EDITAL PREGÃO ELETRÔNICO Nº 21/2025

IDCidadES: 2025.032E0700001.01.0013

A PREFEITURA MUNICIPAL DE ICONHA, ESTADO DO ESPÍRITO SANTO, inscrito no CNPJ: 27.165.646/0001-85, situada à Praça Darcy Marchiori, nº 11, Bairro Jardim Jandira, torna público ao conhecimento dos interessados, que realizará licitação**,** na modalidade de **PREGÃO ELETRÔNICO**, conforme descrito neste Edital e seus Anexos, na forma da Lei Federal n°. 14.133/2021, a Lei Complementar n°. 123/2006, e, subsidiariamente de outras normas aplicáveis ao objeto deste certame, realizara licitação, com ampla participação ou com participação exclusiva de microempresas e empresas de pequeno porte ou com cotas reservadas para microempresas e empresas de pequeno porte, do tipo MENOR PREÇO/MAIOR DESCONTO por LOTE, mediante as condições estabelecidas neste edital.

LOCAL DA REALIZAÇÃO DA SESSÃO: Plataforma Portal de Compras Públicas - www.portaldecompraspublicas.com.br

DATA DE INÍCIO DE ACOLHIMENTO DAS PROPOSTAS: 04/09/2025 às 09:00h

DATA LIMITE PARA PEDIDO DE ESCLARECIMENTO/ IMPUGNAÇÃO: 12/09/2025, às 23:59h

DATA FINAL DE ACOLHIMENTO DAS PROPOSTAS: 18/09/2025 às 07:59h

ABERTURA DA SESSÃO E INÍCIO DA DISPUTA: 18/09/2025 às 08:00h

MODO DE DISPUTA: Aberto

CRITÉRIO DE JULGAMENTO: Menor Preço.

DO OBJETO.

1. Contratação de empresa especializada no fornecimento Licenças do Software Kaspersky Next EDR Foundations Brazilian Edition e Suporte Técnico, para atender as demandas da Prefeitura de Iconha, conforme especificações e condições estabelecidas no Termo de Referência.

DAS DESPESAS E DOS RECURSOS ORÇAMENTÁRIOS

2. As despesas decorrentes da presente licitação correrão por conta:

Secretaria	Ficha	Natureza de Despesa	Fonte de Recursos
ADMINISTRAÇÃO	86	33904000000	172000000000
GABINETE/PROJUR/UCCI	24	33904000000	150000009999
FINANÇAS	126	33904000000	150000009999
SEME	172	33904000000	150000250000
OBRAS	983	33904000000	150000009999
SEMAG	853	33903600000	150000009999
SEMMA	371	33904000000	150000009999
SETCUL	1500	33903900000	1074
SEMADES	430, 461, 671, 692, 720, 798 e 799	33903900000	1500, 1660 e 1661

Do orçamento para o exercício de 2025.

DAS CONDIÇÕES DE PARTICIPAÇÃO

3. Poderão participar deste pregão os interessados que estiverem previamente credenciados no sistema eletrônico disponível, por meio do sitio www.portaldecompraspublicas.com.br ,

4. Para ter acesso ao sistema eletrônico, os interessados em participar deste pregão deverão ter conhecimento acerca do seu funcionamento e regulamento e receber instruções detalhadas para correta utilização do sistema.

5. Não poderão participar deste pregão:

5.1 impedidos de contratar no âmbito da Administração Publica direta e indireta do Município de Iconha, nos termos do atr. 156 III, §4°, da Lei n°.14.133/2021;

5.2 suspensos de participar de licitações e impedidos de contratar com o Município de Iconha, nos termos do art. 87, III, da Lei n°.8.666/1993

5.3 impedidos de licitar e contratar com o Município de Iconha, nos termos do art. 7° da Lei n°.10.520/2002.

5.4 Declarados inidôneos para licitar ou contratar com a Administração Pública, na forma do art. 87 IV, da Lei n°.8.666/1993;

5.5 Declarados inidôneos para licitar ou contratar com a Administração Pública, na forma do art. 156, IV, § 5° da Lei n°. 14.133/2021;

5.6 Estrangeiros que não tenham representações legal no Brasil com poderes expressos para receber citação e responder administrativa e judicialmente.

5.7 Autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre obra, serviços ou fornecimento de bens a ele relacionados, incluindo autores do projeto as empresas integrantes do mesmo grupo econômico;

5.8 Empresa isoladamente ou em consorcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor demais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre obra, serviços ou fornecimento de bens a ela necessários.

5.9 Entidades empresarias cujo socio, ou caso de sociedade anônimas, cujo diretor seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até terceiro grau, inclusive, com ocupantes de cargos de direção ou no exercício de funções administrativas, assim como com servidores ocupantes de cargos de direção, chefia e assessoramento vinculados direta ou indiretamente as unidades situadas na linha hierarquia da área encarregada da licitação deste Município, conforme entendimento dos órgãos de controle externo;

5.10 Aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente publico que desempenhe função na licitação 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;

5.11 Pessoa física ou jurídica que, nos 5 (cinco) anos anteriores a 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;

5.12 Entidades empresariais que estejam sob falência, concurso de credores, em processo de dissolução total ou liquidação;

5.13 Empresas controladoras, controladas ou coligadas, nos termos da Lei n°. 6.404, de 15 de dezembro de 1976, concorrendo entre si;

DA PROPOSTA E DOCUMENTOS DE HABILITAÇÃO

6. O licitante interessado deverá encaminhar proposta exclusivamente por meio do sistema eletrônico www.portaldecompraspublicas.com.br até a data e horário marcados para abertura da sessão, quando então se encerrará automaticamente a etapa de envio da proposta.

   6.1 o licitante interessado poderá, se assim entender, enviar os documentos de habilitação exigidos no edital concomitantemente com a proposta.

7. O licitante deverá consignar na forma expressa no sistema eletrônico www.portaldecompraspublicas.com.br o valor total ofertado para cada item (resultado da multiplicação do valor unitário pela quantidade), já incluso todos tributos, fretes e demais despesas decorrentes da execução do objeto.

8. O licitante deverá fazer em campo próprio do sistema eletrônico www.portaldecompraspublicas.com.br , a descrição detalhada do produto ofertado ou colocar a expressão “de acordo com edital”

9. O licitante deverá declarar em campo próprio do sistema eletrônico www.portaldecompraspublicas.com.br , que cumpre plenamente os requisitos de habilitação, que sua proposta está em conformidade com as exigências do edital e que se observa a proibição prevista no art. 7°, XXXIII, da Constituição Federal, sob pena de inabilitação, sem prejuízo da aplicação das penalidades previstas em tópico específico deste edital.

10. O licitante enquadrado como microempresa ou empresa de pequeno porte devera declarar em campo próprio do sistema eletrônico www.portaldecompraspublicas.com.br, que atende aos requisitos do art. 3° da Lei Complementar n°. 123/2006 para fazer jus aos benefícios previstos nessa Lei.

11. Declaração falsa relativa ao cumprimento dos requisitos de habilitação, à conformidade da proposta ou ao enquadramento como microempresa ou empresa de pequeno porte sujeitará o licitante às sanções previstas neste edital.

12. Todas as propostas ficarão disponíveis no sistema eletrônico www.portaldecompraspublicas.com.br.

13. Qualquer elemento que possa identificar o licitante importará desclassificação da proposta, sem prejuízo das sanções previstas neste edital.

14. Até a abertura da sessão, o licitante poderá retirar ou substituir a proposta anteriormente encaminhada.

15. As propostas terão validade de 60 (sessenta) dias, contados da abertura da sessão pública estabelecida no preâmbulo deste edital.

16. Decorrido o prazo de validade das propostas sem convocação para contratação, ficam os licitantes liberados dos compromissos assumidos.

DA ABERTURA DA SESSÃO PÚBLICA

17. A abertura da sessão pública deste pregão, conduzida pelo pregoeiro, ocorrerá na data e na hora indicadas no preâmbulo deste edital, no Portal de Compras Públicas, www.portaldecompraspublicas.com.br.

18. Durante a sessão pública, a comunicação entre pregoeiro e os licitantes ocorrerá exclusivamente mediante troca de mensagens, em campo próprio do sistema eletrônico www.portaldecompraspublicas.com.br.

19. Cabe ao licitante acompanhar as operações no sistema eletrônico www.portaldecompraspublicas.com.br, durante sessão pública do pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem emitida pelo sistema, inclusive quanto ao não encaminhamento de documento afeto à proposta.

DA CLASSIFICAÇÃO DAS PROPOSTAS

20. As propostas cadastradas pelos licitantes no sistema eletrônico www.portaldecompraspublicas.com.br, que descumprirem as exigências do edital quanto à forma de sua apresentação e/ou apresentarem erros que prejudiquem a oferta de lances e o caráter competitivo do certame também serão desclassificadas, mediante decisão fundamentada do pregoeiro.

21. Somente os licitantes com propostas classificadas participarão da fase de lances.

DA FORMULAÇÃO DE LANCES

22. Aberta a etapa competitiva, os licitantes classificados poderão encaminhar lances sucessivos exclusivamente por meio do sistema eletrônico www.portaldecompraspublicas.com.br, sendo imediatamente informados do horário e do valor consignados no registro de cada lance.

23. O licitante somente poderá oferecer lance inferior ao ultimo ofertado por ele próprio e registrado no sistema eletrônico www.portaldecompraspublicas.com.br, respeitado o intervalor mínimo de diferença de valores entre os lances (conforme conta do orçamento estimativo), que incidirá tanto em relação aos lances intermediários quanto em relação á proposta que cobrir a melhor oferta

24. Será adotado para o envio de lances no pregão eletrônico o modo de disputa “ABERTO”, em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

25. A etapa de lances da sessão pública terá duração de 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 2 (dois) minutos do período de duração da sessão pública.

26. A prorrogação automática da etapa de lances, de que trata o item anterior, será de 2 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

27. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública será encerrada automaticamente.

28. Encerrada a fase competitiva sem que haja a prorrogação automática pelo sistema, poderá o pregoeiro, assessorado pela equipe de apoio, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

29. Havendo eventual empate entre propostas ou lances, o critério de desempate será a reabertura para disputa final, hipótese em que os licitantes empatados poderão apresentar novas propostas em ato continuo à classificação.

30. Os lances apresentados e levados em consideração para efeito de julgamento serão de exclusiva e total responsabilidade do licitante, não lhe cabendo o direito de pleitear qualquer alteração.

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

32. Se ocorrer a desconexão do pregoeiro no decorrer da etapa de lances, mas o sistema eletrônico www.portaldecompraspublicas.com.br, permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

33. No caos de a desconexão do pregoeiro persistir por tempo superior a 10 (dez) minutos, a sessão do pregão será suspensa automaticamente e terá reinício somente após comunicação expressa aos participantes no sítio www.portaldecompraspublicas.com.br

DOS BENEFICIOS AS MICROEMPRESAS E ÀS

EMPRESAS DE PEQUENO PORTE

34. A obtenção de benefícios previstos dos artigos 42 e 49 da Lei Complementar n°.123/2006 fica limitada às microempresas e às empresas de pequeno porte que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública, cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, devendo o licitante apresentar declaração de observância desse limite juntamente para fins de habilitação.

35. Após a fase de lances, se a proposta mais bem classificada não tiver sido apresentada por microempresa ou empresa de pequeno porte apta a usufruir dos benefícios e se houver proposta de microempresa ou empresa de pequeno porte igual ou até 5% (cinco por cento) superior à proposta mais bem classificada, se procederá da seguinte forma:

    35.1 a microempresa ou empresa de pequeno porte mais bem classificada poderá, no prazo de 5 (cinco) minutos, apresentar proposta de preço inferior à do licitante mais bem classificado e, se atendidas as exigências deste edital, ser adjudicatária;

    35.2 não sendo adjudicatária a microempresa ou empresa de pequeno porte mais bem classificada na forma do subitem anterior, e havendo outros licitantes que se enquadrem na condição prevista no caput deste item, estes serão convocados, na ordem classificatórios, para o exercício do mesmo direito;

    35.3 o convocado que não apresentar proposta dentro do prazo de 5 (cinco) minutos, controlado pelo sistema eletrônico, decairá do direito previsto nos arts. 44 e 45 da Lei Complementar n°. 123/2006

36. na hipótese de não adjudicação nos termos previstos nesta clausula, o procedimento licitatório prosseguirá com os demais licitantes.

DA NEGOCIAÇÃO

37. O pregoeiro deverá encaminhar contraproposta diretamente ao licitante que tenha apresentado o lance mais vantajoso, observados o critério de julgamento e o valor estimado para a contratação.

38. A negociação será realizada por meio do sistema eletrônico www.portaldecompraspublicas.com.br, e poderá ser acompanhada pelos demais licitantes.

DA ACEITABILIDADE DA PROPOSTA

39. Encerrada a etapa competitiva de lances, exercido o direito de preferência e concluída a negociação, o pregoeiro iniciará os procedimentos necessários à aceitabilidade da proposta de melhor preço e verificará a conformidade da marca e modelo informados ou especificações técnica dos serviços com as exigências contidas neste edital e a compatibilidade do preço ofertado com o valor estimado para a contratação, podendo solicitar, se necessário, a planilha de composição de custos adequada ao lance equivalente á proposta de melhor preço no prazo estipulado no chat durante a sessão.

40. Se o mesmo licitante vencer tanto a cota reservada quanto a cota principal, a contratação ocorrerá em um único instrumento e pelo menor preço obtido.

41. No caso de não haver vencedor para a cota reservada, esta poderá ser adjudicada ao vencedor da cota principal ou, diante de sua recusa, aos licitantes remanescentes, desde que pratiquem o preço do primeiro colocado da cota principal.

    41.1 no caso de não haver vencedor para a cota principal, esta poderá ser adjudicada ao vencedor da cota reservada ou, diante da sua recusa, aos licitantes remanescentes, desde que pratiquem o preço do primeiro colocado da cota reservada.

42. Se a proposta/lance de menor preço for superior à do orçamento estimativo e se houver indícios de que se encontra dentro dos valores praticados no mercado, excepcionalmente o pregoeiro poderá suspender a sessão pública do pregão para a realização de nova pesquisa de mercado.

43. A nova pesquisa de mercado será submetida ao pregoeiro, o qual decidira fundamentadamente em:

44.1 retornar à sessão mantendo-se incólumes os atos praticados, se considerar que a nova pesquisa de preços não destoou dos valores anteriormente informados na pesquisa de preços, mantendo a recusa das propostas; ou

44.2 submeter o resultado da pesquisa à Autoridade Superior para que este decida sobre a possibilidade de aceitação de proposta (s) com base na nova pesquisa de preços efetuada, se considerar que, de fato, houve elevação superveniente dos preços.

44. Obtida a autorização tratada no subitem anterior, o pregoeiro retornará à sessão pública para efetuar nova negociação com o licitante mais bem classificado.

45. Serão desclassificadas as propostas com o valor superior ao estabelecido no orçamento estimativo contido neste edital

46. Para a obtenção do valor unitário do item cotado, será dividido o valor total pela quantidade prevista para a contratação, quando se considerarão somente as duas primeiras casas após a virgula, sem arredondamento.

46.1 Quando o licitante não conseguir comprovar que possui ou possuirá recursos suficientes para executar a contendo o objeto, será considerada inexequível a proposta de preços ou menor lance que:

46.1.1 for insuficiente para cobertura dos custos da contratação, apresente preços global ou unitários simbólicos, irrisórios ou valor zero,

incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do proposito licitante, para os quais ele renuncie a parcela ou à totalidade de remuneração.

46.1.2 Apresentar um ou mais valores da planilha de custo que sejam inferior aqueles fixados em instrumentos de caráter normativo obrigatório, tais como leis, medidas provisórias e convenções coletivas de trabalho vigentes.

47. Serão desclassificados, da mesma forma, as propostas que não atenderem às demais condições estabelecidas neste edital e anexos.

48. O pregoeiro poderá solicitar parecer de profissional especializado para orientar sua decisão.

49. Não se considerará qualquer oferta ou vantagem não prevista neste edital, inclusive financiamentos subsidiados ou a fundo perdido.

50. 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 dos quais ele renuncie á parcela ou á totalidade da remuneração.

51. O pregoeiro poderá fixar prazo para reenvio do anexo com a planilha de composição de preços quando o preço total ofertado for aceitável, mas quando os preços unitários que compõem necessitem de ajustes aos valores estimados por esta Administração.

DA HABILITAÇÃO

52. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o pregoeiro verificará eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação dele no certame ou futura contratação, mediante consulta aos seguintes cadastros:

I. Inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional de Pessoa Jurídica (CNPJ);

II. Inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicilio ou sede do licitante, pertinente ao seu ramo de atividades e compatível com objeto contratual;

III. Cadastro de Fornecedores do Município;

IV. SICAF

V. Sistema de registro Cadastral Unificado do PNCP;

VI. Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), mantido pela Controladoria-Geral da União;

VII. Cadastro Nacional de Empresas Punidas (CNEP), mantido pela Controladoria-Geral da União;

VIII. Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça; e

IX. Lista de Inidôneos, mantida pelo Tribunal de Contas da União (TCU)

53. A consulta aos cadastros acima referidos será realizada em no nome do licitante e também de seu sócio majoritário, por força do art. 12 da Lei n° 8.429/1992.

54. A habilitação dos licitantes será verificada por meio do cadastro desta Administração Pública, bem como da documentação complementar especificada neste edital.

55. Não é condição obrigatória para habilitação estar cadastrado nesta Prefeitura Municipal.

56. Considera-se documentação complementar que deve ser apresentada pelos licitantes para fins de habilitação quando não constantes do cadastro desta Prefeitura:

I prova de regularidade perante a Fazenda Federal;

II prova de regularidade perante a Fazenda Estadual;

III prova de regularidade perante a Fazenda Municipal do domicílio ou sede do licitante.

IV Prova de regularidade com o FGTS;

V Prova de regularidade com a Justiça do Trabalho;

VI Certidão negativa de efeitos de falência

56.1 Considerando a exigência e amostra posteriormente à fase de habilitação, o envio da documentação relativa à regularidade fiscal será obrigatório apenas após verificada a aceitabilidade da proposta.

56.2 O licitante provisoriamente classificado em primeiro lugar deverá encaminhar, via sistema eletrônico, no prazo fixado pelo pregoeiro, a seguinte documentação complementar:

I. Declaração de que não possui sócio (s) ou, no caso de sociedade anônima, diretor (es) que seja (m) que seja cônjuge (s) ou tenha (m) parentesco em linha reta, colateral ou por afinidade, até o terceiro grau, com

ocupantes de cargos de direção, chefia e assessoramento vinculados direta ou indiretamente ás unidades situadas na linha hierárquica da área encarregada da licitação desta Administração Pública, podendo utilizar o modelo anexo a este edital

II. Declaração de cumprimento da Lei Geral de Proteção de Dados – Lei n°.13.709/2018, devendo utilizar o modelo anexo a este edital:

III. Declaração de que possui ciência e submete-se aos termos do Programa de Integridade desta Prefeitura, implementado pelo Decreto Municipal n° 4.191/2023, devendo utilizar o modelo anexo a este edital;

IV. Declaração de 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, devendo utilizar o modelo anexo a este edital;

V. Em relação às microempresas e às empresas de pequeno porte, declaração de que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte devendo utilizar o modelo anexo a este edital:

57. Os licitantes que não atenderem as exigências de habilitação com as informações constantes no cadastro desta prefeitura deverão encaminhar, via sistema eletrônico no prazo fixado pelo pregoeiro, documentos que supram tais exigências, na forma do art. 70 da Lei n° 14.133/2021.

58. O pregoeiro poderá consultar sítios oficiais de órgãos e entidades emissores de certidões para verificar as condições de habilitação dos licitantes

58.1 As declarações exigidas neste edital poderão ser supridas mediante manifestação expressa do licitante no chat do sistema www.portaldecompraspublicas.com.br

59. Havendo a necessidade de envio de documentos para a confirmação daqueles exigidos neste edital, já apresentados, ou, ainda, de envio de documentos não juntados mas que comprovem que na data da apresentação da proposta o licitante atendia às condições de aceitabilidade da proposta e de habilitação, o licitante será convocado a encaminhá-los, via sistema eletrônico www.portaldecompraspublicas.com.br, no prazo fixado pelo pregoeiro, sob pena de desclassificação ou de inabilitação, prazo durante o qual a sessão não será suspensa.

60. Sob pena de inabilitação, os documentos encaminhados deverão estar em nome do licitante, com indicação precisa de dados capazes de qualificar inequivocamente o licitante.

61. Em se tratando de filial, os documentos de habitação jurídica e regularidade fiscal deverão estar em nome da filiar, exceto que pela própria natureza, são emitidos somente em nome da matriz.

62. Em se tratando de microempresa ou empresa de pequeno porte, havendo alguma restrição na comprovação da regularidade fiscal trabalhista, será assegurado o prazo de 5 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que o proponente for declarado vencedor do certame, prorrogável por igual período, a critério da Administração, para a regularização da documentação, pagamento ou parcelamento do debito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

63. A não regularização da documentação no prazo previsto no subitem anterior implicará decadência do direito a contratação, sem prejuízo das sanções previstas neste edita, e facultará ao pregoeiro convocar os licitantes remanescentes, na ordem de classificação

64. Se a proposta for desclassificada ou, ainda se o licitante não atender às exigências de habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a seleção da proposta que melhor atenda a este edital.

65. Constatado o atendimento às exigências ficadas neste edital, o licitante será declarado o vencedor.

DO RECURSO

66. Caberá recurso em face de:

I. Julgamento das propostas;

II. Ato de habilitação ou inabilitação de licitante;

III. Anulação ou revogação da licitação;

67. Nos recursos de julgamento das propostas e de ato de habilitação ou inabilitação de licitante serão observadas as seguintes disposições:

I. A intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão, e o prazo para apresentação das razões recursais de 3 (três) dias uteis será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação ou, na hipótese de adoção da inversão de fases previstas no §1° do art. 17 da Lei n°. 14.133/2021, da ata de julgamento;

II. A apreciação se dará em fase única;

68. Declarado o vencedor, o pregoeiro abrirá prazo de 10 (dez) minutos, durante o qual qualquer licitante poderá, de forma imediata, em campo próprio do sistema eletrônico www.portaldecompraspublicas.com.br, manifestar sua intenção de recurso.

69. A falta de manifestação no prazo estabelecido autoriza a Administração a adjudicar o objeto ao licitante vencedor.

70. Não será admitida intenção de recurso de caráter protelatório, fundada em mera insatisfação do licitante, ou baseada e fatos genéricos.

71. O pregoeiro examinará a intenção de recurso, aceitando-a ou, motivadamente, rejeitando-a, em campo próprio do sistema eletrônico www.portaldecompraspublicas.com.br.

72. O licitante que tiver sua intenção de recurso aceita deverá registrar as razões do recurso em campo próprio do sistema no prazo de 3 (três) dias uteis, ficando os demais licitantes, desde logo, intimados a apresentar contrarrazões, também via sistema, em igual prazo, que começará a correr a partir do termino do prazo do recorrente.

73. Para justificar sua intenção de recorrer e fundamentar suas razões ou contrarrazões de recurso, o licitante interessado poderá solicitar vista dos autos a partir do encerramento da fase de lances.

74. As intenções de recurso não admitidas e os recursos rejeitados pelo pregoeiro serão a ele dirigidos, que se não reconsiderar o ato ou a decisão no prazo de 3 (três) dias uteis, encaminhara o recurso com sua motivação à autoridade superior, a qual deverá proferir sua decisão no prazo máximo de 10 (dez) dias uteis, contado do recebimento dos autos.

75. O acolhimento do recurso implicará a invalidação apenas dos atos não suscetíveis de aproveitamento.

76. O objeto deste pregão será adjudicado ao licitante vencedor.

77. A homologação do resultado deste pregão compete ao Prefeito Municipal.

DA ATA DE REGISTRO DE PREÇO

78. Não se aplica

DA FORMAÇÃO DO CADASTRO DE RESERVA

79. Não se aplica

DAS SANÇÕES

80. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

I. Deixar de entregar a documentação exigida para o certame:

a) Pena – impedimento do direito de licitar e contratar com Município de Iconha pelo prazo de 15 (quinze) a 120 (cento e vinte) dias;

II. Ensejar o retardamento da execução do certame:

a) Pena – impedimento do direito de licitar e contratar com Município de Iconha pelo prazo de 15 (quinze) a 120 (cento e vinte) dias;

III. Não mantiver a proposta, salvo em decorrência de fato superveniente devidamente justificado:

a) Pena – impedimento do direito de licitar e contratar com o Município de Iconha pelo prazo de 15 (quinze) a 120 (cento e vinte) dias.

IV. Não celebrar o contrato ou a ata de registro de preços no prazo estabelecido no edital ou não retirar/assinar/não dar recebimento aos respectivos instrumentos contratuais:

a) Pena – impedimento do direito de licitar e contratar com o Município de Iconha pelo prazo de 15 (quinze) a 120 (cento e vinte) dias e multa correspondente a 5% (cinco por cento) do valor do item da contratação.

V. Comporta-se de modo inidôneo:

a) Pena – declaração de inidoneidade para licitar ou contratar com todos os entes federativos da Administração Pública Direta e Indireta pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.

81. Além das penalidades acima, os licitantes ficarão sujeitos ao cancelamento de sua inscrição no cadastro desta Prefeitura Municipal e, no que couber, às demais penalidades referidas no Título IV da Lei n°.14.133/2021.

82. Para os fins deste edital, para aplicação de qualquer das penalidades previstas, considera-se:

I. Deixar de entregar a documentação exigida para o certame:

a) Não entregar qualquer documento que tenha sido exigido no edital ou solicitado pelo pregoeiro durante o certame; ou

b) Entregar em desacordo pelo pregoeiro durante o certame;

II. Retardar a execução do certame:

a) Apresentar proposta ou amostra em desacordo com as especificações do edital;

b) Não comprovar os requisitos de habilitação; ou

c) Praticar qualquer ação, ou se omitir, de modo que prejudique o bom andamento do certame;

III. Não mantiver a proposta;

a) Não enviar a proposta;

b) Recusar-se a enviar o detalhamento da proposta quando exigível;

c) Pedir para ser desclassificado quando encerrada a etapa competitiva; ou

d) Deixar de apresentar amostra;

IV. Comporta-se de maneira inidônea:

a) praticar ato de vise a frustrar os objetivos do procedimento licitatório;

b) cometer fraude de qualquer natureza;

c) agir em conluio ou em desconformidade com a lei;

d) induzir deliberadamente a erro no julgamento;

e) apresentar amostra falsificada ou deteriorada;

f) realizar atos como os descritos no art. 156. IV, §5° da Lei n°. 14.133/2021; ou

g) prestar informações falsas ou apresentar documento com informações inverídicas; ou

h) praticar ato lesivo previsto no art, 5° da Lei n°.12.846, de 1° de agosto de 2013, art. 5°. Da Lei n°.12.846 de 1° de agosto de 2013.

83. não será apurada a conduta pertinente à desclassificação ocorrida antes da fase de lances, salvo se houver indícios de má fé.

84. Quando a ação ou omissão do licitante ou do adjudicatário ensejar o enquadramento da conduta em tipos distintos, prevalecerá aquele que comina a sanção mais gravosa.

85. Quando, em um mesmo procedimento licitatório, o licitante cometer mais de uma conduta passível de punição em itens de contratação diversos, será aplicada a pena da conduta mais gravosa, podendo ser majorada até seu patamar máximo, observado o princípio da proporcionalidade.

86. Poderá ser afastada a majoração de que trata o item anterior caso as condutas perpetradas possuam nexo casual entre si.

87. A aplicação de quaisquer das penalidades previstas neste edital será realizada mediante instrução de procedimento administrativo que assegurará o contraditório e a ampla defesa.

88. Detectada prática de conduta que, em tese, configure infração administrativa, o pregoeiro seguirá ao Secretário Municipal gerenciador da contratação que inicie procedimento de apuração em processo apartado, indicando os fatos que ensejam a apuração, o enquadramento dos fatos às normas pertinentes à infração e a identificação do licitante.

89. Caso tenha sido verificada concomitante conduta que configure ato lesivo à administração pública previsto na Lei n° 12.846 de 1° de agosto de 2013, o rito de apuração será aquele previsto na referida Lei.

90. O processo de responsabilização será conduzido por comissão ad hoc composta por 2 (dois) ou mais servidores efetivos, que avaliará fatos e circunstâncias conhecidos e intimará o licitante, para que, no prazo de 15 (quinze) dias úteis, contado da publicação do Diário, apresente defesa escrita e especifique as provas que pretenda produzir.

90.1. O oficio de intimação será encaminhado também ao endereço eletrônico cadastrado na proposta do licitante ou no Cadastro do Fornecedores.

90.2. Exaurida a fase instrutória, a comissão poderá oportunizar a apresentação de alegações finais no prazo de 15 (quinze) dias úteis, nos termos da legislação aplicável.

90.3. A comissão elaborará relatório final conclusivo no qual mencionará os fatos imputados, os dispositivos legais e regulamentares infringidos, as penas a que está sujeito o infrator, as peças principais dos autos, analisará as manifestações da defesa e indicará as provas em que se baseou para formar sua convicção, fazendo referência às folhas do processo onde se encontram

91. A autoridade de competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena e o dano causado à Administração, observados os princípios da proporcionalidade e da razoabilidade.

91.1 Sem modificação dos fatos narrados na autorização de abertura do processo de apuração de responsabilidade, o órgão julgador poderá atribuir definição jurídica diversa, ainda que, em consequência, sujeite o acusado à sanção de declaração de inidoneidade para licitar ou contratar.

92. O licitante ficará isento das penalidades caso reconhecida força maior ou caso fortuito devidamente reconhecido pela Administração, bem como comprovado que a conduta praticada seja decorrente de vícios ou omissões para os quais não tenha contribuído.

93. Na hipótese de aplicação de penalidade de multa, será emitida notificação de cobrança ao licitante, que deverá fazer o recolhimento do valor aos cofres públicos no prazo de 5 (cinco) dias úteis, contados do recebimento da notificação. Sob pena de cobrança judicial.

94. As penalidades serão obrigatoriamente registradas nos Cadastros de Fornecedores competentes após o trânsito em julgado administrativo.

95. Considera-se que a decisão teve o trânsito em julgado administrativo:

I. No dia útil subsequente ao término do prazo para a interposição de recurso, sem a interposição destes;

II. No dia útil subsequente a ciência da decisão em sede de recurso.

DOS ESCLARECIENTOS E DA IMPUGNAÇÃO AO EDITAL

96. Até 3 (três) dias úteis antes da data ficada para abertura da sessão pública, qualquer pessoa, física ou jurídica, poderá impugnar o ato convocatório deste pregão, por irregularidade na aplicação de Lei ou para solicitar esclarecimento sobre os seus termos, mediante petição, a ser enviada exclusivamente para o endereço www.portaldecompraspublicas.com.br

97. O pregoeiro, auxiliado pelo setor técnico competente e pela Assessoria jurídica, decidirá sobre a impugnação do certame.

98. Acolhida a impugnação do certame, será designada nova data para sua realização, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

99. Os pedidos de esclarecimentos deverão ser enviados até o terceiro dia útil que anteceder a data ficada para abertura da sessão pública exclusivamente via internet, para o endereço www.portaldecompraspublicas.com.br

100. As respostas às impugnações e aos esclarecimentos solicitados serão disponibilizadas no sistema eletrônico em até 3 (três) dias uteis, contados do recebimento do pedido, limitado ao último dia útil anterior à data da abertura do certame

DA AMOSTRA OU DO TESTE DE CONFORMIDADE.

101. Não se aplica.

DISPOSIÇÕES FIANIS

102. Ao Prefeito Municipal compete anular este pregão por ilegalidade, de oficio ou por provocação de qualquer pessoa, e revogar o certame por considera-lo inoportuno ou inconveniente diante de fato superveniente, mediante ato escrito e fundamentado.

103. A anulação do pregão induz à do contrato ou da ata de registro de preço.

104. Os licitantes não terão direito a indenização em decorrência da anulação do procedimento licitatório, ressalvo o direito do contratado de boa-fé de ser ressarcido pelos encargos que tiver suportado no cumprimento do contrato.

105. É facultado ao pregoeiro ou à autoridade superior, em qualquer fase deste pregão, promover diligência destinada a esclarecer ou completar a instrução do processo, sendo vedada, ressalvados os casos previstos neste edital. A inclusão posterior de informações ou de documentos que deveriam ter sido apresentados para fins de classificação e habilitação.

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

107. Caso os prazos definidos neste edital não estejam expressamente indicados na proposta, eles serão considerados como aceitos pelos licitantes para efeitos de julgamento deste pregão.

108. Poderá ser solicitada tradução para língua portuguesa, efetuada por tradutor juramentado, de documentos emitidos em língua estrangeira, que também deverão ser devidamente consularizações ou registrados em cartório de títulos e documentos.

109. Em caso de divergência entre normas infralegais e contidas neste edital, prevalecerão as últimas.

110. Este pregão poderá ter a data de abertura da sessão pública transferida por conveniência desta Administração.

111. Na contagem dos prazos estabelecidos neste edital, será excluído o dia do início e incluído o do vencimento, e serão considerados os dias consecutivos, exceto quando for explicitamente disposto em contrário.

112. Só se iniciam e vencem os prazos referidos nesta licitação em dia de expediente na Prefeitura Municipal.

113. São partes integrantes (anexo) deste edital:

I. Termo de Referência;

II. Formulário de Proposta de Preços;

III. Orçamento Estimativo;

IV. Modelo de declarações unificadas;

V. Estudo Preliminar técnico, ou Justificativa de Quantitativo;

VI. Minuta do Contrato.

114. Este edital está disponibilizado, na íntegra, na página da Prefeitura Municipal de Iconha (www.iconha.es.gov.br) e no Portal de Compras Públicas (www.portaldecompraspublicas.com.br), e seu extrato será publicado no Diário Oficial dos Municípios.

DO FORO

115. As questões decorrentes das previsões deste edital que não possam ser dirimidas administrativamente serão processadas e julgadas na Justiça Estadual, no Foro da Comarca de Iconha, com exclusão de qualquer outro, por mais privilegiado que seja.

Iconha-ES, 04 de setembro de 2025

Roger Costa Poloni
Agente de Contratação

TERMO DE REFERÊNCIA

1. OBJETO

1.1. A presente contratação tem por objeto a aquisição de licenças do software Kaspersky Next EDR Foundations Brazilian Edition e Suporte Técnico com vigência de 36 meses.

1.2. Definição/Detalhamento do objeto, conforme especificações técnicas, condições, quantidades e exigências estabelecidas neste instrumento, abaixo discriminadas:

LOTE	Especificação	Unid	Quant.	Valor Unit	Valor Total
01	LICENÇA DO SOFTWARE Kaspersky Next EDR Foundations Brazilian Edition - 3 ANOS	UND	117	302,13	35.349,21
01	SUPORTE TECNICO PLATINUM Next EDR Foundations Brazilian Edition	UND	01	9.338,33	9.338,33

1.3. O critério de julgamento adotado será o “menor preço por LOTE”, observado o valor máximo aceitável elaborado com base em pesquisa de preços, constante do processo administrativo.

2. JUSTIFICATIVA

2.1. Visa proteção do ambiente informatizado desta Prefeitura Municipal, contra ação de pragas virtuais oriundas de navegação na WEB, acesso a dispositivos de

armazenamento, anexos de e-mails, dentre outros, proporcionando aumento da segurança das informações com as sucessivas atualizações da solução de segurança do produto Antivírus.

2.2. A Seção de Segurança adota, dentre outros, o método de proteção em camadas; O método de proteção em camadas consiste em criar várias camadas de proteção distintas e complementares, sendo cada camada atuando de forma especializada em alguns componentes de segurança;

2.3. Uma das camadas de proteção é realizada pelo sistema de antivírus, chamado de segurança das estações de trabalho (Endpoint Protection). Esta camada implementa a segurança das estações de trabalho oferecendo proteção em tempo real contra as ameaças mais comuns da internet como vírus, worms e trojans, além de fornecerem opções avançadas de bloqueio de dispositivos;

2.4. Vale mencionar, também, outra camada de segurança, não menos importante, que é o filtro de e-mail, denominado AntiSpam. O AntiSpam atua na verificação de mensagens de entrada e saída e tem a função de bloquear pragas virtuais oriundas da internet transmitidas por correio eletrônico. Atualmente, o surgimento diário de ataques através de pragas virtuais, coloca em risco todo o conteúdo gerado pelos servidores e jurisdicionados desta prefeitura.

2.5. Esta solução de segurança foi definida junto com a empresa E&L Produções de Software LTDA responsável pelo Sistema Integrado de Gestão Pública utilizado por esta Prefeitura. A aquisição atende plenamente às expectativas, adequando-se as funcionalidades operacionais dos sistemas.

3. DOS REQUISITOS DA CONTRATAÇÃO

3.1. Da forma de requisição do serviço: A CONTRATADA deve obedecer, no ato da entrega da licença a ser adquirido, os requisitos descritos nesse termo de referência;

3.2. Do prazo para entrega do serviço: A licença deverá ser fornecimento após recebimento da Ordem de Serviço;

3.3. Do prazo para a substituição no caso de defeito: Caso as licenças estejam em desacordo com o especificado, os mesmos devem ser substituídos imediatamente, sem que haja prejuízo à realização das atividades administrativas municipais e o funcionamento dos sistemas eletrônicos de uso rotineiro dos servidores;

3.4. Da garantia legal:

Ficará sob inteira responsabilidade da Contratada a garantia da qualidade do serviço prestado, sob pena das sanções legais cabíveis.

Caso a CONTRATANTE venha a sofrer prejuízos oriundos da má qualidade do serviço, a CONTRATADA deverá ressarcir todos os danos causados, bem como promover a reparação.

3.5. Dos custos agregados da prestação de serviço:

Todas as despesas diretas, indiretas, benefícios, encargos trabalhistas, previdenciários, fiscais e comerciais, frete, carga e descarga, tributos, sem qualquer exceção, que incidirem sobre a execução da prestação de serviço, correrão por conta exclusiva da empresa vencedora.

3.6. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:

3.6.1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.

3.6.2. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.

3.6.3. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).

3.6.4. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.

3.6.5. A solução proposta deve suportar o subsistema Linux no Windows.

3.6.6. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

3.6.6.1. Proteção contra ameaças sem arquivos (Fileless);

3.6.6.2. Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

3.6.6.3. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;

3.6.6.4. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.

3.6.7. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.

3.6.8. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.

3.6.9. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.

3.6.10. A solução proposta deve fornecer análise comportamental baseada em machine learning.

3.6.11. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.

3.6.12. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:

3.6.12.1. Controles de aplicativos;

3.6.12.2. Controle web e dispositivos;

3.6.12.3. HIPS e Firewall;

3.6.12.4. Descoberta de patches e vulnerabilidades de sistemas operacionais

Windows;

3.6.12.5. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.

3.6.13. A solução proposta deve ser protegida por senha para evitar que o processo do antimalware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.

3.6.14. A solução proposta deve ter bancos de dados de reputação locais e globais.

3.6.15. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.

3.6.16. A solução proposta deve incluir um módulo capaz, no mínimo, de:

3.6.16.1. Bloqueio de aplicativos com base em sua categorização;

3.6.16.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos;

3.6.16.3. A adição de sub-redes e a modificação de permissões de atividade.

3.6.17. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.

3.6.18. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.

3.6.19. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.

3.6.20. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.

3.6.21. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.

3.6.22. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.

3.6.23. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.

3.6.24. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.

3.6.25. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.

3.6.26. A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.

3.6.27. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;

3.6.28. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;

3.6.29. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.

3.6.30. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.

3.6.31. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.

3.6.32. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.

3.6.33. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.

3.6.34. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.

3.6.35. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.

3.6.36. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.

3.6.37. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.

3.6.38. A solução proposta deve ter categoria de detecção para bloquear banners de sites.

3.6.39. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;

3.6.40. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.

3.6.41. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.

3.6.42. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.

3.6.43. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;

3.6.44. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos

que não sejam aqueles incluídos nas listas de permissões.

3.6.45. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.

3.6.46. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.

3.6.47. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.

3.6.48. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.

3.6.49. A solução proposta deve suportar o controle de scripts executados em PowerShell.

3.6.50. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.

3.6.51. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.

3.6.52. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.

3.6.53. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.

3.6.54. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.

3.6.55. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.

3.6.56. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:

3.6.56.1. Filtro de anexos;

3.6.56.2. Verificação de mensagens de email ao receber, ler e enviar.

3.6.57. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.

3.6.58. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo.

3.6.59. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.).

3.6.60. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.

3.6.61. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.

3.6.62. A solução proposta deve incluir suporte ao protocolo IPv6.

3.6.63. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.

3.6.64. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:

3.6.64.1. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo;

3.6.64.2. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.

3.6.65. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.

3.6.66. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.

3.6.67. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.

3.6.68. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.

3.6.69. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.

3.6.70. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.

3.6.71. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.

3.6.72. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia, bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.

3.6.73. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.

3.6.74. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.

3.6.75. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.

3.6.76. A solução proposta deve suportar endereços IPv6.

3.6.77. A solução proposta deve suportar verificação em duas etapas (autenticação).

3.6.78. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração,

administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.

3.6.79. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.

3.6.80. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.

3.6.81. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.

3.6.82. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.

3.6.83. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.

3.6.84. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.

3.6.85. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos.

3.6.86. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.

3.6.87. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi, Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.

3.6.88. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.

3.6.89. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.

3.6.90. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o

sensor de endpoint está instalado.

3.6.91. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.

3.6.92. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.

3.6.93. A solução proposta deve ter a capacidade de excluir atualizações baixadas.

3.6.94. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.

3.6.95. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.

3.6.96. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.

3.6.97. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.

3.6.98. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.

3.6.99. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.

3.6.100. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.

3.6.101. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.

3.6.102. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:

3.6.103. Múltiplas formas de atualização, incluindo canais de comunicação

globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.

3.6.104. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.

3.6.105. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.

3.6.106. A solução proposta deve gerar relatórios de vulnerabilidades encontradas nos dispositivos com sensor de endpoint instalado.

3.7. Do módulo de gerenciamento de dispositivos móveis:

3.7.1. O modulo deve ser integrado a console de gerenciamento;

3.7.2. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

3.7.2.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition);

3.7.3. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

3.7.3.1. iOS 10–17 ou iPadOS 13–17;

3.7.4. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.

3.7.5. A solução proposta deve suportar dispositivos iOS supervisionados.

3.7.6. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.

3.7.7. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.

3.7.8. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.

3.7.9. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).

3.7.10. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.

3.7.11. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

3.7.12. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.

3.7.13. A solução proposta deve ter recursos de conteinerização para dispositivos Android.

3.7.14. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:

3.7.14.1. Dados em contêineres;

3.7.14.2. Contas de e-mail corporativo;

3.7.14.3. Configurações para conexão à rede Wi-Fi corporativa e VPN;

3.7.14.4. Nome do ponto de acesso (APN);

3.7.14.5. Perfil do Android for Work;

3.7.14.6. Recipiente KNOX;

3.7.14.7. Chave do gerenciador de licença KNOX.

3.7.15. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:

3.7.15.1. Todos os perfis de configuração instalados;

3.7.15.2. Todos os perfis de provisionamento;

3.7.15.3. O perfil iOS MDM;

3.7.15.4. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas.

3.7.16. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:

3.7.16.1. Critérios de verificação do dispositivo;

3.7.16.2. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o

usuário não corrija a não conformidade dentro do prazo definido;

3.7.17. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.

3.7.18. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:

3.7.18.1. Cartões de memória e outras unidades removíveis;

3.7.18.2. Câmera do dispositivo;

3.7.18.3. Conexões Wi-Fi;

3.7.18.4. Conexões Bluetooth;

3.7.18.5. Porta de conexão infravermelha;

3.7.18.6. Ativação do ponto de acesso Wi-Fi;

3.7.18.7. Conexão de área de trabalho remota;

3.7.18.8. Sincronização de área de trabalho;

3.7.18.9. Definir configurações da caixa de correio do Exchange;

3.7.18.10. Configurar caixa de e-mail em dispositivos iOS MDM;

3.7.18.11. Configure contêineres Samsung KNOX;

3.7.18.12. Definir as configurações do perfil do Android for Work;

3.7.18.13. Configurar e-mail/calendário/contatos;

3.7.18.14. Defina as configurações de restrição de conteúdo de mídia;

3.7.18.15. Definir configurações de proxy no dispositivo móvel;

3.7.18.16. Configurar certificados e SCEP.

3.7.19. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay.

3.7.20. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:

3.7.20.1. Google Play, Huawei App Gallery e Apple App Store;

3.7.20.2. Portal de inscrição móvel KNOX;

3.7.20.3. Pacotes de instalação pré-configurados independentes.

3.7.21. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.

3.7.22. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.

3.7.23. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:

3.7.23.1. VMware AirWatch 9.3 ou posterior;

3.7.23.2. MobileIron 10.0 ou posterior;

3.7.23.3. IBM MaaS360 10.68 ou posterior;

3.7.23.4. Microsoft Intune 1908 ou posterior;

3.7.23.5. SOTI MobiControl 14.1.4 (1693) ou posterior.

3.7.24. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.

3.7.25. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:

3.7.25.1. Google Play;

3.7.25.2. Galeria de aplicativos Huawei;

3.7.25.3. Loja de aplicativos da Apple.

3.7.26. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.

3.7.27. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.

3.7.28. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.

3.7.29. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.

3.7.30. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.

3.7.31. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.

3.7.32. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.

3.7.33. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.

3.7.34. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.

3.7.35. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.

3.7.36. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.

3.7.37. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.

3.7.38. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;

3.7.39. A solução proposta deve proteger contra ameaças online em dispositivos iOS.

A. 3.8. Do módulo de EDR:

3.8.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.

3.8.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.

3.8.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças.

3.8.4. Deve apresentar as seguintes informações:

3.8.4.1. Processo;

3.8.4.2. Arquivos;

3.8.4.3. Chaves de registros;

3.8.4.4. Conexões de rede;

3.8.4.5. SHA256 e MD5.

3.8.5. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise.

3.8.6. Deve apresentar informações detalhadas contendo:

3.8.6.1. Usuário que executou a ação;

3.8.6.2. Informações acesso privilegiado.

3.9. Requisitos para documentação da solução:

3.7.1. A documentação da solução do anti-malware incluindo ferramentas de administração, deve incluir os seguintes documentos:

3.7.1.1. Ajuda on-line para administradores;

3.7.1.2. Ajuda on-line para melhores práticas de implementação;

3.7.1.3. Ajuda on-line para proteção de servidores de administração.

3.7.2. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software antimalware.

3.7.3. Deve estar disponível página com informações de ciclo de vida das soluções e módulos.

B. 3.10. Do módulo de gerenciamento simplificado:

3.10.1. A solução proposta deve suportar arquitetura cloud.

3.10.2. A solução proposta deve incluir um console web integrado para o gerenciamento do endpoint, que não deve exigir nenhuma instalação adicional.

3.10.3. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

3.10.4. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.

3.10.5. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.

3.10.6. A solução proposta deve atender as condições apontadas no item e subintes 6.

3.10.7. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.

3.10.8. A solução proposta deve incluir informações do endpoint:

3.8.8.1. IP público de internet;

3.8.8.2. IP interno do dispositivo;

3.8.8.3. Versão do agente de proteção;

3.8.8.4. Última comunicação com a console, contendo data e hora;

3.8.8.5. Informações do sistema operacional.

C. 3.11. Do módulo de gerenciamento avançado:

3.11.1. A solução proposta deve suportar arquitetura cloud-native e on-premisse.

3.11.2. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:

3.11.2.1. Amazon Web Services;

3.11.2.2. Microsoft Azure.

3.11.3. A solução proposta deve incluir as seguintes opções de integração SIEM:

3.11.3.1. HP (Microfoco) ArcSight;

3.11.3.2. IBM QRadar;

3.11.3.3. Splunk;

3.11.3.4. Kaspersky KUMA.

3.11.4. A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

3.11.5. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;

3.11.6. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

3.11.7. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

3.11.8. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

3.11.9. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

3.11.10. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.

3.11.11. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

3.11.12. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.

3.11.13. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

3.11.14. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação:

3.11.14.1. Status do dispositivo;

3.11.14.2. Tag;

3.11.14.3. Diretório ativo;

3.11.14.4. Proprietários de dispositivos;

3.11.14.5. Hardware.

3.11.15. A solução proposta deve suportar os seguintes canais de entrega de notificação:

3.11.15.1. E-mail;

3.11.15.2. Registro de sistema;

3.11.15.3. SMS.

3.11.16. A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:

3.11.16.1. Atributos de rede;

3.11.16.2. Nome;

3.11.16.3. Domínio e/ou Sufixo de Domínio;

3.11.16.4. Endereço de IP;

3.11.16.5. Endereço IP para servidor de gerenciamento;

3.11.16.6. Localização no Active Directory;

3.11.16.7. Unidade organizacional;

3.11.16.8. Grupo;

3.11.16.9. Sistema operacional;

3.11.16.10. Número do pacote de serviço;

3.11.16.11. Arquitetura Virtual;

3.11.16.12. Registro de aplicativos;

3.11.16.13. Nome da Aplicação;

3.11.16.14. Versão do aplicativo;

3.11.16.15. Fabricante;

3.11.16.16. Tipo e versão;

3.11.16.17. Arquitetura.

3.11.17. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.

3.11.18. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.

3.11.19. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:

3.11.19.1. Dispositivos Desktop/Servidores;

3.11.19.2. Dispositivos móveis;

3.11.19.3. Dispositivos de rede;

3.11.19.4. Dispositivos virtuais;

3.11.19.5. Componentes OEM;

3.11.19.6. Periféricos de computador;

3.11.19.7. Dispositivos IoT conectados;

3.11.19.8. Telefones VoIP;

3.11.19.9. Repositórios de rede.

3.11.20. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:

3.11.20.1. Nome da Aplicação;

3.11.20.2. Caminho do aplicativo;

3.11.20.3. Metadados do aplicativo;

3.11.20.4. Aplicativo Certificado digital;

3.11.20.5. Categorias de aplicativos predefinidas pelo fornecedor;

3.11.20.6. SHA256 e MD5.

3.11.21. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:

3.11.21.1. Bluetooth;

3.11.21.2. Dispositivos móveis;

3.11.21.3. Modems externos;

3.11.21.4. CD/DVD;

3.11.21.5. Câmeras e scanners;

3.11.21.6. MTPs;

3.11.21.7. E a transferência de dados para dispositivos móveis.

3.11.22. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

3.11.23. A solução sugerida deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.

3.11.24. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

3.11.24.1. Estruturas de domínios e grupos de trabalho do Windows;

3.11.24.2. Estruturas de grupos do Active Directory;

3.11.24.3. Conteúdo de um arquivo de texto criado manualmente pelo administrador.

3.11.25. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.

3.11.26. A solução proposta deve permitir realizar as seguintes ações para endpoints:

3.11.26.1. Verificação manual;

3.11.26.2. Verificação no acesso;

3.11.26.3. Verificação por demanda;

3.11.26.4. Verificação de arquivos compactados;

3.11.26.5. Verificação de arquivos individuais, pastas e unidades;

3.11.26.6. Bloqueio e verificação de scripts;

3.11.26.7. Proteção contra alteração de registros;

3.11.26.8. Proteção contra estouro de buffer;

3.11.26.9. Verificação em segundo plano/inativa.

3.11.27. Verificação de unidade removível na conexão com o sistema;

3.11.28. A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou antimalware.

3.11.29. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.

3.11.30. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.

3.11.31. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.

3.11.32. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.

3.11.33. A solução proposta deve suportar Windows Failover Cluster.

3.11.34. A solução proposta deve ter um recurso de clustering integrado.

3.11.35. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.

3.11.36. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.

3.11.37. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.

3.11.38. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.

3.11.39. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.

3.11.40. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.

3.11.41. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.

3.11.42. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.

3.11.43. A solução proposta deverá possuir controles para download de DLL e drivers.

3.11.44. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo especifico de prevenção de intrusão.

3.11.45. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.

3.11.46. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).

3.11.47. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.

3.11.48. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.

3.11.49. A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.

3.11.50. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.

3.11.51. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.

3.11.52. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança antimalware através do servidor de administração.

3.11.53. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.

3.11.54. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações antimalware instalados, e para distribuir notificações sobre eventos por e-mail.

3.11.55. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.

3.11.56. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.

3.11.57. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal.

3.11.58. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.

3.11.59. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.

3.11.60. A solução proposta deve permitir ao administrador personalizar relatórios.

3.11.61. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.

3.11.62. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.

3.11.63. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.

3.11.64. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.

3.11.65. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.

3.11.66. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.

3.11.67. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos.

3.11.68. O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.

3.11.69. A solução proposta deve permitir instalar o modulo de gerenciamento onpremisse nos seguintes sistemas operacionais:

3.11.69.1. Windows;

3.11.69.2. Linux.

3.11.70. A solução proposta deverá suportar os seguintes servidores de banco de dados:

3.11.70.1. Windows:

3.11.70.2.1. Microsoft SQL Server;

3.11.70.2.2. Microsoft Banco de dados SQL do Azure;

3.11.70.2.3. MySQL Standard e Enterprise;

3.11.70.2.4. MariaDB 3.1.5. PostgreSQL.

3.11.70.3. Linux:

3.11.70.3.1. MySQL;

3.11.70.3.2. MariaDB;

3.11.70.3.3. PostgreSQL.

3.11.71. A solução proposta deverá suportar as seguintes plataformas virtuais:

3.11.71.2. Windows:

3.11.71.2.1. VMware vSphere 6.7 e 7.0;

3.11.71.2.2. Estação de trabalho VMware 16 Pro;

3.11.71.2.3. Servidor Microsoft Hyper-V 2012 de 64 bits;

3.11.71.2.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits;

3.11.71.2.5. Microsoft Servidor Hyper -V 2016 de 64 bits;

3.11.71.2.6. Servidor Microsoft Hyper-V 2019 de 64 bits;

3.11.71.2.7. Servidor Microsoft Hyper-V 2022 de 64 bits;

3.11.71.2.8. Citrix XenServer 7.1 LTSR;

3.11.71.2.9. Citrix XenServer 8.x 4.1.10. Oracle VM VirtualBox 6.x.

3.11.71.3. Linux:

3.11.71.3.1. VMware vSphere 6.7, 7.0 e 8.0;

3.11.71.3.2. VMware Desktop 16 Pro e 17 Pro;

3.11.71.3.3. Servidor Microsoft Hyper-V 2012 de 64 bits;

3.11.71.3.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits;

3.11.71.3.5. Microsoft Servidor Hyper -V 2016 de 64 bits;

3.11.71.3.6. Servidor Microsoft Hyper-V 2019 de 64 bits;

3.11.71.3.7. Servidor Microsoft Hyper-V 2022 de 64 bits;

3.11.71.3.8. Citrix XenServer 7.1 e 8.x;

3.11.71.3.9. Oracle VM VirtualBox 6.x e7.x.

D.

E. 3.12. Do módulo de proteção de endpoint:

3.12.1. A solução proposta deverá proteger os sistemas operacionais abaixo:

3.12.1.1. Windows 8;

3.12.1.2. Windows 7;

3.12.1.3. Windows 8.1;

3.12.1.4. Windows 10;

3.12.1.5. Windows 11.

3.12.2. Servidores:

3.12.2.1. Windows Small Business Server 2011;

3.12.2.2. Windows MultiPoint Server 2011;

3.12.2.3. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022.

3.12.3. Servidores de terminal Microsoft:

3.12.3.1. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022.

3.12.4. Sistemas operacionais Linux de 32 bits:

3.12.4.1. CentOS 6.7 e posterior;

3.12.4.2. Debian GNU/Linux 11.0 e posterior;

3.12.4.3. Debian GNU/Linux 12.0 e posterior;

3.12.4.4. Red Hat Enterprise Linux 6.7 e posterior.

3.12.5. Sistemas operacionais Linux de 64 bits:

3.12.5.1. Amazon Linux 2;

3.12.5.2. CentOS 6.7 e posterior;

3.12.5.3. CentOS 7.2 e posterior;

3.12.5.4. CentOS Stream 8;

3.12.5.5. CentOS Stream 9;

3.12.5.6. Debian GNU/Linux 11.0 e posterior;

3.12.5.7. Debian GNU/Linux 12.0 e posterior;

3.12.5.8. Linux Mint 20.3 e superior;

3.12.5.9. Linux Mint 21.1 e posterior;

3.12.5.10. OpenSUSE Leap 15.0 e posterior;

3.12.5.11. Oracle Linux 7.3 e posterior;

3.12.5.12. Oracle Linux 8.0 e posterior.

3.12.5.13. Oracle Linux 9.0 e posterior;

3.12.5.14. Red Hat Enterprise Linux 6.7 e posterior;

3.12.5.15. Red Hat Enterprise Linux 7.2 e posterior;

3.12.5.16. Red Hat Enterprise Linux 8.0 e posterior;

3.12.5.17. Red Hat Enterprise Linux 9.0 e posterior;

3.12.5.18. Rocky Linux 8.5 e posterior;

3.12.5.19. Rocky Linux 9.1;

3.12.5.20. SUSE Linux Enterprise Server 12.5 ou posterior;

3.12.5.21. SUSE Linux Enterprise Server 15 ou posterior;

3.12.5.22. Ubuntu 20.04 LTS;

3.12.5.23. Ubuntu 22.04 LTS.

3.12.6. Sistemas operacionais Arm de 64 bits:

3.12.6.1. CentOS Stream 9;

3.12.6.2. SUSE Linux Enterprise Server 15;

3.12.6.3. Ubuntu 22.04 LTS.

3.12.7. Sistemas operacionais MAC OS:

3.12.7.1. macOS 12 – 14.

3.10.8. Ferramentas de virtualização MAC OS:

3.10.8.1. Parallels Desktop 16 para Mac Business Edition;

3.10.8.2. VMware Fusion 11.5 Profissional;

3.10.8.3. VMware Fusion 12 Profissional.

3.10.9. A solução proposta deverá suportar as seguintes plataformas virtuais:

3.10.9.1. VMware Workstation 17.0.2 Pro;

3.10.9.2. VMware ESXi 8.0 Update 2;

3.10.9.3. Microsoft Hyper-V Server 2019;

3.10.9.4. Citrix Virtual Apps e Desktop 7 2308

3.10.9.5. Citrix Provisioning 2308;

3.10.9.6. Citrix Hypervisor 8.2 Update 1.

3.11. Requisitos de Suporte Técnico:

3.11.1. Instalação e Configuração Inicial:

A contratada deverá realizar a instalação e configuração inicial do gerenciador e de 5 (cinco) computadores no local designado pela contratante.

3.11.2. Abertura de Chamados e SLA:

Os chamados deverão ser registrados via sistema Tomticket, com SLA máximo de até 4 (quatro) horas para resposta inicial.

3.11.3. Base de Conhecimento:

A contratada deverá disponibilizar uma base de conhecimento atualizada com informações sobre a solução, acessível ao contratante.

3.11.4. Acesso Remoto:

Em caso de problemas, a contratada deverá prestar suporte técnico via acesso remoto para diagnóstico e solução.

3.11.5. Atendimento via WhatsApp:

O suporte técnico deverá incluir atendimento por WhatsApp, garantindo agilidade na comunicação.

3.11.6. Health Check Trimestral:

A contratada deverá realizar 1 (um) Health Check a cada 3 (três) meses para avaliar o desempenho e funcionamento da solução.

3.11.7. Consultoria Técnica:

A contratada deverá disponibilizar 2 (duas) horas de consultoria técnica para implementação ou ajustes específicos solicitados pela contratante.

3.11.8. Acesso Emergencial:

O contratante tem direito à atendimento emergencial com o primeiro analista disponível em casos críticos que exijam solução imediata.

3.11.9. Implementação Remota:

O contratado fará o auxílio da implementação do Endpoint da solução, criação de regras na solução e configuração para funcionamento.

4. DO PLANO DE FISCALIZAÇÃO/GESTÃO DO CONTRATO

4.1. Nos termos do art. 117 da Lei nº 14.133/2021, será designado representante para acompanhar e fiscalizar a execução do objeto da contratação, anotando em registro próprio todas as ocorrências relacionadas, e determinando o que for necessário à regularização de falhas ou defeitos observados. O proponente deverá indicar preposto e e-mail pelo qual o processo de fiscalização se desenvolverá.

4.2. Do Início da Prestação de Serviço:

4.2.1. A prestação de serviço, bem como a todos os itens que compõem o objeto deste Termo de Referência será supervisionada pelo fiscal do contrato, mediante assinatura no verso do documento fiscal respectivo atestando o recebimento provisório, que após verificação da sua conformidade encaminhará os documentos para o recebimento definitivo pelo gestor do contrato, com os dizeres: “verificada a conformidade, ao gestor para o recebimento definitivo”.

4.2.2. O pagamento do serviço prestado, quando em desacordo com as especificações e quantidades constantes neste Termo de Referência e na proposta, devendo ser solucionados pela Contratada no prazo máximo de 2 (dois) dias úteis, contados da data de recebimento da notificação, às suas custas, sem prejuízo da aplicação de penalidades.

4.2.3. Até que seja sanada a situação prevista no item anterior, ficará interrompido o prazo de recebimento definitivo e o prazo para pagamento ficará suspenso.

5. DAS OBRIGAÇÕES DO CONTRATANTE

5.1. São Obrigações do Contratante:

I. Efetuar o pagamento à CONTRATADA de acordo com o previsto neste instrumento;

II. Comunicar imediatamente à empresa qualquer irregularidade manifestada na execução do serviço;

III. Atestar a execução do serviço por meio do servidor designado para fiscalização do contrato;

IV. Fornecer informações que se façam necessários para a prestação do serviço;

V. Notificar à CONTRATADA sobre qualquer irregularidade encontrada na execução do serviço.

6. DAS OBRIGAÇÕES DA CONTRATADA

6.1. São Obrigações da Contratada:

6.1.1. Prestar o serviço, cotado em estrita conformidade com as especificações de sua proposta, à qual se vincula, não sendo admitidas retificações, cancelamentos, quer seja nos preços, quer seja nas condições estabelecida.

6.1.2. Não transferir a outrem, no todo ou em parte, o bem adjudicado, sem prévia e expressa anuência desta Prefeitura.

6.1.3. Propiciar todas as facilidades indispensáveis à fiscalização da execução do serviço.

6.1.4. Executar o serviço contratado em prazo não superior ao máximo estipulado na proposta. Caso tal serviço não seja executado dentro do prazo, a CONTRATADA ficará sujeita à multa.

6.1.5. Responder por todas as despesas de qualquer natureza relativas a fretes, embalagens, transportes, seguros, impostos, taxas, encargos sociais, trabalhistas, previdenciários, e todos os demais custos necessários ao cumprimento do serviço e à execução da contratação.

6.1.6. Cumprir outras obrigações previstas no Código de Proteção e Defesa do Consumidor (Lei n° 8.078/90) que sejam compatíveis com o regime de direito público.

6.1.7. Executar, perfeita e integralmente, o serviço contratado, no horário estabelecido pela Administração Pública Municipal e nos prazos ajustados, por meio de pessoas idôneas/tecnicamente capacitadas, obrigando-se a indenizar o Município de Iconha, mesmo em caso de ausência ou omissão de fiscalização de sua parte, por quaisquer danos causados às suas instalações, móveis, utensílios, máquinas e equipamentos, quer sejam eles praticados por empregados, prepostos ou mandatários seus. A responsabilidade estender-se-á aos danos causados a terceiros durante a prestação do serviço.

6.1.8. Dar como conferido e perfeito o serviço prestado, cumprindo, rigorosamente, o prazo estabelecido pela Administração Pública Municipal e responsabilizando- se por quaisquer prejuízos que suas falhas ou imperfeições venham causar a Prefeitura Municipal de Iconha ou a terceiros, de modo direto ou indireto, além de realizar novamente o serviço incorreto, se for o caso, sem quaisquer ônus para o Município de Iconha e sem prejuízo das multas contratuais previstas.

6.1.9. Efetuar, de imediato, o afastamento de qualquer profissional, quando se verificar o seguinte:

6.1.9.1. Atuação ou comportamentos julgados inconvenientes ou prejudiciais ao bom andamento do serviço;

6.1.9.2. Ocorrência sistemática de erros ou falhas na execução dos trabalhos;

6.1.9.3. Atos que comprometam a própria segurança ou a de terceiros;

6.1.9.4. Não atendimento às determinações do preposto.

6.1.10. Diligenciar para que seus empregados tratem com urbanidade os funcionários da Prefeitura Municipal de Iconha, bem como ao jurisdicionado, visitantes e demais contratados.

6.1.11. Dar ciência ao Gabinete do Prefeito, imediatamente e por escrito, de qualquer anormalidade que verificar no fornecimento do bem.

6.1.12. Prestar os esclarecimentos que lhe forem solicitados, atendendo prontamente a todas as reclamações e convocações da Prefeitura Municipal de Iconha.

6.1.13. Diligenciar para que seus empregados não prestem serviços que não os previstos no objeto deste contrato.

6.1.14. Apresentar à Prefeitura Municipal de Iconha o requerimento de pagamento pelo serviço prestado, juntamente com a fatura/nota fiscal, Certidão conjunta negativa de débitos relativos aos tributos federais e à Dívida Ativa da União; Certidão negativa de débitos relativos às contribuições previdenciárias e às de terceiros; Certificado de Regularidade do FGTS.

6.1.15. Assumir todas as despesas e ônus relativos ao pessoal e quaisquer outros oriundos, derivados ou conexos com o contrato, ficando ainda, para todos os efeitos legais, consignada, pela CONTRATADA, a inexistência de qualquer vínculo empregatício entre seus empregados/prepostos e a Prefeitura Municipal de Iconha.

6.1.16. Agir com total diligência em eventuais reclamações trabalhistas promovidas por seus empregados que estejam ou, em algum momento, estiveram envolvidos na prestação de serviços objeto deste contrato, comparecendo em todas as audiências designadas, apresentando as necessárias contestações e recursos cabíveis, ainda que extinta a relação contratual com a Prefeitura Municipal de Iconha. A omissão da CONTRATADA, nas demandas dessa natureza, será considerada falta grave, sujeitando-se à aplicação das sanções previstas neste contrato, assegurada a prévia defesa.

6.1.17. Indenizar todas as despesas e custos financeiros que porventura venham a ser suportados pela Prefeitura Municipal de Iconha, por força de sentença judicial que reconheça a responsabilidade subsidiária ou solidária da Prefeitura por créditos devidos aos empregados da CONTRATADA, ainda que extinta a relação contratual entre as partes.

6.1.18. Respeitar e fazer cumprir as normas de segurança e medicina do trabalho previstas na legislação pertinente.

6.1.19. Manter seus empregados, quando em serviço nas dependências da Prefeitura Municipal, devidamente uniformizados. A indumentária de identificação deverá ser oferecida pela CONTRATADA às suas expensas.

6.1.20. Dispor-se a toda e qualquer fiscalização da Prefeitura, no tocante à prestação do serviço, assim como ao cumprimento das obrigações previstas neste contrato.

6.1.21. Fiscalizar o perfeito cumprimento do serviço a que se obrigou, cabendo-lhe integralmente os ônus decorrentes.

6.1.22. Estruturar-se de modo compatível e prover toda a infraestrutura necessária à prestação do serviço previstos neste contrato, com a qualidade e rigor exigidos, garantindo a sua supervisão desde a implantação.

6.1.23. Prover todos os meios necessários à garantia da prestação do serviço contratados, inclusive nos casos de greve ou paralisação de qualquer natureza.

6.1.24. Manter, durante o prazo contratual, todas as qualificações exigidas na licitação, nos termos do Art. 92, XVI, da Lei 14.133/21.

6.1.25. Manter perante a Prefeitura de Iconha durante a vigência do contrato, seu endereço comercial completo (logradouro, cidade, UF, CEP) e eletrônico, telefone, fax e nome dos seus representantes sempre atualizados, para fins de comunicação e encaminhamento de informações e documentos, inclusive os relativos a tributos.

6.1.26. Não manter relação de emprego/trabalho, de forma direta ou indireta, com menor de 18 anos de idade em trabalho noturno, perigoso ou insalubre, nem menor de 16 anos de idade em qualquer trabalho, salvo na condição de aprendiz, a partir dos 14 anos.

6.1.27. Assegurar a não utilização de trabalho em condições degradantes ou em condições análogas à escravidão e de práticas discriminatórias em razão de crença religiosa, raça, cor, sexo, partido político, classe social, nacionalidade.

6.1.28. Comunicar, por escrito, imediatamente, à Fiscalização do contrato, a impossibilidade de execução de qualquer obrigação contratual, para a adoção das providências cabíveis.

6.1.29. Responsabilizar-se por todo e qualquer dano que seus prepostos, empregados, mandatários causar à Prefeitura Municipal de Iconha ou a terceiros, ainda que culposo, não excluindo ou reduzindo essa responsabilidade a fiscalização ou acompanhamento pela Prefeitura.

6.1.30. Responsabilizar-se por qualquer tipo de autuação ou ação que venha a sofrer em decorrência da prestação do serviço, bem como pelos contratos de trabalho de seus empregados, mesmo nos casos que envolvam eventuais

decisões judiciais, assegurando a Prefeitura o exercício do direito de regresso, eximindo a Prefeitura de qualquer solidariedade ou responsabilidade.

6.1.31. Responsabilizar-se por quaisquer multas, indenizações ou despesas impostas a Prefeitura, por autoridade competente, em decorrência do descumprimento de lei ou de regulamento a ser observado na execução do contrato pela CONTRATADA, as quais serão reembolsadas a Prefeitura.

6.1.32. A CONTRATADA autoriza a Prefeitura descontar o valor correspondente aos referidos danos ou prejuízos diretamente das notas fiscais/faturas pertinentes aos pagamentos que lhe forem devidos em relação a este contrato, e/ou das notas fiscais/faturas de quaisquer outros contratos que porventura a CONTRATADA mantenha com a Prefeitura, independentemente de qualquer procedimento judicial, depois de assegurada a prévia defesa em processo administrativo para apuração dos fatos.

7. DA SUBCONTRATAÇÃO

Até regulamentação interna que estabelecerá os casos e percentuais de subcontratação, não será admitida a subcontratação do objeto.

8. DA VIGÊNCIA DA CONTRATAÇÃO

O fornecimento do bem será realizado em uma única etapa com suporte técnico com vigência de 36 meses.

9. DO PAGAMENTO

9.1. A Nota Fiscal/Fatura deverá ser protocolizada juntamente com a solicitação de pagamento.

9.2. A Prefeitura Municipal de Iconha/ES promoverá o pagamento, em conta corrente, mediante ordem bancária, num prazo de até 30 (trinta) dias contados da data do ateste na Nota Fiscal/Fatura realizado por servidor designado.

10. DO REAJUSTE

Os preços serão expressos em reais e fixos e irreajustáveis, durante a vigência do contrato.

11. DAS SANÇÕES ADMINISTRATIVAS

11.1. Comete infração administrativa o fornecedor que infringir as disposições previstas no art. 155 da Lei nº 14.133/2021, quais sejam:

11.1.1. dar causa à inexecução parcial do contrato;

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

11.1.3. dar causa à inexecução total do contrato;

11.1.4. deixar de entregar a documentação exigida para o certame;

11.1.5. não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

11.1.6. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

11.1.7. ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

11.1.8. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

11.1.9. fraudar a dispensa ou praticar ato fraudulento na execução do contrato;

11.1.10. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

11.1.11. considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de negociação;

11.1.12. praticar atos ilícitos com vistas a frustrar os objetivos desta Dispensa;

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

11.2. O fornecedor que cometer qualquer das infrações discriminas nos subitens anteriores, em processo de aplicação de penalidade, estará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) Advertência pela falta do subitem 11.1.1, quando não se justificar a imposição de penalidade mais grave;

b) Multa sobre o valor estimado dos itens prejudicados pela conduta do por quaisquer das infrações dos itens 11.1.1 a 11.1.12;

c) Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, nos casos dos subitens 11.1.2 a 11.1.7, quando não se justificar a imposição de penalidade mais grave;

d) Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes municipais, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 11.1.8 a 11.1.12, bem como nos demais casos que justifiquem a imposição da penalidade mais grave.

11.3. Na aplicação das sanções serão considerados:

11.3.1. a natureza e a gravidade da infração cometida;

11.3.2. as peculiaridades do caso concreto;

11.3.3. as circunstâncias agravantes ou atenuantes;

11.3.4. os danos que dela provierem para a Administração Pública;

11.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

11.4. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

11.5. A aplicação das sanções previstas neste Termo não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

11.6. Na aplicação da sanção prevista na alínea “b” do item 13.2 deste Termo, será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

11.7. Para aplicação das sanções previstas nas alíneas “c” e “d” do item 13.2 deste Termo será instaurado processo de responsabilização, a ser conduzido por comissão composta de 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o contratado para, no prazo de 15 (quinze) dias úteis, contado da data de intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

11.8. Quando o quadro funcional não dispor de servidores estatutários, a comissão a que se refere o item anterior será composta de 2 (dois) ou mais empregados públicos pertencentes aos seus quadros permanentes, preferencialmente com, no mínimo, 3 (três) anos de tempo de serviço no órgão ou entidade.

11.9. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

11.10. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao fornecedor/adjudicatário, observando-se os demais procedimentos previstos na Lei nº 14.133/2021.

12. DA ESTIMATIVA DE PREÇOS

O valor total estimado da contratação é de R$ 44.687,54 (quarenta e quatro mil, seiscentos e oitenta e sete reais e cinquenta e quatro centavos).

13. DOS RECURSOS ORÇAMENTÁRIOS

As despesas decorrentes da presente contratação correrão por conta da seguinte dotação orçamentária:

Secretaria	Ficha	Natureza de Despesa	Fonte de Recursos
ADMINISTRAÇÃO	86	33904000000	172000000000

GABINETE/PROJUR/UCCI	24	33904000000	150000009999
FINANÇAS	126	33904000000	150000009999
SEME	172	33904000000	150000250000
OBRAS	983	33904000000	150000009999
SEMAG	853	33903600000	150000009999
SEMMA	371	33904000000	150000009999
SETCUL	1500	33903900000	1074
SEMADES	430, 461, 671, 692, 720, 798 e 799	33903900000	1500, 1660 e 1661

Iconha/ES, 07 de agosto de 2025.

Elaborado por:

TASSIANE PERUGGIA RIBEIRO
Subsecretaria Municipal de Administração

Aprovado por:

JANDERSON DA SILVA MOTA
Secretário Municipal de Administração

ANEXO II

MODELO DE PROPOSTA DE PREÇOS

(PAPEL TIMBRADO DA EMPRESA LICITANTE)

Nome da empresa (razão social):.....

Endereço:.....

Cidade:.....UF:.....CEP:.....

CNPJ n.....Telefone/fax:.....

E-mail:.....

F. Responsável pela assinatura do(a) contrato/ata:

Nome:.....E-mail:.....

Cargo/função:.....Telefone/fax:.....

G. Dados bancários (com dígito verificador):

Banco n.:.....Agência n.:.....Conta-corrente n.:.....

A presente proposta tem como objeto a aquisição dos itens ou contratação dos serviços abaixo discriminados, em conformidade com as especificações, quantidades e demais condições definidas no edital e seus anexos.

ITEM	DESCRIÇÃO	UNID	QUANT	VALOR UNITÁRIO (R$)	VALOR TOTAL(R$)
1					
2					

Declaro que cumpro e acato todos os dispositivos estabelecidos no edital e seus

anexos.

....., ... de ..... de 2024.

(nome e assinatura do responsável)

ANEXO III

ORÇAMENTO ESTIMATIVO

(papel timbrado da licitante)

ITEM	DESCRIÇÃO	QUANT	UND	VALOR UNITARIO DE REFERENCIA (R$)	VALOR TOTAL DE REFERÊNCIA (R$)	INTERVALO MINIMO DE LANCES (R$ OU %)
1						
2						

ANEXO IV

MODELO DE DECLARAÇÕES A SEREM APRESENTADAS

PARA FINS DE HABILITAÇÃO.

(papel timbrado da licitante)

A – DECLARAÇÃO NEGATIVA DE RELAÇÃO FAMILIAR OU PARENTESCO.

(nome da pessoa física/jurídica) _____, inscrita no CNPJ/CPF sob n° _____, por intermédio de seu representante legal, o (a) Sr (a)._____ portador (a) do CPF n° _____, domiciliado na _____, DELCARA, para todos os efeitos legais que:

1. Não possui sócio (s) ou, no caso de sociedade anônima, diretor (es) que seja (m):

a) cônjuge(s), companheiro(s) ou tenha(m) parentesco em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, com servidores ocupantes de cargos de direção, chefia e assessoramento vinculados direta ou indiretamente às unidades situadas na linha hierárquica da área encarregada da licitação deste Município, ou que tenham ocupado os mencionados cargos, nos 6 (seis) meses anteriores à data de abertura da sessão pública do procedimento licitatório.

2. Está ciente da vedação:

a) da subcontratação, quando autorizada pelo CONTRATANTE, de pessoa física ou jurídica se aquela ou os dirigentes desta mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com servidor ocupante de cargo de direção, chefia ou assessoramento vinculado direta ou indiretamente a unidade situada na linha hierárquica da área encarregada da licitação, ou se deles forem companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau inclusive; e

b) Da manutenção, aditamento ou prorrogação de contrato de prestação de serviços, caso a CONTRATADA venha a contratar empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento, de Secretário da pasta requisitante e/ou gestora da contratação ou de Prefeito e Vice Prefeito.

3. São verdadeiras as informações prestadas no presente documento, sob pena de responsabilidade civil, administrativa e penal.

B – DECLARAÇÃO DE CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS – LEI N°.13.709/2018

1. É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal.
2. As partes se comprometem a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoas sensíveis – repassados em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018, sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do edital/instrumento contratual.
3. As partes responderão administrativa e judicialmente, em caso de causarem danos patrimoniais, morais, individual ou coletivo, aos titulares de dados pessoais, repassados em decorrência da execução contratual, por inobservância à LGPD.
4. Em atendimento ao disposto na Lei n. 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), o CONTRATANTE, para a execução do serviço objeto deste edital, terá acesso aos dados pessoais dos representantes da CONTRATADA, tais como: número do CPF e do RG, endereço eletrônico, cópia do documento de identificação.
5. A CONTRATADA, declara que tem ciência da existência da Lei Geral de Proteção de Dados (LGPD) e, se compromete a adequar todos os procedimentos internos ao disposto na legislação, com intuito de proteção dos dados pessoais repassados pelo CONTRATANTE.
6. A CONTRATADA, fica obrigada a comunicar ao CONTRATANTE, em até 24 (vinte e quatro) horas, qualquer incidente de acessos não

autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito que possa vir a causar risco ou dano relevante aos Titulares de Dados Pessoais, apresentando as informações descritas nos incisos do 1° do art. 48 da LGPD, cabendo ao CONTRATANTE as demais obrigações de comunicação previstas no referido artigo.

C – DECLARAÇÃO DE INTEGRALIDADE DOS CUSTOS

A LICITANTE/CONTRATADA/DETENTORA DA ATA, declara 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.

D – DECLARAÇÃO DE QUE PODE USUFRUIR DOS BENEFÍCIOS DE ME E EPP

A LICITANTE/CONTRATADA/DETENTORA DA ATA declara, para todos os efeitos, que, no ano-calendário de realização da licitação, não celebrou contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, para fins de obtenção dos benefícios previstos dos artigos 42 a 49 da Lei Complementar n°. 123/2006

MINUTA DE CONTRATO Nº. XXX/2025.

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NO FORNECIMENTO DE LICENÇAS DO SOFTWARE KASPERSKY NEXT EDR FOUNDATIONS BRAZILIAN EDITION E SUPORTE TECNICO, PARA ATENDER AS DEMANDAS DAS SECRETARIAS MUNICIPAIS, QUE ENTRE SI CELEBRAM O MUNICÍPIO DE ICONHA, ESTADO DO ESPÍRITO SANTO, E A EMPRESA XXXX.

O **MUNICÍPIO DE ICONHA**, Estado do Espírito Santo, por seu órgão administrativo, a Prefeitura Municipal, sediada à Praça Darcy Marchiori, nº. 11, Jardim Jandira, nesta cidade, inscrito no CNPJ sob nº. 27.165.646/0001-85, doravante denominado simplesmente **CONTRATANTE,** neste ato representado pelo Prefeito Municipal, o **Sr**. **Gedson Brandão Paulino**, brasileiro, divorciado, portador do RG n.º 1.562.453 – SPTC/ES, inscrito no CPF n.º 083.592.647-83, Endereço Comercial: Praça Darcy Marchiori, 11, Jardim Jandira, Iconha - ES, de outro lado, a empresa _____, pessoa jurídica de direito privado, inscrita no CNPJ n° _____, estabelecida na rua _____, nº _____, bairro _____, cidade/UF, CEP nº _____, neste ato representado legalmente pelo Sr. (a) _____, inscrito no CPF sob o nº _____ e documento de identidade sob o nº _____, doravante denominada **CONTRATADA**, resolvem celebrar a presente **CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NO FORNECIMENTO DE LICENÇAS DO SOFTWARE KASPERSKY NEXT EDR FOUNDATIONS BRAZILIAN EDITION E SUPORTE TECNICO, PARA ATENDER AS DEMANDAS DAS SECRETARIAS MUNICIPAIS,** na forma da Lei Federal n°. 14.133/2021, a Lei Complementar n°. 123/2006, subsidiariamente de outras normas aplicáveis, realizara licitação, com ampla participação ou com participação exclusiva de microempresas e empresas de pequeno porte ou com cotas reservadas para microempresas e empresas de pequeno porte, do tipo MENOR PREÇO/MAIOR DESCONTO por item, mediante as condições estabelecidas neste edital.

1) CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O presente contrato tem por objeto a Contratação de empresa especializada no fornecimento Licenças do Software Kaspersky Next EDR Foundations Brazilian Edition e Suporte Técnico, para atender as demandas da Prefeitura de Iconha, de acordo com as condições e especificações constantes do Pregão Eletrônico n.º 21/2025 – Processo Administrativo n.º 2025-S4W6M.

2) CLÁUSULA SEGUNDA – DO LOCAL E PRAZO DE ENTREGA

2.1 Da forma de requisição do serviço: A CONTRATADA deve obedecer, no ato da entrega da licença a ser adquirido, os requisitos descritos nesse termo de referência;

2.2 Do prazo para entrega do serviço: A licença deverá ser fornecimento após recebimento da Ordem de Serviço;

2.3 Do prazo para a substituição no caso de defeito: Caso as licenças estejam em desacordo com o especificado, os mesmos devem ser substituídos imediatamente, sem que haja prejuízo à realização das atividades administrativas municipais e o funcionamento dos sistemas eletrônicos de uso rotineiro dos servidores;

3) CLÁUSULA TERCEIRA – DO PREÇO, VALOR DO CONTRATO E CONDIÇÕES DE PAGAMENTO

3.1. O valor total do presente contrato é de R$ ____.

3.2. Os valores totais e unitários acordados para a aquisição do objeto estão detalhados no Anexo II.

3.3. O pagamento será efetuado em conta corrente, mediante ordem bancária, em **30 (trinta) dias** contados da apresentação da Nota Fiscal/Fatura, devidamente discriminada e atestada por servidor designado.

3.4. Poderão ser descontados dos pagamentos os valores atinentes a penalidades eventualmente aplicadas.

3.5. Em nenhuma hipótese haverá antecipação de pagamento.

3.6. Havendo erro na nota fiscal, a mesma será devolvida à licitante vencedora.

3.7. Qualquer irregularidade que impeça a liquidação da despesa será comunicada à licitante vencedora, ficando o pagamento pendente até que se providenciem as medidas saneadoras.

3.8. No valor ajustado para o fornecimento, deverão estar incluídos todos os insumos e os tributos, inclusive contribuições fiscais e para-fiscais, previdenciárias e encargos trabalhistas, bem como quaisquer outras despesas necessárias à execução deste CONTRATO.

3.9. O licitante deverá manter as mesmas condições previstas neste edital no que concerne à PROPOSTA e HABILITAÇÃO, especialmente quanto às certidões de regularidade do INSS e FGTS, sendo que, caso ocorra alguma irregularidade na documentação, poderá ser instaurado procedimento de rescisão contratual, sem prejuízo das sanções legais cabíveis, conforme entendimento do STJ e do TCU.

4) CLÁUSULA QUARTA - DO REAJUSTE

4.1. Os valores contratados são fixos e irreajustáveis no prazo de um ano contado da data da proposta, em --/--/2025.

5) CLÁUSULA QUINTA – DO CRÉDITO ORÇAMENTÁRIO

5.1. Os recursos orçamentários para o cumprimento das obrigações assumidas pela PMI para este Edital correrão por conta de recursos financeiros:

Secretaria	Ficha	Natureza de Despesa	Fonte de Recursos
ADMINISTRAÇÃO	86	33904000000	172000000000
GABINETE/PROJUR/UCCI	24	33904000000	150000009999
FINANÇAS	126	33904000000	150000009999
SEME	172	33904000000	150000250000
OBRAS	983	33904000000	150000009999
SEMAG	853	33903600000	150000009999
SEMMA	371	33904000000	150000009999
SETCUL	1500	33903900000	1074
SEMADES	430, 461, 671,	33903900000	1500, 1660 e 1661

	692, 720, 798 e 799		

1 - **6) CLÁUSULA SEXTA – DAS OBRIGAÇÕES DO CONTRATANTE**

6.1. A contratante obriga-se a:

I. Propiciar todas as facilidades, inclusive esclarecimentos atinentes ao objeto deste Contrato, para que a empresa possa cumprir as obrigações dentro das normas e condições da aquisição.

II. Efetuar o pagamento à CONTRATADA, de acordo com o previsto neste instrumento.

III. Comunicar imediatamente à empresa qualquer irregularidade manifestada na entrega do objeto.

IV. Atestar a entrega do objeto por meio do servidor designado para fiscalização do contrato.

7) CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DA CONTRATADA

7.1 Prestar o serviço, cotado em estrita conformidade com as especificações de sua proposta, à qual se vincula, não sendo admitidas retificações, cancelamentos, quer seja nos preços, quer seja nas condições estabelecida.

7.2 Não transferir a outrem, no todo ou em parte, o bem adjudicado, sem prévia e expressa anuência desta Prefeitura.

7.3 Propiciar todas as facilidades indispensáveis à fiscalização da execução do serviço.

7.4 Executar o serviço contratado em prazo não superior ao máximo estipulado na proposta. Caso tal serviço não seja executado dentro do prazo, a CONTRATADA ficará sujeita à multa.

7.5 Responder por todas as despesas de qualquer natureza relativas a fretes, embalagens, transportes, seguros, impostos, taxas, encargos sociais, trabalhistas, previdenciários, e todos os demais custos necessários ao cumprimento do serviço e à execução da contratação.

7.6 Cumprir outras obrigações previstas no Código de Proteção e Defesa do Consumidor (Lei n° 8.078/90) que sejam compatíveis com o regime de direito público.

7.7. Executar, perfeita e integralmente, o serviço contratado, no horário estabelecido pela Administração Pública Municipal e nos prazos ajustados, por meio de pessoas idôneas/tecnicamente capacitadas, obrigando-se a indenizar o Município de Iconha, mesmo em caso de ausência ou omissão de fiscalização de sua parte, por quaisquer danos causados às suas instalações, móveis, utensílios, máquinas e equipamentos, quer sejam eles praticados por empregados, prepostos ou mandatários seus. A responsabilidade estender-se-á aos danos causados a terceiros durante a prestação do serviço.

7.7 Dar como conferido e perfeito o serviço prestado, cumprindo, rigorosamente, o prazo estabelecido pela Administração Pública Municipal e responsabilizando- se por quaisquer prejuízos que suas falhas ou imperfeições venham causar a Prefeitura Municipal de Iconha ou a terceiros, de modo direto ou indireto, além de realizar novamente o serviço incorreto, se for o caso, sem quaisquer ônus para o Município de Iconha e sem prejuízo das multas contratuais previstas.

7.9 Efetuar, de imediato, o afastamento de qualquer profissional, quando se verificar o seguinte:

7.9.1 Atuação ou comportamentos julgados inconvenientes ou prejudiciais ao bom andamento do serviço;

7.9.2 Ocorrência sistemática de erros ou falhas na execução dos trabalhos;

7.9.3 Atos que comprometam a própria segurança ou a de terceiros;

7.9.4 Não atendimento às determinações do preposto.

7.10 Diligenciar para que seus empregados tratem com urbanidade os funcionários da Prefeitura Municipal de Iconha, bem como ao jurisdicionado, visitantes e demais contratados.

7.11 Dar ciência ao Gabinete do Prefeito, imediatamente e por escrito, de qualquer anormalidade que verificar no fornecimento do bem.

7.12 Prestar os esclarecimentos que lhe forem solicitados, atendendo prontamente a todas as reclamações e convocações da Prefeitura Municipal de Iconha.

7.13 Diligenciar para que seus empregados não prestem serviços que não os previstos no objeto deste contrato.

7.14 Apresentar à Prefeitura Municipal de Iconha o requerimento de pagamento pelo serviço prestado, juntamente com a fatura/nota fiscal, Certidão conjunta negativa de débitos relativos aos tributos federais e à Dívida Ativa da União; Certidão negativa de débitos relativos às contribuições previdenciárias e às de terceiros; Certificado de Regularidade do FGTS.

7.15 Assumir todas as despesas e ônus relativos ao pessoal e quaisquer outros oriundos, derivados ou conexos com o contrato, ficando ainda, para todos os efeitos legais, consignada, pela CONTRATADA, a inexistência de qualquer vínculo empregatício entre seus empregados/prepostos e a Prefeitura Municipal de Iconha.

7.16 Agir com total diligência em eventuais reclamações trabalhistas promovidas por seus empregados que estejam ou, em algum momento, estiveram envolvidos na prestação de serviços objeto deste contrato, comparecendo em todas as audiências designadas, apresentando as necessárias contestações e recursos cabíveis, ainda que extinta a relação contratual com a Prefeitura Municipal de Iconha. A omissão da CONTRATADA, nas demandas dessa natureza, será considerada falta grave, sujeitando-se à aplicação das sanções previstas neste contrato, assegurada a prévia defesa.

7.17 Indenizar todas as despesas e custos financeiros que porventura venham a ser suportados pela Prefeitura Municipal de Iconha, por força de sentença judicial que reconheça a responsabilidade subsidiária ou solidária da Prefeitura por créditos devidos aos empregados da CONTRATADA, ainda que extinta a relação contratual entre as partes.

7.18 Respeitar e fazer cumprir as normas de segurança e medicina do trabalho previstas na legislação pertinente.

7.19 Manter seus empregados, quando em serviço nas dependências da Prefeitura Municipal, devidamente uniformizados. A indumentária de identificação deverá ser oferecida pela CONTRATADA às suas expensas.

7.20 Dispor-se a toda e qualquer fiscalização da Prefeitura, no tocante à prestação do serviço, assim como ao cumprimento das obrigações previstas neste contrato.

7.21 Fiscalizar o perfeito cumprimento do serviço a que se obrigou, cabendo-lhe integralmente os ônus decorrentes.

7.22 Estruturar-se de modo compatível e prover toda a infraestrutura necessária à prestação do serviço previstos neste contrato, com a qualidade e rigor exigidos, garantindo a sua supervisão desde a implantação.

7.23 Prover todos os meios necessários à garantia da prestação do serviço contratados, inclusive nos casos de greve ou paralisação de qualquer natureza.

7.24 Manter, durante o prazo contratual, todas as qualificações exigidas na licitação, nos termos do Art. 92, XVI, da Lei 14.133/21.

7.25 Manter perante a Prefeitura de Iconha durante a vigência do contrato, seu endereço comercial completo (logradouro, cidade, UF, CEP) e eletrônico, telefone, fax e nome dos seus representantes sempre atualizados, para fins de comunicação e encaminhamento de informações e documentos, inclusive os relativos a tributos.

7.26 Não manter relação de emprego/trabalho, de forma direta ou indireta, com menor de 18 anos de idade em trabalho noturno, perigoso ou insalubre, nem menor de 16 anos de idade em qualquer trabalho, salvo na condição de aprendiz, a partir dos 14 anos.

7.27 Assegurar a não utilização de trabalho em condições degradantes ou em condições análogas à escravidão e de práticas discriminatórias em razão de crença religiosa, raça, cor, sexo, partido político, classe social, nacionalidade.

7.28 Comunicar, por escrito, imediatamente, à Fiscalização do contrato, a impossibilidade de execução de qualquer obrigação contratual, para a adoção das providências cabíveis.

7.29 Responsabilizar-se por todo e qualquer dano que seus prepostos, empregados, mandatários causar à Prefeitura Municipal de Iconha ou a terceiros, ainda que culposo, não excluindo ou reduzindo essa responsabilidade a fiscalização ou acompanhamento pela Prefeitura.

7.30 Responsabilizar-se por qualquer tipo de autuação ou ação que venha a sofrer em decorrência da prestação do serviço, bem como pelos contratos de trabalho de seus empregados, mesmo nos casos que envolvam eventuais decisões judiciais, assegurando a Prefeitura o exercício do direito de regresso, eximindo a Prefeitura de qualquer solidariedade ou responsabilidade.

7.31 Responsabilizar-se por quaisquer multas, indenizações ou despesas impostas a Prefeitura, por autoridade competente, em decorrência do descumprimento de lei ou de regulamento a ser observado na execução do contrato pela CONTRATADA, as quais serão reembolsadas a Prefeitura.

7.32 A CONTRATADA autoriza a Prefeitura descontar o valor correspondente aos referidos danos ou prejuízos diretamente das notas fiscais/faturas pertinentes aos pagamentos que lhe forem devidos em relação a este contrato, e/ou das notas fiscais/faturas de quaisquer outros contratos que porventura a CONTRATADA mantenha com a Prefeitura, independentemente de qualquer procedimento judicial, depois de assegurada a prévia defesa em processo administrativo para apuração dos fatos.

8) CLÁUSULA OITAVA – DAS CONDIÇÕES DE RECEBIMENTO DO MATERIAL

a) A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:

i. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.

ii. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.

iii. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).

iv. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.

v. A solução proposta deve suportar o subsistema Linux no Windows.

vi. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

1. Proteção contra ameaças sem arquivos (Fileless);
2. Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;
3. A solução proposta deve fornecer varredura de memória para estações

de trabalho Windows;

4. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.

vii. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.

viii. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.

ix. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.

x. A solução proposta deve fornecer análise comportamental baseada em machine learning.

xi. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.

xii. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:

1. Controles de aplicativos;
2. Controle web e dispositivos;
3. HIPS e Firewall;
4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;
5. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.

xiii. A solução proposta deve ser protegida por senha para evitar que o processo do antimalware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.

xiv. A solução proposta deve ter bancos de dados de reputação locais e globais.

xv. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e

FTP contra malwares.

xvi. A solução proposta deve incluir um módulo capaz, no mínimo, de:

1. Bloqueio de aplicativos com base em sua categorização;

2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos;

3. A adição de sub-redes e a modificação de permissões de atividade.

xvii. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.

xviii. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.

xix. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.

xx. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.

xxi. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.

xxii. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.

xxiii. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.

xxiv. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.

xxv. A solução proposta deve incluir um componente dedicado para verificação de

conexões criptografadas.

xxvi. A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.

xxvii. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;

xxviii. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;

xxix. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.

xxx. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.

xxxi. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.

xxxii. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.

xxxiii. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.

xxxiv. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.

xxxv. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.

xxxvi. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.

xxxvii. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.

xxxviii. A solução proposta deve ter categoria de detecção para bloquear banners de sites.

xxxix. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos

móveis;

xl. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.

xli. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.

xlii. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.

xliii. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;

xliv. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.

xlv. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.

xlvi. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.

xlvii. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.

xlviii. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.

xlix. A solução proposta deve suportar o controle de scripts executados em PowerShell.

l. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.

li. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.

lii. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.

liii. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.

liv. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.

lv. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.

lvi. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:

1. Filtro de anexos;
2. Verificação de mensagens de email ao receber, ler e enviar.

lvii. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.

lviii. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo.

lix. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.).

lx. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.

lxi. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.

lxii. A solução proposta deve incluir suporte ao protocolo IPv6.

lxiii. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.

lxiv. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:

1. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo;
2. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.

lxv. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.

lxvi. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.

lxvii. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.

lxviii. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.

lxix. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.

lxx. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.

lxxi. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.

lxxii. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia, bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.

lxxiii. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.

lxxiv. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.

lxxv. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.

lxxvi. A solução proposta deve suportar endereços IPv6.

lxxvii. A solução proposta deve suportar verificação em duas etapas (autenticação).

lxxviii. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu

funcionamento.

lxxix. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.

lxxx. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.

lxxxi. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.

lxxxii. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.

lxxxiii. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.

lxxxiv. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.

lxxxv. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos.

lxxxvi. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.

lxxxvii. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi, Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.

lxxxviii. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.

lxxxix. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.

xc. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado.

xci. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.

xcii. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.

xciii. A solução proposta deve ter a capacidade de excluir atualizações baixadas.

xciv. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.

xcv. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.

xcvi. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.

xcvii. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.

xcviii. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.

xcix. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.

c. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.

ci. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.

cii. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:

ciii. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.

civ. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.

cv. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.

cvi. A solução proposta deve gerar relatórios de vulnerabilidades encontradas nos dispositivos com sensor de endpoint instalado.

b. Do módulo de gerenciamento de dispositivos móveis:

i. O modulo deve ser integrado a console de gerenciamento;

ii. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition);

iii. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

1. iOS 10–17 ou iPadOS 13–17;

iv. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.

v. A solução proposta deve suportar dispositivos iOS supervisionados.

vi. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.

vii. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.

viii. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.

ix. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).

x. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.

xi. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

xii. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.

xiii. A solução proposta deve ter recursos de conteinerização para dispositivos Android.

xiv. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:

1. Dados em contêineres;

2. Contas de e-mail corporativo;

3. Configurações para conexão à rede Wi-Fi corporativa e VPN;

4. Nome do ponto de acesso (APN);

5. Perfil do Android for Work;

6. Recipiente KNOX;

7. Chave do gerenciador de licença KNOX.

xv. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:

1. Todos os perfis de configuração instalados;

2. Todos os perfis de provisionamento;

3. O perfil iOS MDM;

4. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas.

xvi. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:

1. Critérios de verificação do dispositivo;

2. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;

xvii. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.

xviii. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:

1. Cartões de memória e outras unidades removíveis;

2. Câmera do dispositivo;

3. Conexões Wi-Fi;
4. Conexões Bluetooth;
5. Porta de conexão infravermelha;
6. Ativação do ponto de acesso Wi-Fi;
7. Conexão de área de trabalho remota;
8. Sincronização de área de trabalho;
9. Definir configurações da caixa de correio do Exchange;
10. Configurar caixa de e-mail em dispositivos iOS MDM;
11. Configure contêineres Samsung KNOX;
12. Definir as configurações do perfil do Android for Work;
13. Configurar e-mail/calendário/contatos;
14. Defina as configurações de restrição de conteúdo de mídia;
15. Definir configurações de proxy no dispositivo móvel;
16. Configurar certificados e SCEP.

xix. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay.

xx. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:

1. Google Play, Huawei App Gallery e Apple App Store;
2. Portal de inscrição móvel KNOX;
3. Pacotes de instalação pré-configurados independentes.

xxi. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.

xxii. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.

xxiii. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:

1. VMware AirWatch 9.3 ou posterior;
2. MobileIron 10.0 ou posterior;
3. IBM MaaS360 10.68 ou posterior;

4. Microsoft Intune 1908 ou posterior;
5. SOTI MobiControl 14.1.4 (1693) ou posterior.

xxiv. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.

xxv. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:

1. Google Play;
2. Galeria de aplicativos Huawei;
3. Loja de aplicativos da Apple.

xxvi. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.

xxvii. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.

xxviii. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.

xxix. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.

xxx. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.

xxxi. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.

xxxii. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.

xxxiii. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.

xxxiv. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.

xxxv. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.

xxxvi. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.

xxxvii. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.

xxxviii. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;

xxxix. A solução proposta deve proteger contra ameaças online em dispositivos iOS.

c. 3.8. Do módulo de EDR:

i. Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.

ii. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.

iii. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças.

iv. Deve apresentar as seguintes informações:

1. Processo;
2. Arquivos;
3. Chaves de registros;
4. Conexões de rede;
5. SHA256 e MD5.

v. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise.

vi. Deve apresentar informações detalhadas contendo:

1. Usuário que executou a ação;
2. Informações acesso privilegiado.

d. Requisitos para documentação da solução:

i. A documentação da solução do anti-malware incluindo ferramentas de administração, deve incluir os seguintes documentos:

1. Ajuda on-line para administradores;
2. Ajuda on-line para melhores práticas de implementação;
3. Ajuda on-line para proteção de servidores de administração.

ii. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software antimalware.

iii. Deve estar disponível página com informações de ciclo de vida das soluções e módulos.

e. 3.10. Do módulo de gerenciamento simplificado:

b) A solução proposta deve suportar arquitetura cloud.

c) A solução proposta deve incluir um console web integrado para o gerenciamento do endpoint, que não deve exigir nenhuma instalação adicional.

d) O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

e) A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.

f) A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.

g) A solução proposta deve atender as condições apontadas no item e subintes 6.

h) A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.

i) A solução proposta deve incluir informações do endpoint:

i. IP público de internet;
ii. IP interno do dispositivo;
iii. Versão do agente de proteção;
iv. Última comunicação com a console, contendo data e hora;
v. Informações do sistema operacional.

b. Do módulo de gerenciamento avançado:

j) A solução proposta deve suportar arquitetura cloud-native e on-premisse.

k) A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:

i. Amazon Web Services;
ii. Microsoft Azure.

l) A solução proposta deve incluir as seguintes opções de integração SIEM:

i. HP (Microfoco) ArcSight;
ii. IBM QRadar;
iii. Splunk;
iv. Kaspersky KUMA.

m)A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

n) A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;

o) A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

p) O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

q) A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

r) A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

s) A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.

t) A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

u) A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.

v) O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

w) O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação:

i. Status do dispositivo;
ii. Tag;
iii. Diretório ativo;
iv. Proprietários de dispositivos;
v. Hardware.

x) A solução proposta deve suportar os seguintes canais de entrega de notificação:

i. E-mail;
ii. Registro de sistema;
iii. SMS.

y) A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:

i. Atributos de rede;
ii. Nome;
iii. Domínio e/ou Sufixo de Domínio;
iv. Endereço de IP;
v. Endereço IP para servidor de gerenciamento;
vi. Localização no Active Directory;
vii. Unidade organizacional;
viii. Grupo;
ix. Sistema operacional;
x. Número do pacote de serviço;

xi. Arquitetura Virtual;
xii. Registro de aplicativos;
xiii. Nome da Aplicação;
xiv. Versão do aplicativo;
xv. Fabricante;
xvi. Tipo e versão;
xvii. Arquitetura.

z) A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.

aa) A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.

As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:

i. Dispositivos Desktop/Servidores;
ii. Dispositivos móveis;
iii. Dispositivos de rede;
iv. Dispositivos virtuais;
v. Componentes OEM;
vi. Periféricos de computador;
vii. Dispositivos IoT conectados;
viii. Telefones VoIP;
ix. Repositórios de rede.

bb) A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:

i. Nome da Aplicação;
ii. Caminho do aplicativo;
iii. Metadados do aplicativo;
iv. Aplicativo Certificado digital;
v. Categorias de aplicativos predefinidas pelo fornecedor;
vi. SHA256 e MD5.

cc) A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:

i. Bluetooth;
ii. Dispositivos móveis;
iii. Modems externos;
iv. CD/DVD;
v. Câmeras e scanners;
vi. MTPs;
vii. E a transferência de dados para dispositivos móveis.

dd) A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

ee) A solução sugerida deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.

ff) A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

i. Estruturas de domínios e grupos de trabalho do Windows;
ii. Estruturas de grupos do Active Directory;
iii. Conteúdo de um arquivo de texto criado manualmente pelo administrador.

gg) A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.

hh) A solução proposta deve permitir realizar as seguintes ações para endpoints:

i. Verificação manual;
ii. Verificação no acesso;
iii. Verificação por demanda;
iv. Verificação de arquivos compactados;
v. Verificação de arquivos individuais, pastas e unidades;
vi. Bloqueio e verificação de scripts;
vii. Proteção contra alteração de registros;

viii. Proteção contra estouro de buffer;

ix. Verificação em segundo plano/inativa.

ii) Verificação de unidade removível na conexão com o sistema;

jj) A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou antimalware.

kk) O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.

ll) A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.

mm) A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.

nn) A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.

oo) A solução proposta deve suportar Windows Failover Cluster.

pp) A solução proposta deve ter um recurso de clustering integrado.

qq) A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.

rr) A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.

ss) O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.

tt) A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.

A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.

uu) A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.

vv) A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.

ww) A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.

xx) A solução proposta deverá possuir controles para download de DLL e drivers.

yy) A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo especifico de prevenção de intrusão.

zz) A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.

aaa) A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).

bbb) A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.

ccc) A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.

ddd) A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.

eee) A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.

fff)A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.

ggg) A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança antimalware através do servidor de administração.

hhh) A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.

iii) A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações antimalware instalados, e para distribuir notificações sobre eventos por e-mail.

jjj) A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.

kkk) A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.

lll) A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal.

mmm) A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.

nnn) A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.

ooo) A solução proposta deve permitir ao administrador personalizar relatórios.

ppp) A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.

qqq) A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.

rrr) A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.

sss) A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.

ttt)A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.

uuu) A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.

vvv) O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos.

www) 3.11.68. O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.

xxx) 3.11.69. A solução proposta deve permitir instalar o modulo de gerenciamento onpremisse nos seguintes sistemas operacionais:

i. 3.11.69.1. Windows;
ii. 3.11.69.2. Linux.

iii. A solução proposta deverá suportar os seguintes servidores de banco de dados:

1. Windows:

a. Microsoft SQL Server;

b. Microsoft Banco de dados SQL do Azure;

c. MySQL Standard e Enterprise;

d. MariaDB 3.1.5. PostgreSQL.

2. Linux:

a. MySQL;

b. MariaDB;

c. PostgreSQL.

iv. A solução proposta deverá suportar as seguintes plataformas virtuais:

1. Windows:

a. VMware vSphere 6.7 e 7.0;

b. Estação de trabalho VMware 16 Pro;

c. Servidor Microsoft Hyper-V 2012 de 64 bits;

d. Servidor Microsoft Hyper-V 2012 R2 de 64 bits;

e. Microsoft Servidor Hyper -V 2016 de 64 bits;

f. Servidor Microsoft Hyper-V 2019 de 64 bits;

g. Servidor Microsoft Hyper-V 2022 de 64 bits;

h. Citrix XenServer 7.1 LTSR;

i. Citrix XenServer 8.x 4.1.10. Oracle VM VirtualBox 6.x.

2. Linux:

a. VMware vSphere 6.7, 7.0 e 8.0;

b. VMware Desktop 16 Pro e 17 Pro;

c. Servidor Microsoft Hyper-V 2012 de 64 bits;

d. Servidor Microsoft Hyper-V 2012 R2 de 64 bits;

e. Microsoft Servidor Hyper -V 2016 de 64 bits;

f. Servidor Microsoft Hyper-V 2019 de 64 bits;

g. Servidor Microsoft Hyper-V 2022 de 64 bits;

h. Citrix XenServer 7.1 e 8.x;

i. Oracle VM VirtualBox 6.x e7.x.

b.

c. 3.12. Do módulo de proteção de endpoint:

yyy) 3.12.1. A solução proposta deverá proteger os sistemas operacionais abaixo:

i. Windows 8;
ii. Windows 7;
iii. Windows 8.1;
iv. Windows 10;
v. Windows 11.

zzz) Servidores:

i. Windows Small Business Server 2011;
ii. Windows MultiPoint Server 2011;
iii. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022.

aaaa) Servidores de terminal Microsoft:

i. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022.

bbbb) Sistemas operacionais Linux de 32 bits:

i. CentOS 6.7 e posterior;
ii. Debian GNU/Linux 11.0 e posterior;
iii. Debian GNU/Linux 12.0 e posterior;
iv. Red Hat Enterprise Linux 6.7 e posterior.

cccc) Sistemas operacionais Linux de 64 bits:

i. Amazon Linux 2;
ii. CentOS 6.7 e posterior;
iii. CentOS 7.2 e posterior;
iv. CentOS Stream 8;
v. CentOS Stream 9;
vi. Debian GNU/Linux 11.0 e posterior;
vii. Debian GNU/Linux 12.0 e posterior;
viii. Linux Mint 20.3 e superior;
ix. Linux Mint 21.1 e posterior;
x. OpenSUSE Leap 15.0 e posterior;

xi. Oracle Linux 7.3 e posterior;
xii. Oracle Linux 8.0 e posterior.
xiii. Oracle Linux 9.0 e posterior;
xiv. Red Hat Enterprise Linux 6.7 e posterior;
xv. Red Hat Enterprise Linux 7.2 e posterior;
xvi. Red Hat Enterprise Linux 8.0 e posterior;
xvii. Red Hat Enterprise Linux 9.0 e posterior;
xviii. Rocky Linux 8.5 e posterior;
xix. Rocky Linux 9.1;
xx. SUSE Linux Enterprise Server 12.5 ou posterior;
xxi. SUSE Linux Enterprise Server 15 ou posterior;
xxii. Ubuntu 20.04 LTS;
xxiii. Ubuntu 22.04 LTS.

dddd) Sistemas operacionais Arm de 64 bits:

i. CentOS Stream 9;
ii. SUSE Linux Enterprise Server 15;
iii. Ubuntu 22.04 LTS.

eeee) Sistemas operacionais MAC OS:

i. macOS 12 – 14.

ffff) Ferramentas de virtualização MAC OS:

i. Parallels Desktop 16 para Mac Business Edition;
ii. VMware Fusion 11.5 Profissional;
iii. VMware Fusion 12 Profissional.

gggg) A solução proposta deverá suportar as seguintes plataformas virtuais:

i. VMware Workstation 17.0.2 Pro;
ii. VMware ESXi 8.0 Update 2;
iii. Microsoft Hyper-V Server 2019;
iv. Citrix Virtual Apps e Desktop 7 2308
v. Citrix Provisioning 2308;
vi. Citrix Hypervisor 8.2 Update 1.

b. Requisitos de Suporte Técnico:

hhhh) Instalação e Configuração Inicial:

iiii) A contratada deverá realizar a instalação e configuração inicial do gerenciador e de 5 (cinco) computadores no local designado pela contratante.

jjjj) Abertura de Chamados e SLA:

kkkk) Os chamados deverão ser registrados via sistema Tomticket, com SLA máximo de até 4 (quatro) horas para resposta inicial.

llll) Base de Conhecimento:

mmmm) A contratada deverá disponibilizar uma base de conhecimento atualizada com informações sobre a solução, acessível ao contratante.

nnnn) Acesso Remoto:

oooo) Em caso de problemas, a contratada deverá prestar suporte técnico via acesso remoto para diagnóstico e solução.

pppp) Atendimento via WhatsApp:

qqqq) O suporte técnico deverá incluir atendimento por WhatsApp, garantindo agilidade na comunicação.

rrrr) Health Check Trimestral:

ssss) A contratada deverá realizar 1 (um) Health Check a cada 3 (três) meses para avaliar o desempenho e funcionamento da solução.

i. Consultoria Técnica:

tttt) A contratada deverá disponibilizar 2 (duas) horas de consultoria técnica para implementação ou ajustes específicos solicitados pela contratante.

i. Acesso Emergencial:

uuuu) O contratante tem direito à atendimento emergencial com o primeiro analista disponível em casos críticos que exijam solução imediata.

i. Implementação Remota:

vvvv) O contratado fará o auxílio da implementação do Endpoint da solução, criação de regras na solução e configuração para funcionamento.

9) CLÁUSULA NONA - DAS PENALIDADES E SANÇÕES ADMINISTRATIVAS:

9.1. Comete infração administrativa o fornecedor que infringir as disposições previstas no art. 155 da Lei nº 14.133/2021, quais sejam:

9.1.1. dar causa à inexecução parcial do Contrato;

9.1.2. dar causa à inexecução parcial do Contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

9.1.3. dar causa à inexecução total do Contrato;

9.1.4. deixar de entregar a documentação exigida para o certame;

9.1.5. não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

9.1.6. não celebrar o Contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

9.1.7. ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

9.1.8. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

9.1.9. fraudar a dispensa ou praticar ato fraudulento na execução do Contrato;

9.1.10. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

9.1.11. considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de negociação;

9.1.12. praticar atos ilícitos com vistas a frustrar os objetivos desta Dispensa;

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

9.2. O fornecedor que cometer qualquer das infrações discriminas nos subitens anteriores, em processo de aplicação de penalidade, estará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) Advertência pela falta do subitem 9.1.1, quando não se justificar a imposição de penalidade mais grave;

b) Multa de 15% (quinze) sobre o valor estimado dos itens prejudicados pela conduta do por quaisquer das infrações dos itens 9.1.1 a 9.1.12;

c) Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, nos casos dos subitens 9.1.2 a 9.1.7, quando não se justificar a imposição de penalidade mais grave;

d) Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes municipais, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 9.1.8 a 9.1.12, bem como nos demais casos que justifiquem a imposição da penalidade mais grave;

9.3. Na aplicação das sanções serão considerados:

9.3.1. a natureza e a gravidade da infração cometida;

9.3.2. as peculiaridades do caso concreto;

9.3.3. as circunstâncias agravantes ou atenuantes;

9.3.4. os danos que dela provierem para a Administração Pública;

9.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

9.4. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração a Promitente Fornecedora, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

9.5. A aplicação das sanções previstas neste Termo não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

9.6. Na aplicação da sanção prevista na alínea “b” do item 9.2 deste Termo, será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

9.7. Para aplicação das sanções previstas nas alíneas “c” e “d” do item 9.2 deste Termo será instaurado processo de responsabilização, a ser conduzido por comissão composta de 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou a Promitente Fornecedora para, no prazo de 15 (quinze) dias úteis, contado da data de intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

9.7.1. Quando o quadro funcional não dispor de servidores estatutários, a comissão a que se refere o item anterior será composta de 2 (dois) ou mais empregados públicos pertencentes aos seus quadros permanentes, preferencialmente com, no mínimo, 3 (três) anos de tempo de serviço no órgão ou entidade.

9.8. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

9.9. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao fornecedor/adjudicatário, observando-se os demais procedimentos previstos na Lei nº 14.133/2021.

10) CLÁUSULA DÉCIMA – DA EXTINÇÃO:

10.1. A ocorrência de quaisquer das hipóteses previstas no art. 137 da Lei n.º 14.133/2021 ensejará a extinção do presente Contrato.

10.2. A extinção poderá se processar pelas hipóteses definidas no art. 138, incisos I, II e III, e estará sob as consequências determinadas pelo art. 139, todos da Lei nº 14.133/2021.

10.3. Os casos de extinção contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à defesa prévia.

11) CLÁUSULA DÉCIMA PRIMEIRA – DA LGPD

11.1. Com exceção do que dispõe o art. 4º da Lei Federal nº 13709/18, que trata da proteção dos dados pessoais, a CONTRANTE se obriga a dar ciência prévia à CONTRATADA quando fizer uso dos dados privados, sempre zelando pelos princípios da minimização da coleta, necessidade de exposição específica da finalidade, sem prejuízo da mera correção dos dados;

11.2. Fica vedado o tratamento de dados pessoais sensíveis por parte da CONTRANTE com objetivo de obter vantagem econômica de qualquer espécie, com exceção daquelas hipóteses previstas no parágrafo 4º do art. 11 da Lei Federal nº 13709/18;

11.3. Multa de 20% (vinte por cento) sobre o valor total do CONTRATO, na hipótese de tratamento de dados pessoais sensíveis com o objetivo de obter vantagem

econômica, ou outra irregularidade havida no cumprimento do CONTRATO, por culpa da CONTRATADA;

11.4. A CONTRATANTE se compromete a zelar pelo tratamento dos dados pessoais dos titulares pessoas naturais vinculadas à CONTRATANTE, sem prejuízo de qualquer responsabilidade, admitindo-se o tratamento nas hipóteses de consentimento específico e destacado por termo de compromisso e ou nas hipóteses previstas nos incisos II a X do art. 7º da Lei Federal nº 13.709/18;

11.5. Multa de 10% (dez por cento) sobre o valor total do CONTRATO, na hipótese de descumprimento da obrigação de zelo no tratamento dos dados pessoais da pessoa natural vinculada à CONTRATANTE, ou em caso de tratamento de dados sem o consentimento específico e destacado por termo de compromisso, ou outra irregularidade havida no cumprimento do CONTRATO, por culpa da CONTRATADA.

12) CLÁUSULA DÉCIMA SEGUNDA – DAS CONDIÇÕES DE GARANTIA

12.1. O Ficará sob inteira responsabilidade da Contratada a garantia da qualidade do serviço prestado, sob pena das sanções legais cabíveis.

Caso a CONTRATANTE venha a sofrer prejuízos oriundos da má qualidade do serviço, a CONTRATADA deverá ressarcir todos os danos causados, bem como promover a reparação.

13) CLÁUSULA DÉCIMA TERCEIRA – DA FISCALIZAÇÃO DO CONTRATO/GESTÃO DE CONTRATO.

13.1. Nos termos do art. 117 da Lei n°14.133/2021, será designado representante para acompanhar e fiscalizar a execução do objeto da contratação, anotando em registro próprio todas as ocorrências relacionadas, e determinando o que for necessário à regularização de falhas ou defeitos.

14) CLÁUSULA DÉCIMA QUARTA – DA VIGÊNCIA DO CONTRATO

14.1. O contrato terá vigência de 12 (doze) meses, a partir da data de sua assinatura.

15) CLÁUSULA DÉCIMA QUINTA – DA VINCULAÇÃO DESTE AJUSTE AO ATO CONVOCATÓRIO E À PROPOSTA COMERCIAL APRESENTADA PELA CONTRATADA

15.1. Este contrato vincula-se, em todos os seus termos, ao ato convocatório referente ao Pregão Eletrônico nº 21/2025, assim como às propostas nela adjudicadas, que integram o presente compromisso de fornecimento independentemente de transcrição, devendo seus termos e condições ser considerados como partes integrantes do presente instrumento contratual.

16) CLÁUSULA DÉCIMA SEXTA – DA LEGISLAÇÃO APLICÁVEL

16.1. Aplica-se à execução deste termo contratual a 14.133/21 e suas alterações, bem como a Lei nº 5.383, de 18 de março de 1997.

17) CLÁUSULA DÉCIMA SÉTIMA – DAS ALTERAÇÕES

17.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

17.2. 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.

17.3. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do CONTRATANTE, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

17.4. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

18) CLÁUSULA DÉCIMA SEXTA - DOS CASOS OMISSOS

18.1 - Os casos omissos serão decididos pelo CONTRATANTE, segundo as disposições contidas na Lei nº 14.133, de 2021, e subsidiariamente, segundo as

disposições contidas na Lei nº 8.078, de 1990 - Código de Defesa do Consumidor - e normas e princípios gerais dos contratos.

19) CLÁUSULA DÉCIMA SÉTIMA – DA PUBLICAÇÃO

19.1. O extrato do presente contrato será publicado no Diário Oficial dos Municípios e na página da Prefeitura Municipal de Iconha (www.iconha.es.gov.br), em conformidade com art. 176, Parágrafo Único, I e II da Lei n°. 14.133/2021

20) CLÁUSULA DÉCIMA OITAVA – DO FORO

20.1. Fica eleito o foro da Comarca de Iconha, estado do Espírito Santo, para dirimir as questões originadas deste Contrato, com exclusão de qualquer outro, por mais privilegiado que seja.

E por estarem de acordo, depois de lido e achado conforme, foi o presente contrato lavrado em três cópias de igual teor e forma e assinado.

Iconha/ES, ___ de _____ de 2025.

MUNICÍPIO DE ICONHA
GEDSON PAULINO
Prefeito Municipal

(RAZÃO SOCIAL DA EMPRESA VENCEDORA)
CNPJ nº. _____
(Representante Legal)