação ao último lance registrado pela própria empresa, respeitando o **decremento mínimo de R\$ 10,00 (dez reais)**.

10.5.2. Não serão aceitos dois ou mais lances iguais, prevalecendo aquele que for recebido e registrado primeiro.

10.5.3. Será permitida a apresentação de lances intermediários.

10.6. Não poderá haver desistência dos lances ofertados após a abertura da sessão, sujeitando-se os licitantes desistentes às sanções previstas neste Edital, salvo se decorrente de caso fortuito ou força maior, com justificativa aceita pelo pregoeiro.

10.7. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

10.8. Durante a fase de lances, o pregoeiro poderá excluir, justificadamente, lance cujo valor seja manifestamente inexecutável.

10.9. A disputa ocorrerá pelo modo aberto.

10.10. A etapa de envio de lances na sessão pública durará dez minutos e, após isso, será prorrogada automaticamente pelo sistema, quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

10.10.1. A prorrogação automática da etapa de envio de lances será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive quando se tratar de lances intermediários.

10.10.2. Na hipótese de não haver novos lances, na forma estabelecida no **subitem 10.10** deste Edital, a sessão pública será encerrada automaticamente.

10.11. Após a definição da melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro poderá admitir o reinício da disputa aberta, conforme **subitem 10.10**, para a definição das demais colocações.

10.12. Definida a proposta vencedora, para fins de empate ficto, aplica-se o disposto no **item 5** deste Edital, se for o caso.

11. DA NEGOCIAÇÃO

11.1. Após o encerramento da etapa de lances e da aplicação do empate ficto, se for o caso, o pregoeiro poderá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado lance mais vantajoso, visando a que seja obtida melhor proposta, observado o critério de julgamento estabelecido, não se admitindo negociar condições diferentes daquelas previstas no Edital.

11.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

12. DA ACEITABILIDADE E DO JULGAMENTO DAS PROPOSTAS

12.1. O pregoeiro convocará o licitante classificado em primeiro lugar, para, em prazo não inferior a 01 (uma) hora, encaminhar, por meio eletrônico - **subitem 2.2** - a proposta de preço, acompanhada do **ANEXO II – MODELO DE PROPOSTA DE PREÇOS**, devidamente preenchido.

12.1.1. A proposta de preços fará parte do contrato, como seu anexo.

12.1.2. O pregoeiro verificará a proposta apresentada, e a desclassificará, motivadamente, se não estiver em conformidade com os requisitos estabelecidos neste Edital e no art. 59 da Lei Federal nº 14.133/2021.

12.2. O licitante que abandonar o certame, deixando de enviar a documentação solicitada, será desclassificado e estará sujeito às sanções previstas neste Edital.

12.3. O pregoeiro poderá solicitar parecer de técnicos pertencentes ao quadro de pessoal do órgão ou entidade contratante ou de terceiros, para orientar sua decisão.

12.4. Não se considerará qualquer oferta de vantagem não prevista neste Edital, inclusive financiamentos subsidiados ou a fundo perdido.

12.5. Não se admitirá proposta que apresente valores simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado, exceto quando se referirem a materiais e instalações de propriedade do licitante, para os quais ele renuncie expressamente à parcela ou à totalidade de remuneração.

12.6. Na verificação da conformidade da melhor proposta apresentada com os requisitos deste Edital, será desclassificada aquela que se enquadrar nas hipóteses previstas nos incisos do art. 59 da Lei Federal nº 14.133/2021.

12.6.1. Erros no preenchimento da Planilha de Custos e Formação de Preços não constituem motivo para desclassificação da proposta, podendo ser ajustada pelo licitante, no prazo indicado pelo pregoeiro, desde que não haja majoração do preço proposto.

12.7. Em caso de divergência entre valores grafados em algarismos e por extenso, prevalecerá o valor por extenso.

12.8. Havendo indicação de que a proposta apresentada seja inexecutável, caberá ao pregoeiro realizar as diligências para aferir a demonstração da exequibilidade da proposta, ou exigir do licitante a demonstração.

12.8.1. Será considerada inexecutável a proposta que não tenha demonstrada sua viabilidade por meio de documentação que comprove que os custos envolvidos na contratação são coerentes com os de mercado.

12.9. Será vencedor o licitante que **atender a íntegra do edital e ofertar o menor preço do lote e item.**

12.10. A classificação dos lances apresentados, a indicação da proposta vencedora e demais informações relativas à sessão pública constarão de ata divulgada no sistema eletrônico, sem prejuízo das demais formas de publicidade previstas na legislação pertinente.

13. DA HABILITAÇÃO

13.1. O licitante que apresentar a melhor proposta, durante a etapa competitiva, será convocado para apresentar os documentos de habilitação, em prazo a ser definido pelo pregoeiro, nunca inferior a 02 (duas) horas.

13.1.1. Os documentos devem ser apresentados através de upload em campo próprio do sistema eletrônico no qual o certame é realizado.

13.2. São exigidos os documentos de habilitação abaixo discriminados.

13.3. Documentos Relativos à Habilitação Jurídica:

13.3.1. documento oficial de identificação com foto, em se tratando de pessoa física;

13.3.2. certificado da condição de microempreendedor individual – CCMEI, em se tratando de Microempreendedor Individual – MEI;

13.3.3. registro comercial, no caso de empresa individual;

13.3.4. ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de

sociedades comerciais, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;

13.3.5. inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício;

13.3.6. decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir;

13.3.7. enquadramento como empresa de pequeno porte ou microempresa, emitido pela Junta Comercial, Industrial e Serviços do Rio Grande do Sul ou Órgão equivalente de outro Estado da Federação, ou, ainda, pela forma prevista no art. 39A da Lei Federal nº 8.934, de 18 de novembro de 1994, acompanhada de declaração na forma eletrônica, quando for o caso.

13.3.8. Declaração de habilitação, conforme o Anexo III deste Edital;

13.3.9. Declaração de composição societária e de nepotismo, conforme o Anexo IV deste Edital;

13.4. Documentos Relativos à Regularidade Fiscal, Social e Trabalhista:

13.4.1. documento oficial que comprove a inscrição no Cadastro de Pessoas Físicas (CPF), em se tratando de pessoa física;

13.4.2. comprovante de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ), em se tratando de pessoa jurídica;

13.4.3. comprovante de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou à sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

13.4.4. comprovante de regularidade para com a Fazenda Federal, Estadual e Municipal da sede do licitante, e, independentemente da sua sede, para com a Fazenda do Estado do Rio Grande do Sul, na forma da lei;

13.4.5. comprovante de regularidade relativa à Seguridade Social e ao Fundo de Garantia do Tempo de Serviço (FGTS), no caso de pessoa jurídica, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei;

13.4.6. comprovante de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de Certidão Negativa de Débitos Trabalhistas (CNDT).

13.5. Documentos Relativos à Qualificação Técnica:

13.5.1. comprovação de aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, mediante a apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado;

13.5.1.1. os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente;

13.5.1.2. somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, 1 (um) ano do início de sua execução, exceto se firmado para ser executado em prazo inferior;

13.5.1.3. considera-se compatível com o objeto da licitação o atestado que certifique a prestação de serviço com quantitativo de, no mínimo, 50% (cinquenta por cento) do objeto licitado.

13.6. Documentos Relativos à Qualificação Econômico-Financeira, em conformidade com o Decreto nº 57.154, de 22 de agosto de 2023, e com a Instrução Normativa CAGE Nº 11, de 4 de dezembro de 2023:

13.6.1. certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do licitante, com data de emissão não superior a 180 (cento e oitenta) dias anteriores à data prevista para o recebimento da documentação da habilitação e da proposta;

13.6.1.1. em se tratando de sociedade simples e pessoa física, deverá ser apresentada a certidão negativa de insolvência civil.

13.6.2. balanço patrimonial e demonstração de resultado de exercício dos dois últimos exercícios sociais, comprovando, em relação ao último exercício social

13.6.2.1. índices de liquidez geral - ILG, de solvência geral - ISG, e de liquidez corrente - ILC, superiores a

1 (um);

13.6.2.1.1. caso qualquer um dos índices referidos no item 13.6.2.1. apresente resultado inferior ou igual a 1 (um), **será exigido um patrimônio líquido mínimo de 10% (percentual por extenso) do valor da proposta final do licitante.**

13.6.3. os documentos do item 13.6.2 poderão ser substituídos pelo Certificado de Ateste e de Avaliação Econômico-Financeira de Licitantes, expedido pela Contadoria e Auditoria-Geral do Estado (CAGE), a ser obtido no site www.sisacf.sefaz.rs.gov.br.

13.6.4. **não será exigida declaração de contratos firmados pela licitante.**

13.6.5. é dos itens 13.6.2., 13.6.3. e 13.6.4. para o Microempresário Individual – MEI, que está prescindido de elaboração do Balanço Patrimonial e demais Demonstrações Contábeis na forma do §2º do art. 1.179 do Código Civil (Lei nº 10.406, de 10 de janeiro de 2002).

13.7. Documentos Complementares para Habilitação:

13.7.1. Além dos documentos relacionados nos **subitens 13.2 a 13.6** deste Edital, serão exigidos os seguintes documentos de habilitação:

13.7.1.1. Previstos no Termo de Referência, no que houver;

13.7.1.2. Para fins de habilitação, as Cooperativas de Trabalho deverão apresentar os seguintes documentos, em conjunto com aqueles previstos no **subitem 13** deste Edital, no que couber:

a) ata de fundação;

b) estatuto social com a ata da assembleia que o aprovou devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede;

c) registro previsto no art. 107 da Lei 5.764/1971.

13.8. Sob pena de inabilitação, os documentos encaminhados deverão estar em nome da participante, com indicação do número de inscrição no CNPJ/CPF.

13.9. Todos os documentos emitidos em língua estrangeira deverão ser entregues acompanhados da tradução para língua portuguesa.

13.10. Tratando-se de filial, os documentos de habilitação deverão estar em nome da filial, exceto aqueles que, pela própria natureza, são emitidos somente em nome da matriz.

13.11. Os documentos referentes à habilitação do licitante deverão estar válidos no dia de abertura da sessão pública.

13.11.1. Caso a data do julgamento da habilitação não coincida com a da abertura da sessão, e não seja possível ao pregoeiro verificar a validade dos documentos por meio de consulta a sites oficiais, o licitante será convocado a encaminhar, no prazo de no mínimo 2 (duas) horas, documento válido que comprove sua condição de habilitação na data da convocação, sob pena de inabilitação, ressalvado o disposto quanto à comprovação de regularidade fiscal das microempresas e empresas de pequeno porte, conforme estatui o art. 43, §1º, da Lei Complementar nº 123/2006.

13.11.2. Convocado o licitante, na forma do **subitem 13.11.1**, fica dispensada a comprovação de que ele estava habilitado na data de abertura da sessão, considerando-se, para fins de habilitação, somente a data da sua última convocação.

13.12. As certidões exigidas que não tenham prazo de validade expresse em seu corpo ter-se-ão como válidas pelo período de 180 (cento e oitenta) dias, a contar da sua emissão.

13.13. Caso seja apresentado o Certificado de Fornecedor do Estado, emitido pela Central de Licitações do Estado do Rio Grande do Sul – CELIC para a família informada nas **Família(s) 400 e/ou 117 de fornecedores a serem aceitas na apresentação do Certificado de Fornecedor do Estado – CFE** e acompanhado do respectivo anexo, este substituirá apenas os documentos que contemple, desde que estejam vigentes.

13.14. Todos os documentos em que se exija assinatura devem ser assinados digitalmente ou firmados e digitalizados antes de sua remessa via sistema.

13.15. Nos casos de apresentação de documento falso, o licitante estará sujeito à tipificação nos crimes de falsidade, previstos nos artigos 297 e 298 do Código Penal Brasileiro, nos crimes previstos nos arts. 337-F e 337-I do Capítulo II-B, do Título XI da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e no art. 5º da Lei Federal nº 12.846/2013, sem prejuízo da aplicação das sanções administrativas previstas no presente Edital.

13.16. Quando da apreciação dos documentos para habilitação, o pregoeiro procederá ao que segue:

13.16.1. se os documentos para habilitação não estiverem completos e corretos, ou contrariarem qualquer dispositivo deste Edital, considerando o disposto no **subitem 24.4** deste Edital, o pregoeiro considerará o licitante inabilitado;

13.16.2. no caso de inabilitação do primeiro classificado, serão retomados os procedimentos descritos no **item 11** deste Edital, respeitada a ordem de classificação do licitante que tenha apresentado lance mais vantajoso, e assim sucessivamente, até que sejam atendidas as condições do Edital.

14. DOS PEDIDOS DE ESCLARECIMENTOS, IMPUGNAÇÕES E RECURSOS

14.1. Qualquer pessoa é parte legítima para impugnar o Edital ou para solicitar esclarecimento sobre os seus termos, devendo protocolar o pedido até 3 (três) dias úteis antes da data de abertura do certame, no endereço indicado no **item 2.1**.

14.1.1. Caberá ao pregoeiro, auxiliado pelo setor técnico responsável, decidir sobre o pedido de esclarecimento ou a impugnação, no prazo de 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

14.1.2. Acolhida a impugnação, será definida e publicada nova data para realização do certame, quando da resposta resultar alteração que interfira na elaboração da proposta.

14.2. Após as etapas de classificação e habilitação, os licitantes receberão notificação pelo sistema, para, querendo, manifestar imediata e motivadamente a intenção de recorrer, obrigatoriamente via sistema eletrônico, com registro em ata da síntese das suas razões, sendo que o recurso terá efeito suspensivo.

14.2.1. A falta de manifestação acerca da intenção de recorrer, nos termos previstos neste Edital, importará a decadência desse direito.

14.2.2. Será concedido o prazo de 3 (três) dias úteis, contado da aceitabilidade da intenção de recorrer, para o licitante interessado apresentar suas razões fundamentadas, exclusivamente via sistema em que foi realizada a disputa constante no **subitem 2.2**, ficando os demais licitantes, desde logo, intimados para, querendo, apresentar contrarrazões em igual prazo, que começará a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses.

14.3. Caberá ao pregoeiro receber, examinar e decidir os recursos, no prazo de 3 (três) dias úteis, encaminhando à autoridade competente, devidamente informados, quando mantiver a sua decisão.

14.3.1. A autoridade competente deverá proferir a sua decisão no prazo de 10 (dez) dias úteis, contados a partir do recebimento dos autos.

14.3.2. O recurso será conhecido pelo pregoeiro, se for tempestivo, se estiver fundamentado conforme as razões manifestadas no final da sessão pública, se estiver de acordo com as condições deste Edital e se atender às demais condições para a sua admissibilidade.

14.3.3. O acolhimento de recurso implicará invalidação apenas dos atos insuscetíveis de aproveitamento.

15. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

15.1. O objeto da licitação será adjudicado ao licitante declarado vencedor, por ato do pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

15.2. Constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

16. DO TERMO DE CONTRATO

16.1. O adjudicatário terá o prazo **5 dias uteis**, após formalmente convocado, para assinar o contrato.

16.2. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do contrato, a Administração poderá encaminhar ao adjudicatário, mediante correspondência eletrônica, o termo de contrato para assinatura eletrônica avançada, conforme § 1º do art. 3º do Decreto nº 56.671, de 26 de setembro de 2022.

16.3. Os prazos previstos nos **subitens 16.1 e 16.2** poderão ser prorrogados, por igual período, por necessidade da Administração, ou por solicitação justificada do adjudicatário e aceita pela Administração.

16.4. **O prazo vigência da contratação será de 36 (trinta e seis) meses, contados a partir da emissão da ordem de fornecimento, podendo ser prorrogado sucessivamente, conforme os limites legais estabelecidos nos artigos 106 e 107 da Lei nº 14.133/2021.**

16.5. O(s) local(is) de execução do(s) serviço(s) será(ão) o(s) previsto(s) no **Termo de Referência**, quando couber.

16.6. Previamente à contratação, será realizada consulta ao Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, ao Cadastro Nacional de Empresas Punidas – CNEP, ao Cadastro de Fornecedores Impedidos de Licitatar e Contratar com a Administração Pública Estadual – CFIL/RS e ao Cadastro Informativo – CADIN/RS, pelo contratante, para identificar possível impedimento relativo ao participante vencedor, cujo comprovante será anexado ao processo.

16.7. Se o adjudicatário, no ato da assinatura do contrato, não comprovar que mantém as condições de habilitação, ou quando, injustificadamente, recusar-se à assinatura, será facultado à Administração convocar os licitantes remanescentes, na ordem de classificação, para a celebração do contrato nas condições propostas pelo licitante vencedor.

16.7.1. Caso o adjudicatário não assine o contrato, proceder-se-á à análise dos requisitos de habilitação dos licitantes remanescentes.

16.7.2. Os licitantes remanescentes ficam obrigados a atender à convocação, e a assinar o contrato no prazo fixado pela Administração, ressalvados os casos de vencimento das respectivas propostas, sujeitando-se às penalidades cabíveis no caso de recusa.

16.8. Na hipótese de nenhum dos licitantes aceitar a contratação, nos termos do **subitem 16.7**, a Administração, observados o valor estimado, poderá convocar os licitantes remanescentes para negociação, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário.

16.9. Na hipótese de nenhum dos licitantes aceitar a contratação nos termos do **subitem 16.8**, a Administração, observados o valor estimado, poderá adjudicar e celebrar o contrato nas condições ofertadas pelos licitantes remanescentes, atendida a ordem classificatória.

16.10. O gestor e os fiscais técnicos do contrato estão indicados:

Gestor do contrato: EDUARDO BORBA SEVERO

Fiscal técnico titular: JUAREZ BAMBERG DA SILVA

Fiscal técnico suplente: RODRIGO BULLOZA GRUPPELLI

17. DO ACORDO DE NÍVEL DE SERVIÇO

17.1. Nas condições **indicadas não será aplicado pela baixa complexidade e entrega única.**

18. DO PAGAMENTO

18.1. As condições para pagamento são as previstas na **Cláusula Sexta da Minuta de Contrato**, que compõe o Anexo I do presente Edital.

19. DO REAJUSTE

19.1. O contrato será reajustado conforme disposto na **Cláusula Oitava do Termo de Contrato**, que compõe o Anexo I do presente Edital.

20. DA FONTE DE RECURSOS

20.1. As despesas decorrentes do contrato objeto desta licitação correrão por conta de recurso orçamentário:

Unidade Orçamentária: 07.01 TRIBUNAL DE JUSTIÇA MILITAR DO RS

Atividade/Projeto: 3902 – GESTAO DE TIC

Natureza da Despesa – NAD: 3.3.90.40 - SERV. TIC - PESS.JURIDICA

Recurso: 2002 – REC VINC LEI

21. DAS OBRIGAÇÕES DO ADJUDICATÁRIO

21.1. O adjudicatário deverá atender às obrigações previstas na Cláusula Décima da Minuta de Contrato e as demais obrigações específicas ao objeto contratual.

22. DA GARANTIA DE EXECUÇÃO

22.1. **Não será solicitada Garantia de Cumprimento do Contrato.**

22.2. Caso não seja observado o prazo fixado para apresentação da garantia, aplicar-se-á o disposto no **subitem 23.4.6** deste Edital.

23. DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

23.1. Das Infrações Administrativas

23.1.1. Comete infração administrativa, nos termos da Lei Federal nº 14.133/2021, o participante ou o contratado que:

23.1.1.1. der causa à inexecução parcial do contrato;

23.1.1.2. der causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

23.1.1.3. der causa à inexecução total do contrato;

23.1.1.4. deixe de entregar a documentação exigida para o certame;

23.1.1.5. não mantenha a proposta, salvo se a não manutenção decorrer de fato superveniente, devidamente justificado;

23.1.1.6. não celebre o contrato ou não entregue a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

23.1.1.7. enseje o retardamento da execução ou da entrega do objeto da licitação, sem motivo justificado;

23.1.1.8. apresente declaração ou documentação falsa exigida para o certame, ou preste declaração falsa durante a licitação ou a execução do contrato;

23.1.1.9. fraude a licitação ou pratique ato fraudulento na execução do contrato;

23.1.1.10. comporte-se de modo inidôneo ou cometa fraude de qualquer natureza;

23.1.1.11. pratique atos ilícitos com vistas a frustrar os objetivos da licitação;

23.1.1.12. pratique ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

23.2. Do Processo Administrativo e das Sanções Administrativas

23.2.1. A aplicação de quaisquer das penalidades aqui previstas realizar-se-á em processo administrativo,

assegurado o contraditório e a ampla defesa, observando-se o procedimento previsto na Lei Federal nº 14.133/2021, e, subsidiariamente, na Lei nº 15.612, de 6 de maio de 2021.

23.2.2. Serão aplicadas ao responsável pelas infrações administrativas, de acordo com a dosimetria estabelecida na norma indicada no INSTRUÇÃO NORMATIVA CELIC/SPGG Nº 02/2023, publicada no DOE do Rio Grande do Sul em 29 de setembro de 2023 (<https://www.diariooficial.rs.gov.br/materia?id=908247>), as seguintes sanções:

23.2.2.1. advertência, para a infração prevista no **subitem 23.1.1.1**, quando não se justificar a imposição de penalidade mais grave;

23.2.2.2. multa, nas modalidades:

23.2.2.2.1. compensatória, de até 10% sobre o valor da parcela inadimplida, para quaisquer das infrações previstas nos **subitens 23.1.1.1. a 23.1.1.12**;

23.2.2.2.2. moratória, pelo atraso injustificado na execução do contrato, de até 0,5% (meio por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

23.2.2.3. impedimento de licitar e contratar, para as infrações previstas nos **subitens 23.1.1.2. a 23.1.1.7**, quando não se justificar a imposição de penalidade mais grave;

23.2.2.4. declaração de inidoneidade para licitar e contratar, para as infrações previstas nos **subitens 23.1.1.8. a 23.1.1.12**.

23.3. Da Aplicação das Sanções

23.3.1. As sanções aqui previstas são independentes entre si, podendo ser aplicadas isoladas ou, no caso das multas, cumulativamente, sem prejuízo de outras medidas cabíveis.

23.3.2. A aplicação de sanções não exime o licitante ou o contratado da obrigação de reparar os danos, perdas ou prejuízos que venha a causar ao ente público.

23.3.2.1. O valor previsto a título de multa compensatória será tido como mínimo da indenização devida à título de perdas e danos, competindo ao contratante provar o prejuízo excedente, nos termos do art. 416 do Código Civil - Lei nº 10.406/2002.

23.3.3. A multa de mora poderá ser convertida em multa compensatória, com a aplicação cumulada de outras sanções previstas neste Edital.

23.3.4 As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

23.3.5. O contrato, sem prejuízo das multas e demais cominações legais previstas no instrumento, poderá ser rescindido unilateralmente, por ato formal da Administração, nos casos enumerados nos incisos do *caput* do art. 137 da Lei Federal nº 14.133/2021.

23.3.6. As sanções previstas neste item não elidem a aplicação das penalidades estabelecidas na Lei Federal nº 12.846, de 1º de agosto de 2013, conforme o disposto no seu art. 30 ou nos arts. 337-E a 337-P, Capítulo II-B, do Título XI da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal).

23.3.7. Serão reputados como inidôneos atos como os descritos nos arts. 337-F, 337-I, 337-J, 337-K, 337-L e no art. 337-M, §§ 1º e 2º, do Capítulo II-B, do Título XI da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal).

23.3.8. As sanções de impedimento de licitar e contratar e de declaração de inidoneidade levam à inclusão do licitante no CFIL/RS.

23.4. Da execução da garantia contratual

23.4.1. O valor da multa poderá ser descontado da garantia contratual.

23.4.2. Se a multa for de valor superior ao da garantia prestada, além da perda desta, responderá o contratado pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pelo contratante.

23.4.3. Se os valores da garantia e das faturas forem insuficientes, fica o contratado obrigado a recolher a diferença devida, no prazo de 15 (quinze) dias, contados da comunicação oficial.

23.4.4. Esgotados os meios administrativos para cobrança do valor devido pelo contratado ao contratante, o débito será encaminhado para inscrição em dívida ativa não tributária.

23.4.5. Caso o valor da garantia seja utilizado, no todo ou em parte, para o pagamento da multa, essa deve ser complementada no prazo de até 10 (dez) dias, contado da solicitação do contratante.

23.4.6. Em se tratando de inobservância do prazo fixado para apresentação da garantia (seja para reforço ou por ocasião de prorrogação), aplicar-se-á multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, observado o máximo de 2% (dois por cento).

24. DAS DISPOSIÇÕES FINAIS

24.1. As atas serão geradas eletronicamente após o encerramento da sessão pública pelo pregoeiro.

24.1.1. Nas atas da sessão pública, deverão constar os registros dos licitantes participantes, das propostas apresentadas, da análise da documentação de habilitação, das manifestações de intenção de interposição de recursos, se for o caso, do respectivo julgamento dos recursos, e do vencedor da licitação.

24.1.2. Os demais atos licitatórios serão registrados nos autos do processo da licitação.

24.2. O licitante deverá examinar detidamente as disposições contidas neste Edital, pois a simples apresentação da proposta o vincula de modo incondicional ao competitivo.

24.3. A falsidade de qualquer documento ou a inverdade das informações nele contidas implicará a imediata desclassificação do licitante que o tiver apresentado, sem prejuízo das demais sanções cabíveis.

24.4. No julgamento da habilitação e das propostas, o pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

24.4.1. É facultado ao pregoeiro ou à autoridade superior convocar os licitantes para quaisquer esclarecimentos necessários ao entendimento de suas propostas.

24.5. As informações, atas e relatórios pertinentes à presente licitação serão disponibilizados no *site* referido no **subitem 2.1**, sem prejuízo às informações prestadas ao Portal Nacional de Contratações Públicas.

24.6. O contratado deverá conceder livre acesso aos seus documentos e registros contábeis, referentes ao objeto da licitação, para os servidores do órgão ou entidade contratante e dos órgãos de controle interno e externo.

24.7. A homologação do resultado desta licitação não implicará direito à contratação.

24.8. O presente Edital, bem como a proposta vencedora, fará parte integrante do instrumento de contrato, como se nele estivessem transcritos.

24.9. Aplicam-se aos casos omissos as disposições constantes na Lei Federal nº 14.133/2021.

24.10. Prevalecerão as disposições deste Edital, em caso de divergência com as demais peças que compõem o processo.

24.11. Fica eleito o foro da Comarca de Porto Alegre para dirimir quaisquer dúvidas ou questões relacionadas a este Edital ou aos seus anexos.

24.12. Integram este Edital, ainda, para todos os fins e efeitos, os seguintes anexos:

ANEXO I – MINUTA DE CONTRATO

ANEXO II – MODELO DE PROPOSTAS DE PREÇOS (preenchida pelo licitante vencedor)

ANEXO III – MODELO DE DECLARAÇÃO PARA HABILITAÇÃO

ANEXO IV – MODELO DE DECLARAÇÃO DE COMPOSIÇÃO SOCIETÁRIA E DE NEPOTISMO

ANEXO V – TERMO DE REFERÊNCIA

ANEXO VI - ANÁLISE CONTÁBIL DA CAPACIDADE FINANCEIRA DE LICITANTE

Pregoeira:

ÂNGELA MARIA BATISTA DE AGUIAR, ID 2320568

Equipe de Apoio:

RODRIGO FREITAS DE ALMEIDA, ID 2695812

MAURO MARCHIORI SCHMIDT, ID 2288451

Porto Alegre, 06 de março de 2025.

HERBERT SCHONHOFEN

Diretor - Geral

ANEXO I - MINUTA DE CONTRATO
TERMO DE CONTRATO Nº/2025 - SEAORÇ-TJM/RS

PREGÃO ELETRÔNICO Nº 002/2025 - SEAORÇ-TJM/RS

Processo SEI – 9.2025.0700-000.....

Termo de Contrato para contratação de empresa(s) especializada(s) para a renovação da licença da solução de antivírus Kaspersky Endpoint Security com upgrade do licenciamento Kaspersky Select para a versão Kaspersky endpoint Detection and Response Optimum (EDR), pelo período de 36 (trinta e seis) meses, para atender as necessidades da Justiça Militar do RS, autorizado no Processo SEI nº 9.2024.0700.000618-7

NOME E QUALIFICAÇÃO DAS PARTES

CONTRATANTE: ESTADO DO RIO GRANDE DO SUL, PODER JUDICIÁRIO - JUSTIÇA MILITAR DO ESTADO DO RIO GRANDE DO SUL, inscrito no CNPJ sob nº 89.522.064/0002-47, com sede nesta Capital, na Avenida Praia de Belas, nº 799, adiante denominado simplesmente CONTRATANTE, por intermédio de seu Representante Legal, competente para o ato, Sra. MARIA EMÍLIA MOURA DA SILVA, Desembargadora Militar Presidente do TJM/RS.

CONTRATADA: [NOME], inscrita no CNPJ sob o número [CNPJ], com sede na [endereço completo], tel. (XX) xxx. xxxx, e-mail xxxxx@xxxxxxxxx.xxx.xx, adiante denominada simplesmente CONTRATADA, representada pelo(a) Senhor(a) [Nome], inscrito no Cadastro de Pessoas Físicas (CPF) sob o número xxx.xxx.xxx-xx.

As partes sujeitam-se às normas da Lei nº 14.133, de 1º de abril de 2021 e alterações posteriores, bem como da Lei nº 11.389/99, regulamentada pelo Decreto nº 42.250, de 19 de maio de 2003 e Lei Complementar nº 116/2003, em consonância com a Consolidação das Leis do Trabalho e Convenção Coletiva de Trabalho da respectiva Categoria Profissional, no que couber.

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. Contratação de empresa para renovação de licenças da solução de antivírus Kaspersky Endpoint Security, incluindo upgrade do licenciamento Kaspersky Select para a versão Kaspersky Endpoint Detection and Response Optimum (EDR). A vigência será de 36 meses, podendo ser prorrogada conforme limites legais (Lei nº 14.133/2021, artigos 106 e 107).

1.2. Este contrato vincula-se ao Edital, identificado no preâmbulo, e à proposta vencedora, independentemente de transcrição.

CLÁUSULA SEGUNDA - DO PREÇO

2.1. O preço total a ser pago pelo contratante, referente à execução dos serviços contratados, é de R\$ _____ (_____), de acordo com a proposta vencedora da licitação, entendido este como preço justo e suficiente para a total execução do presente objeto.

2.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

CLÁUSULA TERCEIRA - DO RECURSO FINANCEIRO

3.1. As despesas decorrentes do presente contrato correrão à conta do seguinte recurso financeiro:

Unidade Orçamentária: 07.01 JUSTICA MILITAR DO ESTADO

Atividade/Projeto: 3902 GESTAO DE TIC – JME

Natureza da Despesa: 3.3.90.40 SERV. TIC - PESS.JURIDICA

Recurso: 2002 TR REC VINC P/LEI-PJ

CLÁUSULA QUARTA – DO PRAZO CONTRATUAL E LOCAL DE PRESTAÇÃO DOS SERVIÇOS

4.1. O prazo de duração do contrato é de 36 (trinta e seis) meses, contados a partir da emissão da ordem de fornecimento, podendo ser prorrogado sucessivamente, conforme os limites legais estabelecidos nos artigos 106 e 107 da Lei nº 14.133/2021.

4.2. A expedição da ordem de início dos serviços somente se efetivará após a assinatura do contrato, com sua divulgação no Portal Nacional de Contratações Públicas.

4.3. O objeto do contrato visa atender às necessidades do Tribunal de Justiça Militar do Estado do Rio Grande do Sul (TJM/RS), da 1ª Auditoria Militar, da 2ª Auditoria Militar, da Auditoria Militar de Santa Maria e da Auditoria Militar de Passo Fundo, conforme as condições, quantidades e exigências estabelecidas neste Termo de Referência.

4.3.1. O local da entrega será na Avenida Praia de Belas, nº 799, Bairro Praia de Belas, em Porto Alegre.

4.3.2. A CONTRATADA poderá disponibilizar o software para download, mediante credenciais de acesso, por meio de ambiente seguro na internet.

4.4. O prazo de duração do presente contrato pode ser prorrogado por interesse das partes até o limite máximo de 10 (dez) anos, desde que haja autorização formal da autoridade competente e observados os seguintes requisitos:

4.4.1. os serviços tenham sido prestados regularmente;

4.4.2. a Administração mantenha interesse na realização do serviço;

4.4.3. o valor do contrato permaneça economicamente vantajoso para a Administração; e

4.4.4. os custos não renováveis já pagos ou amortizados no primeiro ano do contrato deverão ser eliminados.

4.5. O contratado não tem direito subjetivo a prorrogação contratual.

CLÁUSULA QUINTA – DA GARANTIA

5.1. Não será solicitada garantia do fornecedor.

CLÁUSULA SEXTA – DO PAGAMENTO

6.1. O pagamento deverá ser efetuado no prazo de 20 (vinte) dias mediante a apresentação de Nota Fiscal ou da Fatura pelo contratado, que deverá conter o detalhamento dos serviços executados, acompanhada de certidões negativas fiscais.

6.1.1. As faturas deverão ser apresentadas no mês subsequente ao da prestação do serviço.

6.2. O pagamento será efetuado contra empenho, mensalmente, após verificação do fiel cumprimento das obrigações assumidas e o ateste das faturas pela área/fiscal competente.

6.2.1. Notas fiscais eletrônicas deverão ser enviadas para o e-mail informatica@tjmrs.jus.br, com cópia para servico-orcamento@tjmrs.jus.br.

6.3. O documento fiscal deverá ser do estabelecimento que apresentou a proposta vencedora da licitação e, nos casos em que a emissão for de outro estabelecimento da empresa, o documento deverá vir acompanhado das certidões negativas relativas à regularidade fiscal.

6.3.1. Quando o documento for de outro estabelecimento localizado fora do Estado, será exigida também certidão negativa relativa à Regularidade Fiscal junto à Fazenda Estadual do Rio Grande do Sul, independentemente da localização da sede ou filial do licitante.

6.4. A protocolização somente poderá ser feita após a prestação dos serviços por parte do contratado.

6.5. O pagamento será efetuado por serviço efetivamente prestado e aceito.

6.5.1. A glosa do pagamento durante a execução contratual, sem prejuízo das sanções cabíveis, só deverá ocorrer quando o contratado:

6.5.1.1. não produzir os resultados, deixar de executar, ou não executar as atividades com a qualidade mínima exigida no contrato; ou

6.5.1.2. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

6.6. Caso o serviço não seja prestado fielmente e/ou apresente alguma incorreção será considerado como não aceito e o prazo de pagamento será contado a partir da data de regularização.

6.7. Na fase da liquidação da despesa deverá ser efetuada consulta ao CADIN/RS, para fins de comprovação do cumprimento da relação contratual estabelecida, nos termos do disposto no artigo 92, inciso XVI, da Lei Federal nº 14.133/2021;

6.7.1. Constatando-se situação de irregularidade do contratado junto ao CADIN/RS, será providenciada sua notificação, por escrito, para que, no prazo de 15 (quinze) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa.

6.7.2. Persistindo a irregularidade, o contratante poderá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurado ao contratado a ampla defesa.

6.8. Os pagamentos a serem efetuados em favor do contratado, quando couber, estarão sujeitos às retenções tributárias devidas sobre o valor da fatura de serviços do contratado, nos termos da legislação vigente.

6.9. As empresas dispensadas de retenções deverão entregar declaração, anexa ao documento de cobrança, assinadas pelo representante legal, além de informar sua condição no documento fiscal, inclusive o enquadramento legal.

6.10. O contratante poderá reter, do valor da fatura do contratado, a importância correspondente ao inadimplemento contratual, até a regularização das obrigações assumidas pelo contratado.

CLÁUSULA SÉTIMA - DA ATUALIZAÇÃO MONETÁRIA

7.1. Os valores do presente contrato não pagos na data prevista serão corrigidos até a data do efetivo pagamento, *pro rata die*, pelo Índice de Preços ao Consumidor Amplo – IPCA, do Sistema Nacional de Índices de Preços ao Consumidor – SNIPC, ou outro que venha a substituí-lo.

CLÁUSULA OITAVA – DO REAJUSTE DO PREÇO

8.1. O contrato será reajustado, observado o interregno mínimo de um ano, a contar da data-base do orçamento estimado.

8.1.1. Considera-se data-base, para fins de reajuste, a data de montagem da contratação, constante no **Anexo V - Termo de Referência**.

8.1.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

8.2. O valor do contrato será reajustado pelo IPCA, obedecendo-se a metodologia de cálculo adequada para sua atualização.

CLÁUSULA NONA – REEQUILÍBRIO ECONÔMICO-FINANCEIRO

9.1. Caso o contratado pleiteie o reequilíbrio econômico-financeiro do contrato, fica o contratante obrigado a responder em até 30 (trinta) dias da data do requerimento.

9.1.1. O não cumprimento do prazo constante na **subcláusula 9.1** não implica em deferimento do pedido por parte do contratante

9.2. Todos os documentos necessários à apreciação do pedido deverão ser apresentados juntamente com o requerimento.

9.3. O pedido de restabelecimento do equilíbrio econômico-financeiro deverá ser formulado durante a vigência do contrato.

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DO CONTRATADO

10.1. Executar os serviços, conforme especificações contidas no **Anexo V - Termo de Referência**, e na sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além do fornecimento dos materiais, equipamentos, ferramentas e utensílios necessários.

10.2. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação, devendo comunicar ao contratante a superveniência de fato impeditivo da manutenção dessas condições.

10.3. Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor.

10.4. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

10.5. Responsabilizar-se pelos danos causados diretamente à Administração ou aos bens do contratante, ou ainda a terceiros, decorrentes de sua culpa ou dolo, durante a execução deste contrato, ficando o contratante autorizado a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos ao contratado, o valor correspondente aos danos sofridos.

10.6. Apresentar os empregados devidamente uniformizados e identificados por meio de crachá, além de provê-los com os Equipamentos de Proteção Individual - EPI, quando for o caso.

10.7. Apresentar ao contratante, quando for o caso, a relação nominal dos empregados que adentrarão o órgão para a execução do serviço.

10.8. Atender às solicitações do contratante quanto à substituição dos empregados alocados, no prazo fixado pela Administração, nos casos em que ficar constatado descumprimento das obrigações relativas à execução do serviço.

10.9. Orientar seus empregados quanto à necessidade de acatar as normas internas da Administração.

10.10. Orientar seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato.

10.11. Manter preposto formalmente designado nos locais de prestação de serviço, aceito pela Administração, para representá-lo na execução do contrato, quando couber.

10.12. Responder, nos prazos legais, em relação aos seus empregados, por todas as despesas decorrentes da execução do serviço e por outras correlatas, tais como salários, seguros de acidentes, indenizações, tributos, vale-refeição, vale-transporte, uniformes, crachás e outras que venham a ser criadas e exigidas pelo Poder Público.

10.13. Fiscalizar regularmente os seus empregados designados para a prestação do serviço, a fim de verificar as condições de execução.

10.14. Comunicar ao contratante qualquer anormalidade constatada e prestar os esclarecimentos solicitados.

10.15. Arcar com as despesas decorrentes de qualquer infração cometida por seus empregados quando da

execução do serviço objeto deste contrato.

10.16. Realizar os treinamentos que se fizerem necessários para o bom desempenho das atribuições de seus empregados.

10.17. Treinar seus empregados quanto aos princípios básicos de postura no ambiente de trabalho, tratamento de informações recebidas e manutenção de sigilo, comportamento perante situações de risco e atitudes para evitar atritos com servidores, colaboradores e visitantes do órgão.

10.18. Coordenar e supervisionar a execução dos serviços contratados.

10.19. Administrar todo e qualquer assunto relativo aos seus empregados.

10.20. Assumir todas as responsabilidades e adotar as medidas necessárias ao atendimento dos seus empregados acidentados ou acometidos de mal súbito, por meio do preposto.

10.21. Instruir seus empregados quanto à prevenção de acidentes e de incêndios.

10.22. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias, comerciais e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade ao contratante.

10.23. Relatar ao contratante toda e qualquer irregularidade verificada no decorrer da prestação dos serviços

10.24. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.

10.25. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de 14 anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

10.26. Informar endereço eletrônico para recebimento de correspondência oficial.

10.27. Atender às seguintes obrigações, decorrentes da Lei Federal nº 13.709/2018 - Lei Geral de Proteção de Dados – LGPD:

10.27.1. garantir que a gestão dos dados pessoais decorrentes do contrato ocorra com base nas Diretrizes e Normas Gerais da LGPD, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

10.27.2. garantir que os dados pessoais envolvidos no objeto deste contrato não serão utilizados para compartilhamento com terceiros alheios ao objeto de contratação, tampouco utilizados para finalidade avessa à estipulada por este documento, salvo casos previstos em lei.

10.27.3. garantir que os dados regulamentados pela LGPD estarão armazenados dentro do território nacional, salvo exceções de comum acordo com o contratante.

10.27.4. se abster de analisar o comportamento dos titulares dos dados regulados pela LGPD, com o objetivo de divulgação a terceiros, conduta esta que é expressamente vedada pelo presente contrato.

10.27.5. garantir que a execução do objeto da contratação esteja plenamente adequada à LGPD, permitindo auditorias solicitadas pelo contratante.

10.28. Cumprir as exigências de reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz.

10.29. Responder diretamente por quaisquer perdas, danos ou prejuízos que vierem a causar ao contratante ou a terceiros, decorrentes de sua ação ou omissão, dolosa ou culposa, na execução do contrato, independentemente de outras cominações contratuais ou legais a que estiver sujeita.

10.30. O contratado deverá comprovar que possui Programa de Integridade se o prazo de vigência a que se refere a **subcláusula 4.1** for igual ou superior a 180 (cento e oitenta) dias e o valor total da contratação a que se refere a **subcláusula 2.1** for superior ao valor de R\$ 1.585.800,00 (um milhão, quinhentos e oitenta e cinco mil e oitocentos reais), atualizado pela variação da UPF/RS até o ano da assinatura do contrato, conforme art. 7º da Instrução Normativa CAGE nº 6, de 23 de dezembro de 2021.

10.30.1. A comprovação da exigência de Programa de Integridade se dará com a apresentação do Certificado de Apresentação de Programa de Integridade, fornecido pela Contadoria e Auditoria-Geral do Estado.

10.30.1.1. Caso o contratado seja um consórcio de empresas, a empresa líder do consórcio deverá obter o Certificado de Apresentação do Programa de Integridade.

10.30.2. Será de 180 (cento e oitenta) dias corridos, a contar da data de celebração do contrato, o prazo para obter o Certificado de Apresentação do Programa de Integridade.

10.30.3. Caberá ao contratado custear as despesas relacionadas à implantação do Programa de Integridade.

10.30.4. Observar-se-á, para a apresentação e avaliação do Programa de Integridade, as disposições da Lei nº 15.228, de 25 de setembro de 2018, do Decreto nº 55.631, de 9 de dezembro de 2020, e da Instrução Normativa CAGE nº 6, de 23 de dezembro de 2021.

10.31. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objeto da licitação.

10.32. Atender a todas as características e especificações de funcionalidades e serviços descritos no **ANEXO V – TERMO DE REFERÊNCIA.**

CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DO CONTRATANTE

11.1. Exercer o acompanhamento e a fiscalização dos serviços, por servidores designados para esse fim, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

11.2. Exigir o cumprimento de todas as obrigações assumidas pelo contratado, de acordo com as cláusulas contratuais e os termos de sua proposta.

11.3. Notificar o contratado por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção.

11.4. Pagar ao contratado o valor resultante da prestação do serviço, no prazo e condições estabelecidas na **cláusula sexta.**

11.5. Efetuar as retenções tributárias devidas sobre o valor da fatura de serviços do contratado, nos termos da legislação vigente.

CLÁUSULA DÉCIMA SEGUNDA – DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

12.1. Das Infrações Administrativas

12.1.1. Comete infração administrativa, nos termos da Lei Federal nº 14.133/2021, o contratado que:

12.1.1.1. der causa à inexecução parcial do contrato;

12.1.1.2. der causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

12.1.1.3. der causa à inexecução total do contrato;

12.1.1.4. enseje o retardamento da execução ou da entrega do objeto do contrato, sem motivo justificado, o qual se configura quando o contratado:

12.1.1.4.1. deixe de iniciar, sem causa justificada, a execução do contrato após 7 (sete) dias contados da data da ordem de serviço;

12.1.1.4.2. deixe de realizar, sem causa justificada, os serviços definidos no contrato por 3 (três) dias seguidos ou por 10 (dez) dias intercalados.

12.1.1.5. apresente declaração ou documentação falsa, ou preste declaração falsa durante a execução do contrato;

12.1.1.6. pratique ato fraudulento na execução do contrato;

12.1.1.7. comporte-se de modo inidôneo ou cometa fraude de qualquer natureza; ou

12.1.1.8. pratique ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

12.2. Do Processo Administrativo e das Sanções Administrativas

12.2.1. A aplicação de quaisquer das penalidades aqui previstas realizar-se-á em processo administrativo, assegurado o contraditório e a ampla defesa, observando-se o procedimento previsto na Lei Federal nº 14.133/2021, e, subsidiariamente, na Lei nº 15.612, de 6 de maio de 2021.

12.2.2. Serão aplicadas ao responsável pelas infrações administrativas, de acordo com a dosimetria estabelecida na **Instrução Normativa n.º 02/2023 da Subsecretaria da Administração Central de Licitações** (<https://www.diariooficial.rs.gov.br/materia?id=908247>), as seguintes sanções:

12.2.2.1. advertência, para a infração prevista na **subcláusula 12.1.1.1**, quando não se justificar a imposição de penalidade mais grave;

12.2.2.2. multa, nas modalidades:

12.2.2.2.1. compensatória, de até 10% sobre o valor da parcela inadimplida, para quaisquer das infrações previstas nas **subcláusulas 12.1.1.1. a 12.1.1.8**;

12.2.2.2.2. moratória, pelo atraso injustificado na execução do contrato, de até 0,5% (meio por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

12.2.2.2.3. moratória, pela não obtenção do Certificado de Apresentação de Programa de Integridade dentro do prazo referido na **subcláusula 10.30.2**, de até 0,02% (dois centésimos por cento) por dia de atraso sobre o valor do contrato, até o limite de 10% (dez por cento);

12.2.2.2.4. impedimento de licitar e contratar, para as infrações previstas nas **subcláusulas 12.1.1.2. a 12.1.1.4**, quando não se justificar a imposição de penalidade mais grave;

12.2.2.2.5. declaração de inidoneidade para licitar e contratar, para as infrações previstas nas **subcláusulas 12.1.1.5. a 12.1.1.8**.

12.3. Da Aplicação das Sanções

12.3.1. As sanções aqui previstas são independentes entre si, podendo ser aplicadas isoladas ou, no caso das multas, cumulativamente, sem prejuízo de outras medidas cabíveis.

12.3.2. A aplicação de sanções não exime o contratado da obrigação de reparar os danos, perdas ou prejuízos que venha a causar ao ente público.

12.3.2.1. O valor previsto a título de multa compensatória será tido como mínimo da indenização devida à título de perdas e danos, competindo ao contratante provar o prejuízo excedente, nos termos do art. 416 do Código Civil - Lei nº 10.406/2002.

12.3.3. A multa de mora poderá ser convertida em multa compensatória, com a aplicação cumulada de outras sanções previstas neste Edital.

12.3.4 As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

12.3.5. O contrato, sem prejuízo das multas e demais cominações legais previstas no instrumento, poderá ser rescindido unilateralmente, por ato formal da Administração, nos casos enumerados nos incisos do *caput* do art. 137 da Lei Federal nº 14.133/2021.

12.3.6. As sanções previstas neste item não elidem a aplicação das penalidades estabelecidas na Lei Federal nº 12.846, de 1º de agosto de 2013, conforme o disposto no seu art. 30, nos arts. 337-E a 337-P, Capítulo II-B, do Título XI da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), ou na Lei estadual nº 15.228, de 25 de setembro de 2018, em especial seu art. 41.

12.3.7. Serão reputados como inidôneos atos como os descritos nos arts.337-F, 337-I, 337-J, 337-K, 337-L e no art. 337-M, §§ 1º e 2º, do Capítulo II-B, do Título XI da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal).

12.3.8. As sanções de suspensão e de declaração de inidoneidade levam à inclusão do licitante no CFIL/RS.

12.3.9. A aplicação de multa de mora não impedirá que a Administração a converta em compensatória e promova a extinção unilateral do contrato com a aplicação cumulada de outras sanções previstas neste Edital.

12.3.10. A aplicação de qualquer penalidade não exclui a aplicação da multa.

12.4. Da execução da garantia contratual

12.4.1. O valor da multa poderá ser descontado da garantia contratual.

12.4.2. Se a multa for de valor superior ao da garantia prestada, além da perda desta, responderá o contratado pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pelo contratante.

12.4.3. Se os valores da garantia e das faturas forem insuficientes, fica o contratado obrigado a recolher a diferença devida, no prazo de 15 (quinze) dias, contados da comunicação oficial.

12.4.4. Esgotados os meios administrativos para cobrança do valor devido pelo contratado ao contratante, o débito será encaminhado para inscrição em dívida ativa não tributária.

12.4.5. Caso o valor da garantia seja utilizado, no todo ou em parte, para o pagamento da multa, essa deve ser complementada no prazo de até 10 (dez) dias, contado da solicitação do contratante.

12.4.6. Em se tratando de inobservância do prazo fixado para apresentação da garantia (seja para reforço ou por ocasião de prorrogação), aplicar-se-á multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, observado o máximo de 2% (dois por cento).

CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO ANTECIPADA

13.1. O presente Contrato poderá ser extinto antecipadamente por interesse da Administração nas hipóteses do art. 137 com as consequências previstas no art. 139 da Lei Federal nº 14.133/2021, devendo a decisão ser formalmente motivada, assegurando-se ao contratado o contraditório e a ampla defesa.

13.2. O presente Contrato poderá ser extinto antecipadamente por interesse do contratado nas hipóteses do art. 137, §2º, com as consequências previstas no art. 138, §2º, da Lei Federal nº 14.133/2021.

13.3. A extinção antecipada do contrato deverá observar os seguintes requisitos:

13.3.1. levantamento dos eventos contratuais já cumpridos ou parcialmente cumpridos;

13.3.2. relação dos pagamentos já efetuados e ainda devidos;

13.3.3. apuração de indenizações e multas; e

13.3.4. notificação dos emitentes da garantia prevista na cláusula quinta deste contrato, quando cabível.

CLÁUSULA DÉCIMA QUARTA - DAS VEDAÇÕES

14.1. É vedado ao contratado:

14.1.1. caucionar ou utilizar este Contrato para qualquer operação financeira;

14.1.2. interromper a execução dos serviços, sob alegação de inadimplemento por parte do contratante, salvo nos casos previstos em lei.

CLÁUSULA DÉCIMA QUINTA – DAS ALTERAÇÕES

15.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 a 136 da Lei Federal nº 14.133/2021.

15.2. O contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

15.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

CLÁUSULA DÉCIMA SEXTA – DOS CASOS OMISSOS

16.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei Federal nº 14.133/2021 e demais normas aplicáveis.

CLÁUSULA DÉCIMA SÉTIMA – DAS DISPOSIÇÕES ESPECIAIS

17.1. Se qualquer das partes relevar eventual falta relacionada com a execução deste contrato, tal fato não significa liberação ou desoneração a qualquer delas.

17.2. No caso de ocorrer greve de caráter reivindicatório entre os empregados do contratado ou de seus subcontratados, cabe a ele resolver imediatamente a pendência.

17.3. As partes considerarão cumprido o contrato quando todas as obrigações aqui estipuladas estiverem efetivamente satisfeitas, nos termos de direito e aceitas pelo contratante.

17.4. Haverá consulta prévia ao CADIN/RS, pelo órgão ou entidade competente, nos termos da Lei nº 10.697/1996, regulamentada pelo Decreto nº 36.888/1996.

17.5. O presente contrato somente terá eficácia após a assinatura das partes e divulgação no Portal Nacional de Contratações Públicas.

17.5.1. Nos casos de urgência, a eficácia se dará a partir da assinatura das partes, permanecendo a exigência da divulgação no PNCP no prazo de 10 dias úteis.

CLÁUSULA DÉCIMA OITAVA - DAS DISPOSIÇÕES FINAIS

18.1. Fica eleito o Foro de Porto Alegre, como o competente para dirimir quaisquer questões advindas deste contrato, com renúncia expressa a qualquer outro.

18.2. E, assim, por estarem as partes ajustadas e acordadas, assinam este contrato na forma eletrônica, para que produza seus jurídicos efeitos.

MARIA EMÍLIA MOURA DA SILVA	NOME
Desembargadora Militar-Presidente	Representante Legal
Tribunal de Justiça Militar/RS	Empresa

ANEXO II – MODELO DE PROPOSTA DE PREÇOS

Item	Descrição	Qt.	Um.	Valor Unit.	Valor Total

1. DADOS DA EMPRESA

- a) Razão social da empresa, endereço, telefone e e-mail
- b) Número de inscrição no CNPJ (o mesmo constante dos documentos de habilitação e das notas fiscais a serem emitidas)
- c) Nome e telefone da pessoa indicada para contatos
- d) Nome e CPF do representante legal

2. DECLARAÇÕES SOBRE A PROPOSTA DE PREÇOS

2.1. A proponente, acima qualificada, declara que:

- a) Os preços aqui propostos compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta aplicáveis e vigentes nesta data;
- b) Nos preços aqui propostos estão incluídas quaisquer vantagens, abatimentos, impostos, taxas e contribuições sociais, obrigações trabalhistas, previdenciárias, fiscais e comerciais, que eventualmente incidam sobre a operação, além das despesas com transporte ou terceiros;
- c) A presente proposta de preços permanecerá válida por, no mínimo, 60 (sessenta) dias, a contar desta data.

3. DOCUMENTAÇÃO COMPLEMENTAR À PROPOSTA DE PREÇOS

3.1. Documentação técnica:

3.1.1. A licitante classificada provisoriamente em primeiro lugar deverá enviar, acompanhando a sua proposta de preços final, sob pena de desclassificação, um conjunto de documentos técnicos que comprove o atendimento integral de todos os requisitos técnicos dos produtos a serem fornecidos.

3.1.2. Serão aceitas as seguintes formas de apresentação da documentação a ser entregue pela proponente para fins de comprovação do atendimento de cada um dos requisitos técnicos do objeto:

- a) Catálogos, prospectos, folhetos, manuais e outros documentos emitidos pelo fabricante, em língua portuguesa (para objetos relacionados à tecnologia da informação, são também admitidos documentos em língua inglesa);
- b) Documentação oficial emitida pelo fabricante, para os casos em que não seja possível a comprovação das características técnicas por meio dos documentos anteriormente relacionados;
- c) Documentos obtidos pela Internet no site do fabricante, com a impressão das páginas, contendo a indicação do endereço URL em que foram obtidos.

3.1.3. Nos casos em que os documentos mencionados acima forem omissos quanto a alguma característica exigida, a declaração de conformidade do fabricante será suficiente para a avaliação da proposta.

3.1.4. Não serão aceitas declarações do fabricante que afirmem que os produtos propostos atendem às especificações técnicas do edital em sua integralidade, assim como documentos, folhetos, prospectos, impressos de qualquer natureza ou páginas da Internet produzidas com a finalidade específica de possibilitar a qualificação técnica da proposta da licitante, nem será válida a mera indicação do site do fabricante, mas sim o endereço específico que contenha a informação comprobatória do atendimento dos requisitos técnicos.

Local e data,/...../.....

Nome, assinatura, telefone e e-mail do representante legal

ANEXO III – MODELO DE DECLARAÇÃO PARA HABILITAÇÃO

....., inscrita no CNPJ sob nº, por intermédio de seu representante legal,
o(a) Sr.(a)
....., portador(a) da Carteira de Identidade nº e inscrito no CPF sob nº
.....,

DECLARA:

- a) que cumpre plenamente os requisitos de habilitação;
- b) que até a presente data inexistem fatos impeditivos à sua habilitação no presente processo licitatório;
- c) que não foi considerada inidônea por nenhum órgão da Administração Pública;
- d) que não está descumprindo o disposto no art. 7º, inciso XXXIII, da Constituição Federal;
- e) que, no caso de enquadramento, atende ao disposto no art. 93 da Lei nº 8.213/1991, preenchendo o percentual exigido dos seus cargos com beneficiários da Previdência Social reabilitados ou pessoas portadoras de deficiência, habilitadas;
- f) que, caso vencedora, solicitará, se ainda não possuir, cadastro na Secretaria da Fazenda do Estado do Rio Grande do Sul, para fins de comprovação de regularidade perante o fisco estadual, como condição para assinatura do contrato ou emissão de instrumento equivalente, no prazo de 5 (cinco) dias úteis contados da homologação da licitação.

Local e data

Nome e assinatura do representante legal

ANEXO IV – MODELO DE DECLARAÇÃO DE COMPOSIÇÃO SOCIETÁRIA E DE NEPOTISMO

....., CNPJ nº, por seu representante legal, , CPF nº, declara, para fins de participação no procedimento licitatório deflagrado pelo edital _____, que: **(i) não incide** no impedimento de contratação previsto no art. 14 da Lei nº 14.133/2021, **não possuindo em seu quadro societário** servidor ou dirigente de órgão ou entidade contratante ou responsável pela licitação, bem como, em observância aos termos da Resolução nº 07/2005 do Conselho Nacional de Justiça, **(ii) não tem em seu quadro societário** cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, dos magistrados ocupantes de cargos de direção ou no exercício de funções administrativas, assim como de servidores ocupantes de cargos de direção, chefia e assessoramento vinculados direta ou indiretamente às unidades situadas na linha hierárquica da área encarregada da licitação. **a vedação constante do item "ii" se estende às contratações cujo procedimento licitatório tenha sido deflagrado quando os magistrados e servidores geradores de incompatibilidade estavam no exercício dos respectivos cargos e funções, assim como às licitações iniciadas até 6 (seis) meses após a desincompatibilização.**

Local e data

Nome e assinatura do representante legal

ANEXO V- TERMO DE REFERÊNCIA - TR

FAMÍLIAS CELIC: 400 e/ou 117

LOTE 01

A. DEFINIÇÃO DO OBJETO

O objeto deste Termo de Referência consiste na contratação de empresa(s) especializada(s) para a renovação da licença da solução de antivírus Kaspersky Endpoint Security com upgrade do licenciamento Kaspersky Select para a versão Kaspersky endpoint Detection and Response Optimun (EDR), pelo período de 36 (trinta e seis) meses. Esta contratação inclui a atualização de versões e suporte técnico, visando atender às necessidades do Tribunal de Justiça Militar do Estado do Rio Grande do Sul (TJM/RS), da 1ª Auditoria Militar, da 2ª Auditoria Militar, da Auditoria Militar de Santa Maria/RS e da Auditoria Militar de Passo Fundo/RS, nos termos da tabela abaixo e conforme as condições, quantidades e exigências estabelecidas neste Termo de Referência.

OBJETO	Quantidade Licenças	Preço de Referência R\$	Total Estimado R\$
Lote 1. Contratação de empresa(s) especializada(s) para a renovação da licença da solução de antivírus Kaspersky Endpoint Security - pelo período de 36 (trinta e seis) meses, incluindo atualização de versões e suporte.	212	421,98	89.881,21
2. Solução de proteção, detecção e resposta a incidente de endpoint; 2.1. Servidor de Administração e Console Gerenciamento 2.1.1. Compatibilidade: 2.1.1.1. Microsoft Storage Server 2012 e Server R2 x64; 2.1.1.2. Microsoft Windows Server 2012 e R2 Standard / Core / Datacenter x64; 2.1.1.3. Microsoft Windows Server 2016 Standard / Core / Datacenter x64; 2.1.1.4. Microsoft Windows Server 2019 Standard / Core / Datacenter x64; 2.1.1.5. Microsoft Windows Server 2022			

Standard / Core / Datacenter x64;

2.1.1.6. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;

2.1.1.7. Microsoft Windows 8 Professional / Enterprise x64;

2.1.1.8. Microsoft Windows 8.1 Professional / Enterprise x32/x64;

2.1.1.9. Microsoft Windows 10 x32/x64;

2.1.1.10. Windows 11 Home / Pro / Enterprise / Education x64;

2.1.2. Suporta as seguintes plataformas virtuais:

1.2.1. Vmware: Workstation 16 Pro, vSphere 6.7, vSphere 7.0;

1.2.2. Microsoft Hyper-V: 2012, 2012 R2, 2016, 2019 x64 e 2022 x64;

1.2.5. Parallels Desktop 17;

1.2.7. Citrix XenServer 7.1, 8.x;

1.2.8. Oracle VM VirtualBox 6;

2.1.3. Características:

2.1.3.1. O console deve ser acessado via WEB (HTTPS) ou MMC;

2.1.3.2. O console deve suportar arquitetura on-premise e arquitetura cloud-based;

2.1.3.3. Console deve ser baseado no modelo cliente/servidor;

2.1.3.4. O console deve suportar autenticação de dois fatores;

2.1.3.5. Deve possuir compatibilidade com Windows Failover Clustering;

2.1.3.6. O servidor de administração deve possuir modelo de cluster ativo-passivo;

2.1.3.7. Deve permitir a atribuição de perfis para os administradores da solução de Antivírus;

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

2.1.3.9. Console deve ser totalmente integrado com suas funções e módulos, caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, gerenciamento de vulnerabilidades, detecção e resposta de endpoint, avaliação de vulnerabilidades, gerenciamento de dispositivos moveis;

2.1.3.10. 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;

2.1.3.11. Deverá ser possível buscar novos produtos e soluções a partir da console;

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

2.1.3.13. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, através da console de gerenciamento e GPO de AD.

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

2.1.3.15. Deve armazenar histórico das alterações feitas em políticas;

2.1.3.16. 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;

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

2.1.3.18. A solução de gerencia deve permitir,

através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

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

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

2.1.3.21 Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por sub-rede com os seguintes parâmetros: KB/s e horário;

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

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

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

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

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

2.1.3.27. 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;

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

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

2.1.3.30. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

- Nome do computador;
- Nome do domínio;
- Range de IP;
- Sistema Operacional;
- Máquina virtual.

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

2.1.3.32. Deve ter a capacidade de descobrir novos dispositivos na rede, utilizando as seguintes técnicas:

2.1.3.32.1. Pesquisa de rede (Windows pooling);

2.1.3.32.2. Pesquisa ativa do AD (AD pooling);

2.1.3.32.3. Pesquisa de IP (IP pooling);

2.1.3.32.4. Pesquisa de rede (Zeroconf pooling);

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

2.1.3.34. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;

2.1.3.35. 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 ser adicionada a proteção;

2.1.3.36. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets 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;

2.1.3.37. 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 2 dias, etc;

2.1.3.38. 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;

2.1.3.39. Deve fornecer as seguintes informações dos computadores:

2.1.3.39.1. Se o antivírus está instalado;

2.1.3.39.2. Se o antivírus está iniciado;

2.1.3.39.3. Se o antivírus está atualizado;

2.1.3.39.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;

2.1.3.39.5. Minutos/horas desde a última atualização de vacinas;

2.1.3.39.6. Data e horário da última verificação executada na máquina;

2.1.3.39.7. Versão do antivírus instalado na máquina;

2.1.3.39.8. Se for necessário reiniciar o computador para aplicar mudanças;

2.1.3.39.9. Quantidade de vírus encontrados (contador) na máquina;

2.1.3.39.10. Nome do computador;

2.1.3.39.11. Domínio ou grupo de trabalho do computador;

2.1.3.39.12. Data e horário da última atualização de vacinas;

2.1.3.39.13. Sistema operacional com Service Pack;

2.1.3.39.14. Quantidade de processadores;

2.1.3.39.15. Quantidade de memória RAM;

2.1.3.39.16. Sessões de usuários, com informações de contato (caso disponível no Active Directory);

2.1.3.39.17. Endereço IP;

2.1.3.39.18. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;

2.1.3.39.19. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD e placa mãe;

2.1.3.39.20. Vulnerabilidades de aplicativos instalados na máquina;

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

2.1.3.41. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

2.1.3.41.1. Alteração de Gateway Padrão;

2.1.3.41.2. Alteração de sub-rede;

2.1.3.41.3. Alteração de domínio;

2.1.3.41.4. Alteração de servidor DHCP;

2.1.3.41.5. Alteração de servidor DNS;

2.1.3.41.6. Alteração de servidor WINS;

2.1.3.41.7. Resolução de Nome;

2.1.3.41.8. Disponibilidade de endereço de conexão SSL;

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

2.1.3.43. Capacidade de instalar outros servidores administrativos para balancear a

carga e aperfeiçoar tráfego de link entre sites diferentes;

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

2.1.3.45. O console de gerenciamento deve suportar funções de controle de acesso com base na função (RBAC) para a hierarquia de servidores;

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

2.1.3.47. Capacidade de herança de configuração de tarefas, políticas e relatórios na estrutura de hierarquia de servidores on-premisse com servidor em cloud.

2.1.3.48. 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 aperfeiçoar tráfego da rede;

2.1.3.49. 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;

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

2.1.3.51. Capacidade de monitoramento do sistema através de um SNMP client;

2.1.3.52. Capacidade enviar eventos através de protocolo de syslog;

2.1.3.53. Capacidade exportar eventos para sistemas de SIEM no formato LEEF e CEF.

2.1.3.54. Deve ser capaz de enviar os eventos

para sistemas de SIEM em canal encriptado.

2.1.3.55. Dever ter a capacidade de exportar eventos para sistemas de SIEM, compatível com Qradar, ArcSight e Splunk.

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

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

2.1.3.58. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e sub-rede;

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

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

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

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

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

2.1.3.64. 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;

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

2.1.3.66. 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.

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

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

2.1.3.69. Deve criar um backup de todos os arquivos deletados em computadores durante a desinfecção para que possam ser restaurados;

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

2.1.3.71. Capacidade de realizar resumo de hardware de cada máquina cliente;

2.1.3.72. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

2.2. Sistemas operacionais Windows

2.2.1. Deve ser compatível com os seguintes sistemas de estação de trabalho:

2.2.1.1. Microsoft Windows 7
Home/Professional/Enterprise/Ultimate SP1;

2.2.1.2. Microsoft Windows 8

Professional/Enterprise;

2.2.1.3. Microsoft Windows 8.1 Professional / Enterprise;

2.2.1.4. Microsoft Windows 10 Pro / Enterprise / Home / Education;

2.2.1.5. Microsoft Windows 11 Pro / Enterprise / Home / Education;

2.2.2. Deve ser compatível com os seguintes sistemas servidores:

2.2.2.1. Windows Small Business Server 2011 Essentials / Standard (64-bit)

2.2.2.2. Windows MultiPoint Server 2011 (64-bit);

2.2.2.3. Windows Server 2008 R2 Standard/Enterprise/Datacenter SP 1 e superior;

2.2.2.4. Windows Server 2012 e R2 Foundation / Essentials / Standard / Datacenter;

2.2.2.5. Windows Server 2016 Essentials / Standard / Datacenter;

2.2.2.6. Windows Server 2019 Essentials / Standard / Datacenter;

2.2.2.7. Windows Server 2022.

2.2.3. Suporta as seguintes plataformas virtuais:

2.2.3.1. VMware Workstation 16.2.3;

2.2.3.2. VMware ESXi 7.0 Update 3d;

2.2.3.3. Microsoft Hyper-V Server 2019;

2.2.3.4. Citrix Virtual Apps and Desktops 7 2203;

2.2.3.5. Citrix Provisioning 2203;

2.2.3.6. Citrix Hypervisor 8.2.

2.3. Características:

2.3.1.1. Deve prover as seguintes proteções:

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

modificado;

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

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

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

2.3.1.1.5. Deve possuir módulo dedicado contra prevenção de intrusão, Prevenção de intrusão do host;

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

2.3.1.1.7. Controle de dispositivos externos;

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

2.3.1.1.9. Controle de acesso a sites por horário;

2.3.1.1.10. Controle de acesso a sites por usuários;

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

2.3.1.1.12. Controle de execução de aplicativos;

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

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

2.3.1.3. 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);

2.3.1.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar

incompatibilidade, bloqueando a instalação;

2.3.1.5. 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;

2.3.1.6. 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;

2.3.1.7. Deverá possuir módulo dedicado para proteção contra port scanning;

2.3.1.8. Deverá possuir módulo dedicado para proteção contra network flooding;

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

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

2.3.1.11. 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;

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

2.3.1.13. Deverá possuir módulo para proteção contra malwares que tenta realizar criptografia de arquivos em pastas compartilhadas.

2.3.1.14. Deve ter a capacidade de detectar ameaças instaladas na BIOS ROM do endpoint.

2.3.1.15. Deverá realizar scanner de firmware

em busca de rootkits.

2.3.1.16. Ao detectar uma ameaça, a solução deve exibir informações:

2.3.1.17. Do objeto SHA256;

2.3.1.18. Do objeto MD5.

2.3.1.19. Capacidade de verificar somente arquivos novos e alterados;

2.3.1.20. Capacidade de verificar objetos usando heurística;

2.3.1.21. Capacidade de agendar uma pausa na verificação;

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

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

2.3.1.24. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.3.1.24.1. Perguntar o que fazer, ou;

2.3.1.24.2. Bloquear acesso ao objeto;

2.3.1.24.2.1. Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);

2.3.1.24.2.2. Caso positivo de desinfecção:

2.3.1.24.2.2.1. Restaurar o objeto para uso;

2.3.1.24.2.3. Caso negativo de desinfecção:

2.3.1.24.2.3.1. Mover para uma área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

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

2.3.1.26. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;

2.3.1.27. Capacidade de verificar links inseridos

em e-mails contra phishings;

2.3.1.28. Capacidade de verificar todo o tráfego web de acessos à internet nos protocolos HTTP, HTTPS e FTP, utilizando técnicas de banco de dados, serviços da nuvem do fabricante e análise de heurística bloqueada arquivos, sites de phishing e URL maliciosas;

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

2.3.1.30. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

2.3.1.30.1. Perguntar o que fazer, ou;

2.3.1.30.2. Bloquear o e-mail;

2.3.1.30.2.1. Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);

2.3.1.30.2.2. Caso positivo de desinfecção:

2.3.1.30.2.3. Restaurar o e-mail para o usuário;

2.3.1.30.2.4. Caso negativo de desinfecção:

2.3.1.30.2.4.1. Mover para uma área de backup ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

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

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

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

2.3.1.34. Deve ser possível realizar o monitoramento das atividades de rede em tempo real, visualizando portas UDP/TCP e Tráfego de rede por aplicativo.

2.3.1.35. Capacidade de alterar as portas monitoradas pelos módulos de ameaças web, controle de acesso à web e e-mail;

2.3.1.36. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

2.3.1.36.1. Perguntar o que fazer, ou;

2.3.1.36.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

2.3.1.36.3. Permitir acesso ao objeto;

2.3.1.37. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

2.3.1.37.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;

2.3.1.37.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;

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

2.3.1.39. 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;

2.3.1.40. 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;

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

2.3.1.42. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

2.3.1.43. Deve possuir módulo para proteção contra port scans, network flooding e MAC

spoofing. A base de dados de análise deve ser atualizada juntamente com as vacinas;

2.3.1.44. Deve permitir a importação e exportação de listas de regras e exclusões para as aplicações no formato XML;

2.3.1.45. Deve permitir a criação de zonas confiáveis locais independentes por parte do usuário.

2.3.1.46. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

2.3.1.46.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

2.3.1.46.2. 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.

2.3.1.47 Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

2.3.1.47.1. Discos de armazenamento locais;

2.3.1.47.2. Armazenamento removível;

2.3.1.47.3. Impressoras;

2.3.1.47.4. CD/DVD;

2.3.1.47.5. Modems;

2.3.1.47.6. Dispositivos multifuncionais;

2.3.1.47.7. Leitores de smart card;

2.3.1.47.8. Wi-Fi;

2.3.1.47.9. Adaptadores de rede externos;

2.3.1.47.10. Dispositivos MP3 ou smartphones;

2.3.1.47.11. Dispositivos Bluetooth;

2.3.1.47.12. Câmeras e Scanners.

2.3.1.48. Capacidade de liberar acesso a um

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

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

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

2.3.1.51. Deve permitir controlar o acesso a dispositivos externos com base em prioridade de regras.

2.3.1.52. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos, etc.

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

2.3.1.54. 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);

2.3.1.55. Ter a capacidade de detectar a modificação de firmware em dispositivos USB mal-intencionado.

2.3.1.56. Deverá realizar a validação dos dispositivos que se conectam via USB que emulam teclados;

2.3.1.57. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

2.3.1.57.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.3.1.57.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas

por regras.

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

2.3.1.59. 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;

2.3.1.60. 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;

2.3.1.61. 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.

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

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

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

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

2.3.1.66. Deve permitir realizar o gerenciamento por meio de integração via REST API.

2.3.1.67. Deve permitir o gerenciamento remoto da solução por meio de aplicativos de administração remota.

2.4. Estações Mac OS X

2.4.1. Compatibilidade:

2.4.1.1. macOS Mojave 10.14

2.4.1.2. macOS Catalina 10.15

2.4.1.3. macOS Big Sur 11.0

2.4.1.4. macOS Monterey 12

2.4.2. Características:

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

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

2.4.2.3. Possuir módulo de bloqueio á ataques na rede;

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

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

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

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

2.4.2.8. 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);

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

2.4.2.10. 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;

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

2.4.2.12. 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;

2.4.2.13. Capacidade de verificar somente arquivos novos e alterados;

2.4.2.14. Capacidade de verificar objetos usando heurística;

2.4.2.15. Capacidade de agendar uma pausa na verificação;

2.4.2.16. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.4.2.16.1. Perguntar o que fazer, ou;

2.4.2.16.2. Bloquear acesso ao objeto;

2.4.2.16.2.1. Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);

2.4.2.16.2.2. Caso positivo de desinfecção:

2.4.2.16.2.1. Restaurar o objeto para uso;

2.4.2.16.2.2. Caso negativo de desinfecção:

2.4.2.16.2.3. Mover para área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

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

2.4.2.18. Capacidade de verificar arquivos de formato de email;

2.4.2.18. 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;

2.4.2.19. Capacidade de, através da mesma console central de gerenciamento:

2.4.2.19.1. Ser instalado;

2.4.2.19.2. Ser removido;

2.4.2.19.3. Ser gerenciado;

2.5. Sistemas operacionais Linux

2.5.1. Compatibilidade:

2.5.1.1. Plataforma 32-bits:

2.5.1.1.1. Red Hat Linux 6.7 e superior;

2.5.1.1.2. CentOS 6.7 e superior;

2.5.1.1.3. Debian 9.4 e superior;

2.5.1.1.4. Debian 10.1 e superior;

2.5.1.1.5. Debian 11.1 e superior;

2.5.1.1.6. Linux Mint 19 e superior;

2.5.1.1.7. Mageia 4;

2.5.1.2. Plataforma 64-bits:

2.5.1.2.1. Ubuntu 18.04 e superior;

2.5.1.2.2. Ubuntu 20.04;

2.5.1.2.3. Red Hat Enterprise Linux 6.7;

2.5.1.2.4. Red Hat Enterprise Linux 7.2;

2.5.1.2.5. Red Hat Enterprise Linux 8.0;

2.5.1.2.6. CentOS 6.7 e superior;

2.5.1.2.7. CentOS 7.2 e superior;

2.5.1.2.8. CentOS 8.0 e superior;

2.5.1.2.9. Debian 9.4 e superior;

2.5.1.2.10. Debian 10.1 e superior;

2.5.1.2.11. OracleLinux 7.3 e superior;

2.5.1.2.12. OracleLinux 8 e superior;

2.5.1.2.13. SUSE Server 12 e superior;

2.5.1.2.14. SUSE Server 15 e superior;

- 2.5.1.2.15. openSUSE Leap 15;
- 2.5.1.2.16. Amazon Linux 2;
- 2.5.1.2.17. Linux Mint 19 e superior;
- 2.5.1.2.18. Linux Mint 20.1 e superior;
- 2.5.1.2.19. Oracle Linux 7.3 e superior;
- 2.5.1.2.20. Oracle Linux 8.0 e superior;
- 2.5.1.2.21. RED OS 7.2;

2.6. Características:

- 2.6.1.1. Deve prover as seguintes proteções:
- 2.6.1.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- 2.6.1.3. Deve permitir gerenciamento, no mínimo, das seguintes formas:
 - 2.6.1.3.1. Via linha de comando;
 - 2.6.1.3.2. Via console administrativa;
 - 2.6.1.3.3. Via GUI;
 - 2.6.1.3.4. Via web (remotamente);
- 2.6.1.4. Deve possuir funcionalidade de scan de drives removíveis, tais como:
 - 2.6.1.4.1. CDs;
 - 2.6.1.4.2. DVDs;
 - 2.6.1.4.3. Discos blu-ray;
 - 2.6.1.4.4. Flash drives (pen drives);
 - 2.6.1.4.5. HDs externos;
 - 2.6.1.4.6. Disquetes;
- 2.6.1.5. Deve fornecer os seguintes controles para dispositivos externos conectados ao computador:
 - 2.6.1.5.1. Por tipo de dispositivo;
 - 2.6.1.5.2. Por barramento de conexão.
- 2.6.1.6. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
- 2.6.1.7. Capacidade de configurar a permissão

de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

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

2.6.1.7.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

2.6.1.7.3. Leitura de configurações;

2.6.1.7.4. Modificação de configurações;

2.6.1.7.5. Gerenciamento de Backup;

2.6.1.7.6. Visualização de logs;

2.6.1.7.7. Gerenciamento de logs;

2.6.1.7.8. Gerenciamento de ativação da aplicação;

2.6.1.7.9. Gerenciamento de permissões (adicionar/excluir permissões acima);

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

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

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

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

2.6.1.12. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

2.6.1.12.1. Alta;

2.6.1.12.2. Média;

2.6.1.12.3. Baixa;

2.6.1.12.4. Recomendado;

2.6.1.13. Gerenciamento de backup de arquivos: Fazer backup de objetos suspeitos e corrompidos, salvando tais arquivos em uma

pasta de backup;

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

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

2.6.1.16. Capacidade de definir o consumo de recursos nas varreduras para não impactar outros aplicativos que necessitem de mais recursos de memória ou processamento;

2.6.1.17. Deverá ser possível priorizar a execução de tarefas;

2.6.1.18. Capacidade de verificar objetos usando heurística;

2.6.1.19. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em malicioso;

2.6.1.20. Deve fornecer análise de todo o tráfego HTTP/HTTPS/FTP;

2.6.1.21. O módulo de análise de tráfego deve fornecer os seguintes componentes de proteção:

2.6.1.21.1. Detecção de phishing e sites maliciosos;

2.6.1.21.2. Bloqueio de download de arquivos maliciosos;

2.6.1.21.3. Bloqueio de adware;

2.6.1.21.4. Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

2.6.1.22. Deve fornecer a possibilidade de administração remota através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux);

2.6.1.23. Deverá fornecer informações de todas as executáveis das aplicações;

2.6.1.24. Deve possuir módulo de proteção contra criptografia maliciosa.

2.6.1.25. Deverá possuir controle de execução de aplicações;

2.6.1.26. O módulo de controle de aplicação deverá possuir as seguintes funcionalidades:

2.6.1.26.1. Criação de lista de bloqueio de aplicação;

2.6.1.26.2. Criação de lista de permissão de aplicação;

2.6.1.27. Deverá realizar busca de ameaças em setores críticos do sistema operacional:

2.6.1.27.1. Setor de inicialização;

2.6.1.27.2. Objetos de inicialização;

2.6.1.27.3. Processos de memória;

2.6.1.27.4. Memória do kernel;

2.7. Compatibilidade com servidores windows;

2.7.1. Compatibilidade de sistema legado:

2.7.2. Plataforma x32 ou x64:

2.7.2.1. Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;

2.7.2.2. Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;

2.7.3. Características:

2.7.3.1. Deve prover as seguintes proteções:

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

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

2.7.3.1.3. Firewall com IDS;

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

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

2.7.3.3. Deve permitir gerenciamento, no mínimo, das seguintes formas:

2.7.3.3.1. Via console administrativo;

2.7.3.3.2. Via web (remotamente);

2.7.3.4. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

2.7.3.5. Deverá ter a capacidade de customizar o uso de CPU para realização de scanner no dispositivo.

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

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

2.7.3.6.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

2.7.3.6.3. Leitura de configurações;

2.7.3.6.4. Modificação de configurações;

2.7.3.6.5. Gerenciamento de backup;

2.7.3.6.6. Visualização de logs;

2.7.3.6.7. Gerenciamento de logs;

2.7.3.6.8. Gerenciamento de ativação da aplicação;

2.7.3.6.9. Gerenciamento de permissões (adicionar/excluir permissões acima);

2.7.3.6.10. Deve possuir bloqueio de inicialização de aplicativos baseado em whitelists.

2.7.3.7. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

2.7.3.7.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

2.7.3.7.2. 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.

2.7.3.8. 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;

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

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

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

2.7.3.12. Deve possuir funcionalidade de análise personalizada de logs do Windows.

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

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

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

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

2.7.3.17. 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;

2.7.3.18. 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;

2.7.3.19. Capacidade de verificar somente arquivos novos e alterados;

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

2.7.3.21. Capacidade de verificar objetos usando heurística;

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

2.7.3.23. Capacidade de agendar uma pausa na verificação;

2.7.3.24. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.7.3.24.1. Perguntar o que fazer, ou;

2.7.3.24.2. Bloquear acesso ao objeto;

2.7.3.24.2.1. Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);

2.7.3.24.2.2. Caso positivo de desinfecção:

2.7.3.24.2.2.1. Restaurar o objeto para uso;

2.7.3.24.2.3. Caso negativo de desinfecção:

2.7.3.24.2.3.1. Mover para área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

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

2.7.3.26. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos maliciosos em área de backup;

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

2.7.3.28. Em caso de detecção de sinais de uma infecção ativa, deve possuir capacidade de, automaticamente:

2.7.3.28.1. Executar os procedimentos pré-configurados pelo administrador;

2.7.3.28.2. Em caso de ausência de procedimentos pré-configurados, criar tais procedimentos e executá-los.

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

2.7.3.30. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros;

2.7.3.31. Capacidade de detectar anomalias no comportamento de um software usando análise heurística.

2.7.3.32. 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.

2.7.3.33. Deve possuir controle de dispositivos externos.

2.8. Smartphones e tablets

2.8.1. Compatibilidade:

2.8.1. Suportar o Android das versões: 5.0 ao 12.

2.8.2. Características:

2.8.2.1. Deve prover as seguintes proteções:

2.8.2.1.1 Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

2.8.2.1.2. Proteção contra adware e autodialers;

2.8.2.1.3. Todos os objetos transmitidos;

2.8.2.1.4. Arquivos abertos no smartphone;

2.8.2.1.5. Programas instalados usando a interface do smartphone

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

2.8.2.2 Deverão isolar em área de backup os arquivos infectados;

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

2.8.2.4. Capacidade de desativar por política:

2.8.2.4.1. Wi-fi;

2.8.2.4.2. Câmera;

2.8.2.4.3. Bluetooth.

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

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

2.8.2.6. Deverá ter firewall pessoal;

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

2.8.2.7. Capacidade de enviar comandos remotamente de:

2.8.2.7.1. Localizar;

2.8.2.7.2. Bloquear.

2.8.2.7.3. Capacidade de detectar Root nos dispositivos;

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

2.8.2.7.5. Capacidade de bloquear o acesso a sites phishing ou maliciosos;

2.8.2.7.6. Capacidade de configurar White e blacklist de aplicativos;

2.8.2.7.7. Capacidade de localizar o dispositivo quando necessário;

2.8.2.7.8. Permitir atualização das definições quando estiver em "roaming";

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

2.8.2.7.9. Capacidade de agendar uma verificação;

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

2.8.2.7.11. Capacidade de fazer a instalação do agente através de um link QRCode;

2.8.2.7.12. Capacidade de executar as seguintes ações caso a desinfecção falhe:

ü Deletar;

ü Ignorar;

ü Fazer backup;

ü Perguntar ao usuário.

2.8.3. Gerenciamento de dispositivos móveis (MDM) – Android:

2.8.3.1. Compatibilidade:

2.8.3.1.1. Dispositivos com os sistemas operacionais:

2.8.3.1.1.1. Do Android versão 5.0 a 12

2.8.3.1.1.2. Deverá possuir integração com sistemas de gerenciamentos:

2.8.3.1.2.1. VMWare AirWatch 9.3;

2.8.3.1.2.2. MobileIron;

2.8.3.1.2.3. IBM Maas360;

2.8.3.1.2.4. Microsoft Intune;

2.8.3.1.2.5. SOTI MobiControl;

2.8.3.2 Características:

2.8.3.2.1. Capacidade de aplicar políticas de Activesync através do servidor Microsoft Exchange;

2.8.3.2.2. Capacidade de ajustar as configurações de:

2.8.3.2.2.1. Sincronização de e-mail;

2.8.3.2.2.2. Uso de aplicativos;

2.8.3.2.2.3. Senha do usuário;

2.8.3.2.2.4. Criptografia de dados;

2.8.3.2.2.5. Conexão de mídia removível.

2.8.3.2.2.6. Capacidade de instalar certificados digitais em dispositivos móveis;

2.8.3.2.2.7. Deve permitir configurar horário para sincronização do dispositivo com o console de gerenciamento;

2.8.3.2.2.8. Capacidade de desinstalar remotamente o antivírus do dispositivo;

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

2.8.3.2.2.10 Capacidade de sincronizar com Samsung Knox;

2.8.4. Gerenciamento de dispositivos móveis (MDM) – iOS

2.8.4.1. Compatibilidade:

2.8.4.1.1. Ser compatível com dispositivos com os sistemas operacionais:

2.8.4.1.1.1. iOS 10.0 – 10.3.3

2.8.4.1.1.2. iOS 11.0 – 11.3

2.8.4.1.1.3. iOS 12.0

2.8.4.1.1.4. iOS 13.0

2.8.4.1.1.5. iPadOS 13 ao 15

2.8.4.1.2 Características:

2.8.4.1.2.1. Capacidade de aplicar políticas de Activesync através do servidor Microsoft

Exchange;

2.8.4.1.3. Capacidade de ajustar as configurações de:

2.8.4.1.3.1. Sincronização de e-mail;

2.8.4.1.3.2 Senha do usuário;

2.8.4.1.3.3 Criptografia de dados;

2.8.4.1.3.4 Capacidade de instalar certificados digitais em dispositivos móveis;

2.8.4.1.3.5 Capacidade de instalar as ferramentas necessárias para o gerenciamento dos dispositivos clientes através de:

2.8.4.1.3.5.1. Link por e-mail;

2.8.4.1.3.5 .2 Link por mensagem de texto;

2.8.4.1.3.5.3 QR Code

2.8.4.1.3.6 Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;

2.8.4.1.3.7 Capacidade de, remotamente, bloquear um dispositivo iOS;

2.9 Criptografia

2.9.1. Compatibilidade:

2.9.1.2. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;

2.9.1.3. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;

2.9.1.4. Microsoft Windows 7 Professional SP1 ou superior x86/x64;

2.9.1.5. Microsoft Windows 8 Enterprise x86/x64;

2.9.1.6. Microsoft Windows 8 Pro x86/x64;

2.9.1.7. Microsoft Windows 8.1 Pro x86/x64;

2.9.1.8. Microsoft Windows 8.1 Enterprise x86/x64;

2.9.1.9. Microsoft Windows 10 Enterprise x86/x64;

2.9.1.10. Microsoft Windows 10 Pro x86/x64;

2.9.2. Características:

2.9.2.1. 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;

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

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

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

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

2.9.2.6. Deve permitir que o usuário monitore a criptografia do disco ou o processo de descriptografia em tempo real;

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

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

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

2.9.2.10. Criptografar todos os arquivos individualmente;

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

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

2.9.2.13. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem

criptografados automaticamente;

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

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

2.9.4. Verifica compatibilidade de hardware antes de aplicar a criptografia;

2.9.5. Possibilita estabelecer parâmetros para a senha de criptografia;

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

2.9.7. Permite criar exclusões para não criptografar determinados "discos rígidos" através de uma busca por nome do computador ou nome do dispositivo;

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

2.9.9 Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

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

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

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

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

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

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

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

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

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

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

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

2.9.21. Capacidade de fazer "Hardware encryption";

2.10. Gerenciamento de Sistemas

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

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

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

2.10.1.4. 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;

2.10.1.5. Capacidade de gerenciar licenças de softwares de terceiros;

2.10.1.6. Capacidade de atualizar informações sobre hardware presentes nos relatórios após mudanças de hardware nas máquinas gerenciadas;

2.10.1.7. Capacidade de gerenciar um inventário

de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc);

2.10.2 Possibilita fazer distribuição de software de forma manual e agendada;

2.10.3 Suporta modo de instalação silenciosa;

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

2.10.1.5 Possibilita fazer a distribuição através de agentes de atualização;

2.10.1.6 Utiliza tecnologia multicast para evitar tráfego na rede;

2.10.1.7 Possibilita criar um inventário centralizado de imagens;

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

2.10.1.9. Suporte a WakeOnLan para deploy de imagens;

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

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

2.10.1.12 Capacidade de gerar relatórios de vulnerabilidades e patches;

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

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

2.10.1.15 Permite baixar atualizações para o computador sem efetuar a instalação;

2.10.1.16 Permite o administrador instalar

somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;

2.10.1.17 Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;

2.10.1.18 Permite selecionar produtos a serem atualizados pela console de gerenciamento;

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

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

2.10.1.20 Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;

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

2.10.1.22 Deve permitir selecionar o idioma das aplicações que serão atualizadas;

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

2.11 Detecção e Resposta

2.11.1. Compatibilidade:

2.11.1.1 Deve ser compatível com os seguintes sistemas de estação de trabalho:

2.11.1.1.1 Microsoft Windows 7 Home/Professional/Enterprise/Ultimate SP1;

2.11.1.1.2 Microsoft Windows 8 Professional/Enterprise;

2.11.1.1.3 Microsoft Windows 8.1 Professional / Enterprise;

2.11.1.1.4 Microsoft Windows 10 Pro / Enterprise / Home / Education;

2.11.1.1.5 Microsoft Windows 11 Pro / Enterprise / Home / Education;

2.11.1.1.6 Deve ser compatível com os seguintes sistemas servidores:

2.11.1.1.6.1 Windows Small Business Server 2011 Essentials / Standard (64-bit)

2.11.1.1.6.2. Windows MultiPoint Server 2011 (64-bit);

2.11.1.1.6.3. Windows Server 2008 R2 Standard/Enterprise/Datacenter SP 1 e superior;

2.11.1.1.6.4. Windows Server 2012 e R2 Foundation / Essentials / Standard / Datacenter;

2.11.1.1.6.5. Windows Server 2016 Essentials / Standard / Datacenter;

2.11.1.1.6.6. Windows Server 2019 Essentials / Standard / Datacenter;

2.11.1.1.6.7. Windows Server 2022.

2.11.2. Características

2.11.2.1 As funcionalidades relacionadas a detecção e resposta solicitadas nesse item, devem ser operadas na mesma console de gerenciamento da solução de endpoint;

2.11.2.2 A solução deve oferecer módulo focado em capacidades de EDR "Endpoint Detection and Response", incluindo no mínimo as seguintes capacidades:

2.11.2.3 O agente deve ter capacidade de coletar e processar dados relacionados ao veredito e ao contexto da ameaça;

2.11.2.4 Deve fornecer graficamente a visualização da cadeia do ataque;

2.11.2.5 Deve possuir a capacidade de varredura, para identificar a presença de um artefato detectado em outros dispositivos na rede, através de indicadores de comprometimento (IoC).

2.11.3. A varredura deve oferecer opções de resposta automatizada (sem intervenção do administrador), para serem executadas caso o IoC seja encontrado em outro dispositivo, com no mínimo as seguintes opções:

2.11.3.1. Isolar o host;

2.11.3.2. Iniciar uma varredura nas áreas críticas;

2.11.3.3. Quarentenar o objeto;

2.11.4 A solução deve criar um report detalhado sobre o incidente, tendo a capacidade de incluir no mínimo os seguintes dados:

2.11.5 Visibilidade das detecções provenientes de endpoint;

2.11.5.1. Processos;

2.11.5.2. Conexões remotas;

2.11.5.3 Alterações de registros;

2.11.5.4 Objetos baixados

2.11.6 Capacidade de integração com a solução de sandbox cloud do fabricante;

2.11.7 Varredura por todos os dispositivos executada a partir de indicador de comprometimento (IoC) gerado através da solução e importado pelo administrador.

2.11.8 Deverá possuir informações de assinaturas digitais da ameaça;

2.11.9 Deve ser capaz de trazer informações do arquivo sobre sua geolocalização;

2.11.10 Possibilidade de informar quando o arquivo foi detectado pela base de conhecimento;

2.11.11 Trazer a identificação de comportamento e/ou descrição sobre o arquivo;

2.11.12 A solução deve oferecer no mínimo as seguintes opções de resposta:

2.11.12.1 Prevenir a execução de um arquivo;

2.11.12.2. Quarentenar um arquivo;

<p>2.11.12.3. Iniciar uma varredura por IoC;</p> <p>2.11.12.4. Parar um processo;</p> <p>2.11.12.5. Executar um processo;</p> <p>2.11.13 Ferramenta que possibilite o isolamento do host infectado com no mínimo as características abaixo:</p> <p>2.11.13.1 A opção de isolamento deve estar disponível junto a visualização do incidente;</p> <p>2.11.13.2 Na análise do incidente a ferramenta deverá apresentar recomendações de ações que o analista precisa executar para remediar o incidente;</p> <p>2.11.13.3 As recomendações devem ser guiadas juntamente com guias das opções selecionadas pelo analista, apresentando pop-up guiando as ações.</p> <p>2.11.13.4 Deverá ser possível remover a máquina do isolamento a partir do incidente;</p> <p>2.11.13.5 Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra;</p> <p>2.11.13.6 Deve oferecer informações de inteligência de ameaças do próprio fabricante;</p> <p>2.11.13.7 Deverá possuir detecção baseada em sandbox do tipo cloud;</p> <p>2.11.13. 8 Deverá suportar IoC de terceiros em formatos OpenIOC.</p>			
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--

O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

O prazo de vigência da contratação será de 36 (trinta e seis) meses, contados a partir da emissão da ordem de fornecimento, podendo ser prorrogado sucessivamente, conforme os limites legais estabelecidos nos artigos 106 e 107 da Lei nº 14.133/2021.

A fixação do prazo de 36 meses alinha-se à dinâmica do setor **detecnologia da informação**, especialmente em relação a **softwares de segurança**, que demandam atualizações frequentes e aprimoramento constante para acompanhar a **rápida evolução tecnológica e novas ameaças cibernéticas**. Tal duração permite um ciclo contratual adequado para garantir a **continuidade do serviço**, evitando-se descontinuidade na proteção e suporte técnico, além de possibilitar uma **melhor gestão orçamentária** e a **manutenção da estabilidade**

operacional da infraestrutura tecnológica do órgão.

B. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

Como foi publicado em março de 2024 pelo TCE-RS, o PCA ainda está sendo elaborado, porém está alinhado com o PPA 2023/2027 e LOA 2025.

C. DESCRIÇÃO DA SOLUÇÃO NA TOTALIDADE CONSIDERANDO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

A descrição da solução como um todo se encontra pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

D. REQUISITOS DA CONTRATAÇÃO

1. Sustentabilidade:

A presente contratação de um serviço baseado em nuvem não se aplica ao impacto ambiental de forma direta, pois a responsabilidade pela infraestrutura física e seu consumo energético recai sobre os fornecedores de serviços em nuvem. Esses provedores utilizam data centers aprimorados e frequentemente adotam práticas de eficiência energética e fontes renováveis para reduzir seu impacto ambiental. Portanto, a utilização de serviços em nuvem pelo Tribunal não gera impactos ambientais diretos, uma vez que a operação e manutenção desses recursos não são realizadas internamente.

D.2 Subcontratação:

Não é admitida a subcontratação do objeto contratual.

C.2 Garantia da contratação:

Não haverá exigência da garantia da contratação dos arts. 96 e seguintes da Lei nº 14.133/2021, pelas razões constantes do Estudo Técnico Preliminar.

D. MODELO DE EXECUÇÃO DO OBJETO

E.1. Condições de Entrega

1. O prazo de entrega das licenças de uso do software antivírus é de até 20 (vinte) dias, contados do início do contrato, em remessa única.

2. Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 05 (cinco) dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

3. As licenças, acompanhadas da respectiva Nota Fiscal, deverão ser entregues, no caso de mídia física, no Setor de Tecnologia da Informação do TJMRS, localizado na Avenida Praia de Belas, 799, Porto Alegre- RS, ou, no caso de mídia digital, através do e-mail informatica@tjmrs.jus.br ou eduardo-severo@tjmrs.jus.br, e/ou outro que venha a ser informado pelo fiscal/gestor de contrato. Garantia, manutenção e assistência técnica

4. O prazo de garantia é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

5. A garantia será prestada com vistas a manter as licenças fornecidas em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.

7. A garantia abrange a realização da manutenção corretiva das licenças pelo próprio Contratado, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

8. Uma vez notificado, o Contratado realizará a reparação ou substituição das licenças que apresentarem vício ou defeito no prazo de até 05 (cinco) dias úteis, contados a partir da data de ciência da notificação.

9. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada do Contratado, aceita pelo Contratante.

10. Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do Contratante ou a apresentação de justificativas pelo Contratado, fica o Contratante autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir do Contratado o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.

E.2 Local e horário da prestação dos serviços

O serviço de Gestão de Banco de Dados – GBD é executado nas instalações da Contratada, sendo que a Contratada deverá disponibilizar o serviço durante as 24 (vinte e quatro) horas diárias, nos 7 (sete) dias da semana, ressalvadas as paradas para manutenção ou instalação de equipamentos da Contratada, que deverão ser previamente comunicadas a Coordenadoria de Tecnologia da Informação e Comunicação - TIC - Telefone (51) 3214-1074 e-mail "Coordenadoria de TIC" <informatica@tjmrs.jus.br>, ou "Eduardo Severo" eduardo@tjmrs.jus.br.

E.3 Materiais a serem disponibilizados

Por se tratar da contratação de um serviço em nuvem, não há fornecimento de materiais e equipamentos.

E.4. Especificação da garantia do serviço

Não haverá exigência da garantia da contratação dos arts. 96 e seguintes da Lei nº 14.133/2021, pelas razões constantes do Estudo Técnico Preliminar.

E.5 Procedimentos de transição e finalização do contrato

As exigências abaixo asseguram uma transição suave e eficiente, com a continuidade do serviço e a retenção do conhecimento necessário para a operação:

Revisão do cumprimento do contrato: Verificar se todas as obrigações contratuais foram atendidas, incluindo a entrega de serviços conforme os termos definidos e a conclusão de tarefas específicas.

Auditoria dos resultados: Realizar uma auditoria técnica para avaliar a performance do serviço durante o período contratual, identificando melhorias implementadas, incidentes resolvidos e a qualidade do suporte prestado.

Documentação de transferência: Garantir que todos os dados relevantes e a documentação técnica sejam transferidos para a equipe interna ou o próximo fornecedor, incluindo registros de configurações, planos de manutenção e procedimentos de backup.

Verificação de Segurança: Confirmar a revogação de acessos administrativos e credenciais que o fornecedor utilizou para a gestão do banco de dados, assegurando a proteção e a integridade do ambiente de TI.

Relatórios Finais: Solicitar relatórios finais detalhando as atividades realizadas, os resultados obtidos e as lições aprendidas, para documentar o histórico do contrato.

Desativação de Ferramentas e Acessos: Proceder à desativação de ferramentas ou serviços fornecidos sob o contrato e garantir a remoção de software de monitoramento ou gerenciamento instalado pelo fornecedor.

Transferência de Conhecimento e Capacitação: O contratado deve realizar a transição contratual de forma estruturada, assegurando a transferência de conhecimento, tecnologia e técnicas empregadas durante a execução do serviço, sem perda de informações críticas. Essa transição deve incluir, quando exigido, a capacitação dos técnicos do contratante ou da nova empresa que assumirá a continuidade dos serviços. O objetivo é garantir que a Administração mantenha o domínio sobre os processos e que o novo prestador de serviços possa dar continuidade às operações de forma eficaz e sem interrupções.

Encerramento Formal do Contrato: Conduzir uma reunião de encerramento para confirmar a finalização do serviço e assinar a documentação de término contratual, incluindo a emissão de atestados de execução e certificações de conformidade.

Retenção de Garantias e Obrigações Pós-contratuais: Verificar cláusulas de obrigações pós-contratuais, como períodos de garantia adicional ou suporte pós-fim do contrato, caso aplicável.

F. MODELO DE GESTÃO DO CONTRATO

O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

1. Fiscalização

A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133/2021, art. 117, caput).

O gestor e fiscais técnicos do contrato indicados segue:

Gestor do contrato: EDUARDO BORBA SEVERO

Fiscal técnico titular: JUAREZ BAMBERG DA SILVA

Fiscal técnico suplente: RODRIGO BULLOZA GRUPPELLI

F.1.1- Fiscalização Técnica

O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (IN CAGE Nº 003/2023, de 2022, art. 10, VI);

O fiscal técnico do contrato anotarà no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei 14.133/2021, art. 117, §1º, e IN CAGE Nº 003/2023, de 2022, art. 10, II)

Identificada qualquer inexecução ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Instrução Normativa CAGE Nº 003/2023, de 2022, art. 10, III);

O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Instrução Normativa CAGE Nº 003/2023, de 2022, art. 10, IV).

No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Instrução Normativa CAGE Nº 003/2023, de 2022, art. 10, IV).

O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Instrução Normativa CAGE Nº 003/2023, de 2022, art. 10, V).

F.1.2 Gestor do Contrato

O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (IN CAGE Nº 003/2023, de 2022, art. 9, I).

O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassem a sua competência. (IN CAGE Nº 003/2023, de 2022, art. 9, II).

O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotarà os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Instrução Normativa CAGE Nº 003/2023, de 2022, art. 9, III).

O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Instrução Normativa CAGE Nº 003/2023, de 2022, art. 9 VIII).

O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização

para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Instrução Normativa CAGE Nº 003/2023, de 2022, art. 9 X).

O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Instrução Normativa CAGE Nº 003/2023, de 2022, art. 9 VI).

O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

G. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

A medição será realizada com base na entrega efetiva e validação das licenças contratadas, incluindo os serviços complementares, conforme definido no contrato e no Termo de Referência.

A empresa contratada deve disponibilizar um relatório técnico que comprove:

A entrega e ativação das 212 licenças no ambiente de TI do contratante.

A funcionalidade e integridade da solução instalada, incluindo atualização automática e suporte técnico.

O funcionamento do painel de administração central (se aplicável) para gerenciamento das licenças.

O contratante verificará, por meio de sua equipe técnica, se as licenças foram entregues e definidas de forma correta.

Após a confirmação da entrega, será emitido um relatório de aceite pelo gestor do contrato, autorizando o pagamento.

1.Recebimento

Por se tratar da contratação de um serviço em nuvem não se aplica.

2. Liquidação

Para fins de liquidação, o contratante verificará se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

- o prazo de validade;
- a data da emissão;
- os dados do contrato e do órgão contratante;
- o período respectivo de execução do contrato;
- o valor a pagar; e

eventual destaque do valor de retenções tributárias cabíveis.

Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal mediante consulta aos sítios eletrônicos oficiais ou à documentação

mencionada no art. 68 da Lei nº 14.133, de 2021.

Constatando-se a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação.

3. Forma de pagamento

O pagamento será realizado no valor total da contratação, em parcela única após o recebimento da fatura de serviços por meio de ordem bancária, para crédito em banco, agência e conta correntes indicados pelo contratado.

Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

H. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E FORMA DE FORNECIMENTO

1. Forma de seleção e critério de julgamento da proposta

Trata de uma contratação por pregão eletrônico, menor preço nos termos permitidos pela legislação vigente.

1. Forma de fornecimento

A prestação dos serviços será de forma continuada.

1. Qualificação Econômico-Financeira

Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, incisoII);

1. Qualificação Técnica

Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

Caso admitida a participação de cooperativas, será exigida a seguinte documentação complementar:

A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971;

A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

A comprovação do capital social proporcional ao número de cooperados necessários à execução contratual; O registro previsto na Lei n. 5.764, de 1971, art. 107;

A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato; e

Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa:

- a) ata de fundação;
- b) estatuto social com a ata da assembleia que o aprovou;
- c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia;
- d) editais de convocação das três últimas assembleias gerais extraordinárias;
- e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

I. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

As estimativas de custo para a atualização das licenças de antivírus foi definida com base em pesquisa realizada nos principais sites eletrônicos oficiais de contratações públicas e complementada por cotações obtidas junto a fornecedores especializados no mercado. O preço estimado para a contratação, no valor de **R\$ 89.881,21 (oitenta e nove mil, oitocentos e oitenta e um reais e vinte e um centavos)**, contempla a aquisição de 212 licenças pelo período de 36 meses, em parcela única.

Essa estimativa reflete as especificidades técnicas do objeto contratado, considerando:

1. **Características da contratação:** Trata-se da atualização de licenças de antivírus já em uso no ambiente do TJM/RS, o que inclui suporte técnico contínuo e atualizações regulares, mantendo a padronização e a integridade da infraestrutura tecnológica.

2. **Parâmetros de mercado:** A média de preços foi elaborada com base nos valores praticados por fornecedores consolidados no setor e em contratações similares realizadas por outros órgãos da Administração Pública, conforme registrado no Plano Nacional de Contratações Públicas (PNCP) e no levantamento de mercado.

3. Eficiência operacional e custo-benefício: A renovação elimina custos adicionais relacionados à aquisição de novas soluções, como treinamento da equipe, implementação de infraestrutura e migração de dados.

Em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos do disposto na alínea "d" do inciso II do caput do art. 124 da Lei nº 14.133/2021;

Em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

Serão reajustados os preços registrados, respeitada a contagem da anualidade e o índice previsto para a contratação; ou poderão ser repactuados, a pedido do interessado, conforme critérios definidos para a contratação.

J. ADEQUAÇÃO ORÇAMENTÁRIA

As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados na Lei Orçamentária Vigente.

A contratação será atendida pela seguinte dotação:

§ UO TRIBUNAL DE JUSTIÇA MILITAR

§ IP: 3902 GESTAO DE TIC – JME

§ NAD: 3.3.90.40 SERV. TIC - PESS.JURÍDICA

§ RECURSO: 2002 RECURSO

Integrante Técnico:

Nome: Juarez Bamberg da Silva

Cargo: Coordenador de Tecnologia da Informação e de Comunicação - TIC- Substituto

E-mail: juarez-bamberg@tjmrs.jus.br

Integrante administrativo:

Nome: Juliana Guglermano Deon Gardin

Cargo: Servidor

E-mail: juliana-gardin@tjmrs.jus.br

Porto Alegre, 25 de fevereiro de 2025.

ANEXO VI - MODELO ANÁLISE CONTÁBIL DA CAPACIDADE FINANCEIRA DE LICITANTE

 GOVERNO DO ESTADO DO RIO GRANDE DO SUL ANEXO II AO DECRETO Nº 36.601, de 10-04-96.	J	IDENTIFICAÇÃO DO PROCESSO					
	NÚMERO				FOLHA		
ANÁLISE CONTÁBIL DA CAPACIDADE FINANCEIRA DE LICITANTE – ACF							
A IDENTIFICAÇÃO DO EDITAL							
CÓDIGO	NOME DO LICITADOR		NÚMERO	MODALIDADE	DATA		
B IDENTIFICAÇÃO DO LICITANTE							
CGC/MF:			ATIVIDADE PRINCIPAL		CNAE	SE	
FIRMA/RAZÃO SOCIAL:			CNJ		CGC/TE		
ENDEREÇO (rua, avenida, praça, etc.)				NÚMERO	CONJ.	CEP	
NOME DO REPRESENTANTE LEGAL					TELEFONE		
BALANÇO APRESENTADO PERÍODO:		DATA DO BALANÇO ANUAL	Nº LIVRO DIÁRIO		Nº DO RJC		
C IDENTIFICAÇÃO DO CONTADOR OU TÉCNICO EM CONTABILIDADE							
NOME:			CP	Nº DO REGISTRO NO CRC		TELEFONE	
ENDEREÇO (rua, avenida, praça, etc.)				NÚMERO	CONJ.	CEP	
D IDENTIFICAÇÃO DA AUDITORIA							
NOME:					Nº DO REGISTRO NO CRC		
E BALANÇO PATRIMONIAL REESTRUTURADO			F DEMONSTRAÇÃO DA ANÁLISE FINANCEIRA DO LICITANTE				
CONTAS		Em R\$ Mil	ÍNDICE	VALOR	NOTA	PESO	NP
1	ATIVO CIRCULANTE AJUSTADO (ACA)		1	LIQUIDEZ CORRENTE			
2	PASSIVO CIRCULANTE (PC)						
3	ACA + REALIZÁVEL A LONGO PRAZO		2	LIQUIDEZ GERAL			
4	PC + PASSIVO A LONGO PRAZO						

5	ATIVO PERMANENTE		3	GRAU DE IMOBILIZAÇÃO				
6	PATRIMÔNIO LÍQUIDO AJUSTADO							
7	PASSIVO CIRCULANTE		4	ENDIVIDAMENTO DE CURTO PRAZO				
8	PATRIMÔNIO LÍQUIDO AJUSTADO							
9	PC + PASSIVO A LONGO PRAZO		5	ENDIVIDAMENTO GERAL				
10	PATRIMÔNIO LÍQUIDO AJUSTADO							
11	DESPESA ANTECIPADA		NFR	NOTA FINAL DA CAPACIDADE FINANCEIRA RELATIVA = $\frac{a}{NP}$				
12	RESULTADOS DE EXERCÍCIOS FUTUROS							
13	CAPITAL SOCIAL INTEGRALIZADO		G	RESULTADO DA ANÁLISE				
14	PATRIMÔNIO LÍQUIDO							
15	CONSISTÊNCIA (vide instruções no verso)							

H IDENTIFICAÇÃO DO SERVIDOR PÚBLICO

NOME: _____ MATRÍCULA _____

I DECLARAÇÃO E ASSINATURAS

O representante legal da empresa licitante e o contador ou técnico em contabilidade declaram, sob as penas da Lei, que as informações prestadas neste formulário são a expressão da verdade, bem como autorizam o licitador, por si ou por outrem e a qualquer tempo, examinar os livros e os documentos relativos à escrituração contábil, para confrontação dos dados aqui demonstrados.

LICITANTE	CONTADOR OU TÉCNICO EM CONTABILIDADE	LICITADOR
DATA:	DATA:	DATA:

OBSERVAÇÃO: Nos casos de envio do Anexo VI- CCFL, o documento deverá ser encaminhado devidamente assinado e preenchido, no que couber, sob pena de desclassificação.



Documento assinado eletronicamente por **Herbert Schonhofen, Diretor-Geral**, em 12/03/2025, às 14:07, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade deste documento pode ser conferida em <https://sei.tjms.jus.br/autenticidade>, informando o código verificador **0164728** e o código CRC **1024175D**.