TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
Av. André Araújo, S/N - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tjam.jus.br

EDITAL DE LICITAÇÃO - PE - SECOP/SEAC

EDITAL DO PREGÃO ELETRÔNICO N.º 039/2026-TJAM

Objeto: Contratação de empresa especializada para fornecimento de licença de uso de software de segurança de endpoint, tipo Endpoint Detection and Response (EDR), para 5.000 (cinco mil) ativos, incluindo suporte técnico especializado e um banco de 120 (cento e vinte) horas de consultoria, pelo período de 36 (trinta e seis) meses, para atender às necessidades de segurança cibernética do Tribunal de Justiça do Estado do Amazonas (TJAM).

SISTEMA DE REGISTRO DE PREÇOS? ( ) Sim (X) Não

Valor Total Estimado: R$ 5.763.000,00 (cinco milhões, setecentos e sessenta e três mil reais)

Data de divulgação do Edital: 25/05/2026
Início do cadastramento eletrônico de propostas.
Divulgação do Pregão, mediante aviso publicado no Diário de Justiça Eletrônico e nos sítios eletrônicos:
www.gov.br/compras e **www.tjam.jus.br**.

Data de abertura: 11/06/2026, às 10h00 (Horário de Brasília)
No sítio www.gov.br/compras UASG: 925866

Licitação Exclusiva ME/EPP? ( ) Sim (X) Não	**Há Itens Exclusivos ME/EPP e/ou Reserva de cota ME/EPP?** ( ) Sim (X) Não
Decreto 7.174/10? ( ) Sim (X) Não	**Margem de preferência?** ( ) Sim (X) Não
Vistoria? ( ) Obrigatória ( ) Facultativa (X) Não se aplica	**Amostra/ Catálogo?** ( ) Sim (X) Não
Pedidos de esclarecimentos Até 08/06/2026 às 15 h (Horário de Brasília) exclusivamente pelo e-mail colic@tjam.jus.br	**Impugnação** Até 08/06/2026 às 15 h (Horário de Brasília) exclusivamente pelo e-mail colic@tjam.jus.br
Informações Adicionais	
Exclusivamente pelo e-mail colic@tjam.jus.br	**Endereço:** Av. André Araújo, s/nº, Aleixo Manaus/AM-CEP: 69060-000

Todas as referências de tempo contidas neste Edital observarão o horário de Brasília-DF.

Todos os documentos a serem encaminhados eletronicamente deverão ser configurados, preferencialmente, nos seguintes formatos: Adobe Acrobat Reader (extensão .PDF), Word (extensão .DOC ou .DOCX), Excel (extensão .XLS ou .XLSX), podendo ainda ser processados por compactação nos formatos ZIP (extensão .ZIP) ou RAR (extensão .RAR).

Telefone em caso de dúvidas ou problemas técnicos relacionados à utilização do Portal de Compras do Governo Federal: 0800-978-9001.

Acompanhe as sessões públicas dos Pregões do Tribunal de Justiça do Amazonas pelo endereço **www.gov.br/compras/pt-br/acesso-a-informacao/consulta-detalhada** selecionando as opções Pregões > Em

andamento > Cód. UASG “925866”. O Edital está disponível para download nos endereços **www.gov.br/compras** e www.tjam.jus.br (Licitações>Editais, Avisos, Erratas e Docs>Licitação 2026>Pregões Eletrônicos).		

O **Tribunal de Justiça do Estado do Amazonas (TJAM)**, por meio de sua **Presidência**, informa a designação de Pregoeiro(a) pelo Ato n.º 8/2025 de 03 de janeiro de 2025, pela Portaria n.º 4.715/2023 de 07 de dezembro de 2023 e Portaria nº 2.099 de 13 de junho de 2024, e comunica aos interessados que realizará licitação na modalidade **PREGÃO ELETRÔNICO**, do tipo **MENOR PREÇO GLOBAL**, conforme **Processo Administrativo nº. 2026/000002456-00**, nos termos da Lei Federal n.º 14.133/2021, da Lei Complementar n.° 123/2006, do Decreto Estadual n.° 47.133/2023, da Resolução n.° 64/2023 TJAM, demais legislações aplicáveis e, ainda, de acordo com as condições estabelecidas neste edital e seus anexos.

CLÁUSULA PRIMEIRA
DO OBJETO

1.1. O objeto da presente licitação é a Contratação de empresa especializada para fornecimento de licença de uso de software de segurança de endpoint, tipo Endpoint Detection and Response (EDR), para 5.000 (cinco mil) ativos, incluindo suporte técnico especializado e um banco de 120 (cento e vinte) horas de consultoria, pelo período de 36 (trinta e seis) meses, para atender às necessidades de segurança cibernética do Tribunal de Justiça do Estado do Amazonas (TJAM), conforme condições, quantidades e exigências estabelecidas no Termo de Referência deste Edital.

1.2. Em caso de discrepância entre as especificações deste objeto descritas no sistema Compras.gov.br e as constantes deste Edital, prevalecerão as últimas.

CLÁUSULA SEGUNDA
DA DOTAÇÃO ORÇAMENTÁRIA

2.1. A despesa com a execução do objeto desta licitação é estimada em **R$ 5.763.000,00 (cinco milhões, setecentos e sessenta e três mil reais)**), conforme Planilha de Valores Estimados, e será custeada pelo orçamento do Poder Judiciário do Estado do Amazonas, Evento 200084, Unidade Orçamentária 04703, Programa de Trabalho 02126329026270001, Fonte de Recurso 175920100000 e Natureza da Despesa 0339040.

CLÁUSULA TERCEIRA
DAS COMUNICAÇÕES

3.1. A comunicação, durante o certame, entre Licitantes e a Coordenadoria de Licitação (COLIC), será realizada exclusivamente pelo sistema Comprasgov ou através do e-mail colic@tjam.jus.br.

3.2. Quando necessário, a COLIC publicará Comunicados atinentes ao andamento do certame no sistema Comprasgov e no site deste Poder (Licitação > Documentos > Editais, Avisos, Erratas e Docs > Licitações 2026 > Pregão Eletrônico).

CLÁUSULA QUARTA
DA IMPUGNAÇÃO E DO PEDIDO DE ESCLARECIMENTO

4.1. Até **03 (três) dias úteis** antes da data fixada para abertura da sessão pública, a encerrar em 08/06/2026, às 15h (horário de Brasília/DF), qualquer pessoa poderá **impugnar** o ato convocatório deste pregão mediante **petição**, que deverá obrigatoriamente conter a identificação da Impugnante (CPF/CNPJ), a ser enviada para o endereço eletrônico colic@tjam.jus.br.

4.2. O **pedido de esclarecimento**, mediante **petição**, que deverá obrigatoriamente conter a identificação do Interessado (CPF/CNPJ), deve ser enviado ao(à) Pregoeiro(a), em até **03 (três) dias úteis** anteriores à data

fixada para abertura da sessão pública, a encerrar em 08/06/2026, às 15h (horário de Brasília/DF), para o endereço eletrônico colic@tjam.jus.br.

4.3. A resposta à impugnação ou ao pedido de esclarecimento será divulgada em sítio eletrônico oficial no prazo de até **3 (três) dias úteis**, limitado ao último dia útil anterior à data da abertura do certame.

4.3.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo(a) Pregoeiro(a), nos autos do processo de licitação.

4.4. Acolhidos os argumentos da(s) petição(ões) das Cláusulas 4.1 e 4.2, será designada nova data para a realização do certame, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

4.5. As impugnações, esclarecimentos, bem como as devidas respostas serão disponibilizadas no sistema eletrônico Compras.gov.br (https://www.gov.br/compras/pt-br/acesso-a-informacao/consulta-detalhada/consulta-detalhada) e no site oficial do TJAM https://www.tjam.jus.br/index.php/documentos-licitacao/editais-avisos-erratas-e-docs.

CLÁUSULA QUINTA
DO CREDENCIAMENTO E DAS CONDIÇÕES DE PARTICIPAÇÃO

5.1. A sessão deste pregão será pública e realizada na data, horário e endereço eletrônico indicado.

5.2. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras), por meio de Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil.

5.3. Para ter acesso ao sistema eletrônico, os interessados em participar deste pregão deverão dispor de chave de identificação e senha pessoal, obtidas junto à Secretaria de Gestão do Ministério da Economia (SEGES), onde também deverão informar-se a respeito do seu funcionamento, regulamento e receber instruções detalhadas para sua correta utilização.

5.4. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

5.5. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

5.6. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

5.7. Não poderá disputar esta licitação:

5.7.1. Aquele que não atenda às condições deste Edital e seu(s) anexo(s);

5.7.2. Impedidos de contratar no âmbito da Administração Pública direta e indireta do Estado do Amazonas, nos termos do art. 156, III, § 4º, da Lei Federal n.º 14.133/2021;

5.7.3. Suspensos de participar de licitações e impedidos de contratar com o Tribunal de Justiça do Estado do Amazonas, nos termos do art. 87, III, da Lei n.° 8.666/1993, por meio de punições pretéritas e ainda vigentes;

5.7.4. Declarados inidôneos para licitar ou contratar com a Administração Pública, na forma do art. 87, IV, da Lei n.° 8.666/1993, por meio de punições pretéritas e ainda vigentes;

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

5.7.6. Estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa e judicialmente;

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

5.7.8. Agente público do órgão ou entidade licitante;

5.7.9. Quaisquer interessados que se enquadrem nas vedações previstas no art. 14º da Lei Federal n.º 14.133/2021;

5.7.10. Empresas sob a forma de consórcio, haja vista a baixa complexidade e o valor estimado da contratação;

5.7.11. Empresas sob a forma de cooperativas, consoante a jurisprudência do Tribunal de Contas da União (Súmula 281 – TCU);

5.7.12. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

5.7.13. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei Federal n.º 14.133/2021.

5.8. Não será permitida a subcontratação total ou parcial do objeto desta licitação, ficando sob a inteira responsabilidade da licitante contratada o cumprimento de todas as condições contratuais, atendendo aos requisitos técnicos e legais para esta finalidade.

CLÁUSULA SEXTA
DA VISTORIA TÉCNICA

6.1. Para participação nesta licitação **não será exigida** a realização de vistoria técnica no local de execução do objeto.

CLÁUSULA SÉTIMA
DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

7.1. A presente licitação seguirá as seguintes fases, em sequência: apresentação de propostas e lances, julgamento, habilitação, recursal e homologação.

7.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

7.3. Os licitantes poderão retirar ou substituir a proposta até a abertura da sessão pública.

7.4. Após a abertura da sessão, fica vedada a alteração da proposta, exceto para ajustes diligenciados pelo(a) Pregoeiro(a).

7.5. A apresentação da proposta implica a aceitação plena e total das condições deste Edital e seus anexos.

7.6. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

7.7. Os documentos que compõem a proposta e a habilitação da licitante melhor classificada somente serão disponibilizados, pelo sistema, para avaliação do(a) Pregoeiro(a) e para acesso público após o encerramento do envio de lances.

7.8. Os documentos complementares à proposta e à habilitação, quando necessários à confirmação daqueles exigidos no Edital e já apresentados, serão exigidos da licitante melhor classificada após o julgamento das propostas.

7.9. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da

inobservância de mensagens emitidas pela Administração ou de sua desconexão.

7.10. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

CLÁUSULA OITAVA
DAS DECLARAÇÕES

8.1. Todas as declarações exigidas no sistema Compras.gov.br, bem como as supervenientes e eventualmente exigidas durante o certame, serão aferidas para fins de habilitação.

8.1.1. O não envio das declarações poderá ocasionar a inabilitação, observados os prazos de que trata este instrumento convocatório.

8.2. A licitante deverá declarar:

8.2.1. Que está ciente e de acordo com as condições contidas no Edital e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

8.2.2. Que até a presente data, inexistem fatos impeditivos para sua habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores;

8.2.3. Que elaborou de maneira independente sua proposta de preço para participar desta licitação;

8.2.4. Que não emprega menores de dezoito anos em trabalho noturno, perigoso ou insalubre, nem menores de dezesseis anos em qualquer trabalho, salvo na condição de aprendiz, a partir dos quatorze anos;

8.2.5. Que, por ser enquadrado como microempresa ou empresa de pequeno porte, atende aos requisitos do art. 3º da Lei Complementar n.º 123/2006, para fazer jus aos benefícios previstos na legislação;

8.2.6. Que, conforme disposto no art. 93 da Lei nº 8.213/1991, está ciente do cumprimento da reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que, se aplicado ao número de funcionários da empresa, atende às regras de acessibilidade previstas na legislação;

8.2.7. Que cumpre a cota de aprendizagem nos termos estabelecidos no art. 429 da CLT;

8.2.8. Que não possui em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, nos termos do inciso III e IV do art.1º e no inciso III do Art. 5º da Constituição Federal.

8.3. O(A) Pregoeiro(a) poderá exigir declarações não previstas no Edital, justificando motivadamente a diligência.

8.3.1. O(A) Pregoeiro(a) poderá diligenciar o envio ou reenvio de declarações exigidas ou apresentadas no certame.

8.3.2. As declarações devem ser encaminhadas por meio da opção “enviar anexo” do sistema Compras.gov.br ou para o endereço eletrônico colic@tjam.jus.br.

8.4. A falsidade da declaração de que trata a Cláusula Oitava sujeitará a licitante às sanções previstas na Resolução n.° 64/2023 TJAM.

CLÁUSULA NONA
DO PREENCHIMENTO DA PROPOSTA

9.1. A Proposta de Preços deverá atender o Anexo III do Edital.

9.2. Todas as especificações do objeto contidas na proposta vinculam o licitante.

9.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

9.4. A proposta de preços deverá estar devidamente datada e assinada pelo Responsável Legal, devendo ainda conter as informações dispostas no Formulário Proposta de Preços (Anexo III deste Edital), tais como os seus

dados cadastrais, dados bancários, indicação de marcas, modelos, tipos e fabricantes dos produtos, se houver, preços unitários e totais.

9.5. Não é permitida a cotação de quantidade inferior àquela constante no Termo de Referência.

9.6. Os preços unitários e totais deverão estar em moeda nacional (R$), com apenas duas casas decimais após a vírgula, e em caso de divergência entre preços unitários e totais, prevalecerão os primeiros.

9.7. Poderão ser corrigidos automaticamente pelo(a) Pregoeiro(a) quaisquer erros aritméticos e o preço global da proposta, se necessário.

9.8. Não será aceita proposta com itens cujos valores estejam acima do estimado por este Poder.

9.8.1. Se houver necessidade de correção, não serão aceitas propostas contendo valores de itens superiores aos anteriormente apresentados pela licitante.

9.9. Não será admitida proposta que apresente valores simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado.

9.10. Não será considerada qualquer oferta de vantagem não prevista neste Edital.

9.11. Se a proposta não for aceitável, se a licitante deixar de enviá-la, se deixar de atender solicitação feita ou não atender às exigências deste Edital, o(a) Pregoeiro(a) examinará a proposta subsequente e, assim, sucessivamente, na ordem de classificação, até a apuração daquela que atenda aos requisitos.

9.12. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

9.13. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

9.14. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

9.15. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

9.16. O prazo de validade da proposta será de 60 (sessenta) dias, a contar da data de sua apresentação.

9.16.1. A data inicial de validade da proposta será renovada quando do envio da proposta adequada ao último lance ofertado após a negociação.

CLÁUSULA DÉCIMA
DAS AMOSTRAS, DOS FOLDERS, CATÁLOGOS, DOS PROSPECTOS OU MANUAIS

10.1. Para esta licitação **não** será exigida a apresentação de amostras, folders, catálogos, prospectos e/ou manuais.

CLÁUSULA DÉCIMA PRIMEIRA
DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

11.1. A abertura da sessão pública deste pregão, conduzida pelo(a) Pregoeiro(a), ocorrerá na data e na hora indicada no preâmbulo deste Edital, no sítio www.gov.br/compras.

11.2. Durante a sessão pública, a comunicação entre o(a) Pregoeiro(a) e as licitantes ocorrerá exclusivamente mediante troca de mensagens, em campo próprio do sistema eletrônico.

11.2.1. Na intercorrência de qualquer dificuldade técnica, a comunicação poderá ser realizada por meio do endereço eletrônico colic@tjam.jus.br, sendo posteriormente publicado no site do TJAM e informado em sessão.

11.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

11.4. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

11.5. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

11.6. Durante a sessão pública, as licitantes serão informadas, pelo sistema, em tempo real, do valor do menor lance registrado, vedada a identificação da licitante.

11.7. A licitante somente poderá oferecer valor inferior ao último lance por ela ofertado e registrado pelo sistema, observado o intervalo mínimo entre lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta.

11.8. O sistema não aceitará dois ou mais lances iguais e prevalecerá aquele que for recebido e registrado primeiro.

11.9. O procedimento seguirá de acordo com o modo de disputa “aberto”.

11.10. No modo de disputa “aberto”, os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

11.10.1. 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.

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

11.10.3. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

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

11.12. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

11.13. 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.

11.14. Durante a fase de lances, o(a) Pregoeiro(a) poderá excluir, justificadamente, lance cujo valor seja manifestamente inexequível.

11.15. Se ocorrer a desconexão do(a) Pregoeiro(a) no decorrer da etapa de lances, mas o sistema eletrônico permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

11.16. Quando a desconexão do sistema eletrônico para o(a) Pregoeiro(a) persistir por tempo superior a 10 (dez) minutos, a sessão pública será suspensa e reiniciada somente após decorridas 24 (vinte e quatro horas) da comunicação do fato pelo(a) Pregoeiro(a) aos participantes, no sítio eletrônico utilizado para divulgação.

11.17. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei Federal n.º 14.133/2021.

CLÁUSULA DÉCIMA SEGUNDA
DOS BENEFÍCIOS ÀS MICROEMPRESAS, EMPRESAS DE PEQUENO PORTE E EQUIPARADAS

12.1. São consideradas microempresas, empresas de pequeno porte e equiparadas, aquelas definidas nos incisos I e II do caput e § 4° do art. 3° da Lei Complementar Federal n.° 123/2006, em face do que determina o art. 1°, §1° da Lei Estadual n.° 6.269/2023.

12.1.1. Nos termos do art. 34 da Lei n.° 11.488/2007, equipara-se às microempresas e empresas de pequeno porte as sociedades cooperativas, desde que tenham auferido, no ano-calendário anterior, receita bruta até o limite definido no inciso II do caput do art. 3° da Lei Complementar n.° 123/2006, nela incluídos os atos cooperados e não-cooperados.

12.2. Nos termos do art. 4º, §1º, inciso I da Lei nº 14.133, de 2021, não serão aplicados os benefícios e as disposições constantes dos arts. 42 a 49 da Lei Complementar nº 123, de 14 de dezembro de 2006 no caso de contratação de licitação para aquisição de bens ou contratação de serviços em geral, ao item cujo valor estimado for superior à receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

CLÁUSULA DÉCIMA TERCEIRA
DA FASE DE JULGAMENTO

13.1. Encerrada a etapa anterior, o(a) Pregoeiro(a) verificará se o licitante classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei Federal n.º 14.133/2021, legislação correlata e no item 5.7 do Edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

13.1.1. SICAF;

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

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

13.1.4. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://portaldatransparencia.gov.br/sancoes/consulta?cadastro=1&ordenarPor=nomeSancionado&direcao=asc); e

13.1.5. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://portaldatransparencia.gov.br/sancoes/consulta?cadastro=2&ordenarPor=nomeSancionado&direcao=asc).

13.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n.° 8.429/1992.

13.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o(a) Pregoeiro(a) diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas (IN n° 3/2018, art. 29, caput).

13.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimentos similares, dentre outros. (IN n° 3/2018, art. 29, § 1°).

13.3.2. Identificada qualquer situação que possa caracterizar o impedimento indireto, o(a) Pregoeiro(a) convocará o licitante para manifestação prévia, no prazo de 02 (duas) horas.

13.3.3. Apresentada a manifestação prévia, ou transcorrido o decurso do prazo, serão os autos encaminhados para análise e manifestação da Assessoria Jurídico-Administrativa da Presidência, a qual se manifestará no prazo de 3 (três) dias.

13.3.4. A Assessoria Jurídico-Administrativa da Presidência, para instruir a sua análise, avaliando a necessidade de cada caso, poderá solicitar junto à Coordenadoria de Licitação a realização de novas manifestações e/ou diligências.

13.3.5. Na ausência de manifestação, ou em caso de não atendimento integral da diligência solicitada pela Assessoria Jurídico-Administrativa da Presidência, a empresa restará impedida de participar do certame, por falta de condição de participação.

13.4. Caso atendidas as condições de participação, será iniciado o procedimento de julgamento da proposta.

13.5. Caso o licitante classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o(a) Pregoeiro(a) verificará se faz jus ao benefício, em conformidade com a Cláusula Décima Segunda deste Edital.

13.6. Verificadas as condições de participação e de utilização do tratamento favorecido, o(a) Pregoeiro(a) examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos.

13.6.1. O(A) Pregoeiro(a) solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

13.6.2. Os documentos elencados no item 13.6.1 deverão ser encaminhados via sistema Compras.gov.br.

13.6.3. Na intercorrência de qualquer dificuldade técnica, o envio mencionado no subitem anterior poderá ser realizado por meio do endereço eletrônico colic@tjam.jus.br, sendo posteriormente publicado no site do TJAM e informado em sessão.

13.6.4. É facultado ao(à) Pregoeiro(a) prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante ou por meio de e-mail à Coordenadoria de Licitação (colic@tjam.jus.br), antes de findo o prazo.

13.7. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

13.7.1. A inexequibilidade, na hipótese de que trata o caput, só será considerada após diligência do agente de contratação ou da comissão de contratação, quando o substituir, que comprove:

a) que o custo do licitante ultrapassa o valor da proposta; e

b) inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

13.8. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

13.9. Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de Planilha de Custos e Formação de Preços elaborada pela Administração, o licitante classificado em primeiro lugar será convocado para apresentar Planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

13.10. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço.

13.10.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas.

13.10.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

CLÁUSULA DÉCIMA QUARTA
DA NEGOCIAÇÃO

14.1. Definido o resultado do julgamento, o(a) Pregoeiro(a) poderá negociar condições mais vantajosas com o primeiro colocado.

14.1.1. O prazo de negociação oferecido aos licitantes não será inferior a 5 (cinco) minutos.

14.2. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

14.3. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes, cujo resultado será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

14.4. O(A) Pregoeiro(a) solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao valor atualizado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

14.4.1. Os documentos elencados no item anterior deverão ser encaminhados na forma dos itens 13.6.1 a 13.6.4, adequando-se ao valor atualizado após a negociação realizada.

CLÁUSULA DÉCIMA QUINTA
DA FASE DE HABILITAÇÃO

15.1. Vencida a etapa anterior, promover-se-á a análise dos documentos para fins de habilitação.

15.2. A habilitação das licitantes será verificada por meio do Sistema de Cadastramento Unificado de Fornecedores (SICAF), bem como de outros sistemas públicos de consulta, e documentação complementar disposta nas Cláusulas seguintes.

15.2.1. No caso da documentação já cadastrada no SICAF estar em desconformidade com o previsto na legislação aplicável no momento da habilitação, ou haja a necessidade de solicitar documentos complementares aos já apresentados, o(a) Pregoeiro(a) deverá comunicar à licitante para que promova a regularização no prazo de 02 (duas) horas.

15.2.2. O referido prazo poderá ser dilatado motivadamente pelo(a) Pregoeiro(a) a depender das circunstâncias ou, havendo justo motivo, mediante solicitação formal de prorrogação por parte da licitante antes do fim do prazo concedido.

15.2.3. Os documentos elencados no item 15.2.1 deverão ser encaminhados via sistema Compras.gov.br.

15.2.4. Na intercorrência de qualquer dificuldade técnica, o envio mencionado no subitem anterior poderá ser realizado por meio do endereço eletrônico colic@tjam.jus.br, sendo posteriormente publicado no site do TJAM e informado em sessão.

15.3. Serão verificadas a Habilitação Jurídica, a Qualificação Econômico-Financeira, a Regularidade Fiscal (Federal, Estadual, Distrital e Municipal) e a Regularidade perante a Justiça do Trabalho.

15.3.1. A comprovação da Habilitação Jurídica será aferida mediante a apresentação de:

a) Cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

b) No caso de Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

c) No caso de Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

d) Nos casos de Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

e) No caso de Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.° 77/2020;

f) No caso de Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

g) Nos casos de Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

h) No caso de Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei n.° 5.764/1971;

i) No caso de Agricultor familiar: Declaração de Aptidão ao Pronaf – DAP ou DAP-P válida, ou, ainda, outros documentos definidos pelo órgão regulador;

j) No caso de Produtor Rural: matrícula no Cadastro Específico do INSS – CEI, que comprove a qualificação como produtor rural pessoa física;

15.3.1.1. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

15.3.2. A comprovação da Qualificação Econômico-Financeira, será aferida mediante a apresentação de:

a) certidão negativa de falência ou recuperação judicial, expedida pelo distribuidor da sede da pessoa jurídica do licitante, com exceção das sociedades cooperativas que, por força de lei, não estão sujeitas à falência;

b) balanço patrimonial dos 2 (dois) últimos exercícios sociais, apresentado na forma da lei, com o cumprimento das seguintes formalidades:

b.1) Indicação do número das páginas e números do livro onde estão inscritos o balanço patrimonial e a Demonstração do Resultado do Exercício (DRE) no Livro Diário, além do acompanhamento do respectivo Termo de Abertura e Termo de Encerramento do mesmo;

b.1.1) Os Termos de Abertura e de Encerramento não serão exigidos:

b.1.1.1) para microempresas, empresas de pequeno porte e equiparadas, conforme definidas nos incisos I e II do caput e § 4° do art. 3° da Lei Complementar Federal n.° 123/2006, em face do que determina o art. 1°, §1° da Lei Estadual n.° 6.269/2023;

b.1.1.2) para as empresas obrigadas a adotar a Escrituração Contábil Digital (ECD), via Sistema Público de Escrituração Digital (SPED), na forma do art. 3° da Instrução Normativa RFB n.° 2.003/2021;

b.2) Assinatura do contador e do titular ou representante legal da empresa no balanço patrimonial, DRE e no recibo de entrega da ECD;

b.3) Prova de registro na Junta Comercial ou Cartório (devidamente carimbado, com etiqueta, chancela da Junta Comercial ou código de registro) ou recibo de entrega do ECD;

b.4) Demonstração da escrituração Contábil/Fiscal/pessoal regular;

b.5) Comprovante de habilitação do profissional, bem como sua situação regular perante o seu Conselho Regional de Contabilidade à época da assinatura do registro na Junta Comercial/Cartório ou da data da entrega do ECD;

b.5.1) Nos casos em que ocorrer a substituição do profissional responsável pela elaboração do balanço patrimonial da empresa, a qualificação do profissional atualmente encarregado será sujeita a avaliação;

b.5.2) Na mesma hipótese do subitem anterior, o profissional atualmente encarregado validará o(s) balanço(s) apresentados, anexando declaração expressa a ser juntado no momento do envio da proposta ajustada.

15.3.3. A comprovação da Regularidade Fiscal (Federal, Estadual, Distrital e Municipal) e Regularidade perante a Justiça do Trabalho, será aferida mediante a apresentação de:

a) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda (CNPJ);

b) prova de inscrição no cadastro de contribuintes estadual e/ou municipal, relativo à sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) prova de regularidade para com a Fazenda Federal, Estadual e Municipal da sede do licitante ou outra prova equivalente, na forma da lei;

d) prova de regularidade relativa à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço (FGTS), demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei;

e) prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa.

15.3.4. As licitantes deverão encaminhar a seguinte documentação complementar para verificação da sua Qualificação Técnica:

15.3.4.1. Atestado(s) de Capacidade Técnica, emitido(s) por pessoa jurídica de direito público ou privado, que comprove(m) a execução satisfatória de serviços de implantação, configuração e operação de solução de segurança do tipo *Endpoint Protection*, em quantidade mínima de 50% para o Item 1, sendo admitido o somatório de atestados.

15.3.4.2. A licitante deverá apresentar obrigatoriamente, no momento da habilitação, carta de autorização emitida pelo fabricante da solução ofertada, que comprove a qualificação e credenciamento da empresa vencedora junto ao fabricante, citando nominalmente este processo licitatório.

15.3.4.3. No caso de pessoa jurídica de direito público, o(s) atestado(s) ou certidão(ões) deverá(ão) ser assinado(s) pelo responsável do setor competente do órgão, preferencialmente munidos de mecanismos de verificação ou autenticação.

15.3.4.4. No caso de pessoa jurídica de direito privado, o(s) atestado(s) ou certidão(ões) deverá(ão) conter dados suficientes para identificação civil do declarante, com referência ao cargo/função que ocupa na empresa e formas de contato, ou munidos de mecanismos de verificação ou autenticação.

15.3.4.5. Os documentos apresentados poderão ser objeto de diligências, a critério da Administração

15.4. O(A) Pregoeiro(a) poderá, no julgamento da habilitação, sanar erros ou falhas que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível aos licitantes, e lhes atribuirá validade e eficácia para fins de classificação, observado o disposto no art. 55, da Lei Estadual n.° 2.794/2003.

15.5. No que diz respeito à habilitação das microempresas, empresas de pequeno porte e as equiparadas, e caso se aplique, serão seguidas as diretrizes estabelecidas na Cláusula Décima Segunda.

15.6. Todos os documentos emitidos em língua estrangeira deverão ser entregues acompanhados da tradução para língua portuguesa, efetuada por tradutor juramentado, e também devidamente consularizados ou registrados no cartório de títulos e documentos.

15.7. Documentos de procedência estrangeira, mas emitidos em língua portuguesa, também deverão ser apresentados devidamente consularizados ou registrados em cartório de títulos e documentos.

15.8. A entidade que tiver unidade operacional ou de negócios, quer como filial, agência, sucursal ou assemelhada, e que optar por sistema de escrituração descentralizado, deve ter registros contábeis que permitam a identificação das transações de cada uma dessas unidades.

15.9. Se a licitante não atender às exigências de habilitação, se a licitante deixar de enviá-los ou deixar de atender diligência complementar solicitada em sessão, o(a) Pregoeiro(a) examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a seleção da proposta que atenda a este Edital.

15.10. Constatado o atendimento às exigências fixadas neste Edital, a licitante será declarada vencedora.

CLÁUSULA DÉCIMA SEXTA
DOS RECURSOS

16.1. Declarada a vencedora, o(a) Pregoeiro(a) abrirá prazo de 10 (dez) minutos, durante o qual qualquer licitante poderá, de forma imediata, em campo próprio do sistema, manifestar sua intenção de recorrer.

16.1.1. A ausência de manifestação imediata do licitante quanto à intenção de recorrer, nos termos do disposto na Cláusula 16.1, importará na decadência desse direito.

16.2. A licitante que manifestou intenção de recurso deverá registrar as razões do recurso, em campo próprio do sistema, no prazo de 03 (três) dias, ficando as demais licitantes, desde logo, intimadas a apresentar contrarrazões, também via sistema, em igual prazo, que começará a correr do término do prazo da recorrente.

16.3. O acolhimento do recurso implicará a invalidação apenas dos atos insuscetíveis de aproveitamento.

16.4. Não serão providos recursos de caráter protelatório, fundada em mera insatisfação da licitante, podendo ainda ser aplicado, supletiva e subsidiariamente, no que couberem, as regras previstas na Lei n.° 13.105/2015.

CLÁUSULA DÉCIMA SÉTIMA

DA ADJUDICAÇÃO E HOMOLOGAÇÃO

17.1. O objeto deste pregão será adjudicado e homologado pela Presidência do Tribunal de Justiça do Amazonas, inclusive quando houver recurso.

CLÁUSULA DÉCIMA OITAVA
DO CONTRATO E DA GARANTIA CONTRATUAL

18.1. Será firmado o contrato com a empresa vencedora, que terá suas cláusulas e condições reguladas pela Lei Federal n.º 14.133/2021, pela Lei Complementar n.° 123/2006, pelo Decreto Estadual n.° 47.133/2023, pela Resolução n.° 64/2023 TJAM, e no que couber pelas demais Cláusulas e condições constantes neste Edital e no Termo de Referência.

18.2. A Divisão de Contratos e Convênios deste Poder convocará a empresa licitante para a assinatura do Termo de Contrato.

18.3. Na hipótese da empresa vencedora não apresentar situação regular ou não comparecer para assinar o Termo de Contrato será convocado outro licitante para celebrar o Contrato, observada a ordem de classificação, e assim sucessivamente, sem prejuízo da aplicação das sanções cabíveis.

18.4. Para a execução do futuro contrato, decorrente desta licitação, **será exigida** prestação de garantia, nos termos da Cláusula DÉCIMA TERCEIRA da Minuta de Contrato (anexo V).

CLÁUSULA DÉCIMA NONA
DOS PROCEDIMENTOS PARA O REGISTRO DE PREÇOS

19.1. A presente licitação **não** será realizada mediante Sistema de Registro de Preços.

CLÁUSULA VIGÉSIMA
DA NOTA DE EMPENHO

20.1. O Tribunal de Justiça do Amazonas convocará a licitante vencedora para, no prazo máximo de 05 (cinco) dias úteis, retirar a Nota de Empenho ou a encaminhará via e-mail, devendo, nesse caso, ser acusado seu recebimento no mesmo prazo, sob pena de decair o direito do fornecimento **ou** da prestação do serviço sem prejuízo das sanções legais cabíveis.

20.2. O prazo da convocação poderá ser prorrogado uma vez, por igual período, quando solicitado pela licitante vencedora, desde que ocorra motivo justificado e aceito pelo Tribunal de Justiça do Amazonas.

20.3. A licitante vencedora fica obrigada a aceitar, nas mesmas condições das propostas, os acréscimos ou supressões que porventura se fizerem necessários em até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato que se fizerem nas obras, nos serviços ou nas compras, e, no caso de reforma de edifício ou de equipamento, o limite para os acréscimos será de 50% (cinquenta por cento), nos termos do art. 125, da Lei Federal n.° 14.133/2021.

CLÁUSULA VIGÉSIMA PRIMEIRA
DO PRAZO E DAS CONDIÇÕES DE FORNECIMENTO OU DA PRESTAÇÃO DOS SERVIÇOS

21.1. O objeto desta licitação deverá ser executado de acordo com as especificações e as condições, e nos prazos definidos no Termo de Referência, no Termo de Contrato e na proposta de preço.

21.2. As despesas com seguros, transporte, fretes, tributos, encargos trabalhistas e previdenciários e demais despesas envolvidas no fornecimento do objeto ou na prestação do serviço correrão por conta da empresa contratada.

21.3. Após o fornecimento do objeto ou a prestação do serviço pela empresa contratada, o Tribunal de Justiça do Amazonas verificará o cumprimento das exigências constantes no Termo de Referência, no Termo de Contrato e na proposta de preços. As verificações serão realizadas pela Secretaria de Tecnologia da Informação e Comunicação deste Poder.

21.4. No caso de constatada divergência entre o objeto entregue ou o serviço prestado com as especificações ou as condições definidas no Termo de Referência, no Termo de Contrato e/ou na Proposta de Preços, o licitante contratado deverá efetuar a troca e/ou a correção nos prazos estabelecidos no Termo de Referência e no Termo de Contrato, contados a partir da comunicação da recusa.

21.5. Caso a licitante contratada não entregue o objeto ou preste o serviço nas condições estabelecidas neste Edital, deverá a Secretaria de Tecnologia da Informação e Comunicação deste Poder comunicar, de forma oficial e imediata, **à Presidência do Tribunal de Justiça do Amazonas** para as providências cabíveis.

CLÁUSULA VIGÉSIMA SEGUNDA
DAS OBRIGAÇÕES DO CONTRATANTE E DA CONTRATADA

22.1. Caberá ao Tribunal de Justiça do Amazonas, sem prejuízo das demais obrigações e responsabilidades constantes neste Edital, no Termo de Referência e no Termo de Contrato:

22.1.1. Acompanhar e fiscalizar o contrato por 1 (um) ou mais fiscais do contrato, representantes da Administração especialmente designados conforme requisitos estabelecidos no art. 7.º da Lei Federal n.º 14.133/2021, ou pelos respectivos substitutos, permitida a contratação de terceiros para assisti-los e subsidiá-los com informações pertinentes a essa atribuição;

22.1.2. Proporcionar todas as condições necessárias, para que o credenciado contratado possa cumprir o estabelecido no contrato;

22.1.3. Prestar todas as informações e esclarecimentos necessários para a fiel execução contratual, que venham a ser solicitados pelo contratado;

22.1.4. Fornecer os meios necessários à execução, pelo contratado, dos serviços objeto do contrato;

22.1.5. Garantir o acesso e a permanência dos empregados do contratado nas dependências do contratante, quando necessário para a execução do objeto do contrato;

22.1.6. Efetuar os pagamentos pelos serviços prestados, dentro dos prazos previstos no contrato, no Edital de credenciamento e na legislação.

22.2. Caberá à empresa licitante contratada, sem prejuízo das demais obrigações e responsabilidades constantes neste Edital, no Termo de Referência e no Termo de Contrato:

22.2.1. Executar o objeto desta licitação de acordo com as especificações e/ou condições constantes neste Edital, no Termo de Referência e no Termo de Contrato;

22.2.2. Manter preposto para representá-lo durante a execução do contrato;

22.2.3. Responder, em relação aos seus empregados, por todas as despesas decorrentes da execução do objeto desta licitação, tais como: salários, seguros de acidentes, taxas, impostos e contribuições, indenizações, vales refeição, vales transporte e outras que porventura sejam estabelecidas em convenções ou acordos coletivos, bem como as criadas e exigidas pelo Poder Público;

22.2.4. Ser responsável pelos danos causados ao Tribunal de Justiça do Amazonas ou a terceiros, decorrentes de sua culpa ou dolo quando da execução do objeto desta licitação, não excluindo ou reduzindo essa responsabilidade em virtude da fiscalização ou do acompanhamento pela contratante;

22.2.5. Solicitar a repactuação do contrato sempre que houver variação do equilíbrio econômico-financeiro, oferecendo para tanto os elementos e justificativas que fundamentam o pedido;

22.2.6. Comunicar por escrito ao Tribunal de Justiça do Amazonas qualquer anormalidade na execução do objeto desta licitação;

22.2.7. Observar as normas legais de segurança a que está sujeita a execução do objeto desta licitação;

22.2.8. Manter, durante toda a execução do contrato, em compatibilidade com obrigações assumidas, todas as condições de habilitação e qualificação exigidas nesta licitação.

CLÁUSULA VIGÉSIMA TERCEIRA
DAS OBRIGAÇÕES SOCIAIS, COMERCIAIS E FISCAIS

23.1. À empresa licitante contratada caberá, ainda:

23.1.1. Assumir a responsabilidade por todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, vez que os seus empregados não manterão nenhum vínculo empregatício com o Tribunal de Justiça do Amazonas;

23.1.2. Assumir, também, a responsabilidade por todas as providências e as obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados durante a execução do objeto desta licitação, ainda que acontecidos nas dependências do Tribunal de Justiça do Amazonas;

23.1.3. Assumir todos os encargos de demanda trabalhista, cível ou penal, relacionados a esse processo licitatório e ao respectivo contrato;

23.1.4. Assumir, ainda, a responsabilidade pelos encargos fiscais e comerciais resultantes da adjudicação desta licitação.

CLÁUSULA VIGÉSIMA QUARTA
DO PAGAMENTO

24.1. O pagamento será efetuado pela Secretaria de Orçamento e Finanças do TJAM, de acordo com a legislação vigente, após recebimento da Nota Fiscal ou Fatura, conferida e atestada pelo setor requisitante, comprovando a prestação do serviço de maneira satisfatória.

24.2. Poderão ser solicitados para o pagamento: Nota Fiscal, de acordo com a legislação vigente, provas de regularidade perante o Fundo de Garantia por Tempo de Serviço (Certidão de Regularidade do FGTS), perante o Instituto Nacional do Seguro Social (Certidão Negativa de Débito do INSS), perante a Fazenda Federal (Certidão Conjunta Negativa de Débitos relativos aos TRIBUTOS FEDERAIS e à DÍVIDA ATIVA DA UNIÃO), perante a Fazenda Estadual (Certidão Negativa de DÉBITO DO ESTADO), perante a Fazenda Municipal (Certidão Negativa de DÉBITO MUNICIPAL), e perante a Justiça do Trabalho.

24.3. Constatada qualquer incorreção na Nota Fiscal, de acordo com a legislação vigente, bem como qualquer outra circunstância que desaconselhe o seu pagamento, o prazo para pagamento fluirá a partir da respectiva regularização.

24.4. O pagamento observará o disposto na Cláusula OITAVA da Minuta de Contrato (anexo V).

CLÁUSULA VIGÉSIMA QUINTA
DA EXTINÇÃO DO CONTRATO

25.1. A inexecução total ou parcial do contrato enseja a sua rescisão, com as consequências previstas neste instrumento e na legislação pertinente à matéria.

25.2. Constituem motivo para rescisão do contrato:

25.2.1. O não cumprimento de cláusulas, especificações, condições ou prazos previstos neste instrumento e seus anexos;

25.2.2. O cumprimento irregular de cláusulas, especificações, condições ou prazos previstos neste instrumento e seus anexos;

25.2.3. A lentidão do seu cumprimento que impossibilite a conclusão do fornecimento ou da prestação do serviço nos prazos estipulados;

25.2.4. O atraso injustificado no início do fornecimento ou da prestação do serviço;

25.2.5. A subcontratação total ou parcial do seu objeto, nos termos do item 5.8 deste Edital;

25.2.6. O desatendimento das determinações regulares da autoridade designada para acompanhar e fiscalizar a contratação, assim como as de seus superiores;

25.2.7. O cometimento reiterado de faltas no fornecimento do objeto;

25.2.8. A decretação de falência ou a instauração de insolvência civil;

25.2.9. A dissolução da sociedade ou o falecimento do contratado;

25.2.10. A alteração social ou a modificação da finalidade ou da estrutura da empresa, que prejudique o fornecimento do objeto;

25.2.11. Razões de interesse público, de alta relevância e amplo conhecimento, justificadas e determinadas pela autoridade competente e exaradas no processo administrativo a que se refere o contrato;

25.2.12. A supressão da contratação, por parte da Administração, acarretando modificação do valor inicial do contrato além dos limites estabelecidos na legislação vigente;

25.2.13. A ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da execução do contrato.

25.2.14. Descumprimento do disposto no inciso VI do art. 68 da Lei Federal n.° 14.133/21, sem prejuízo das sanções penais cabíveis;

25.2.15. Outras ocorrências previstas na legislação pertinente à matéria.

25.3. Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa.

25.4. A rescisão do contrato poderá ser:

25.4.1. Determinada por ato unilateral e escrito da Administração, nos casos previstos na legislação pertinente;

25.4.2. Amigável, por acordo entre as partes, reduzida a termo no processo da licitação, desde que haja conveniência para a Administração;

25.4.3. Judicial, nos termos da legislação.

25.4.1.1. A rescisão administrativa ou amigável deverá ser precedida de autorização escrita e fundamentada da autoridade competente.

25.4.1.2. Quando a rescisão ocorrer com base nos subitens 25.2.11 a 25.2.13 do item 25.2, sem que haja culpa do contratado, será este ressarcido dos prejuízos regularmente comprovados que houver sofrido, nos termos da lei.

25.5. A rescisão contratual observará a legislação pertinente e em especial a Lei Federal n.° 14.133/2021 e suas alterações.

25.6. A rescisão contratual relativa a execução do objeto desta licitação observará o disposto na Cláusula DÉCIMA SÉTIMA da Minuta de Contrato (anexo V).

CLÁUSULA VIGÉSIMA SEXTA
DA INEXECUÇÃO

26.1. Pelo descumprimento total ou parcial das obrigações assumidas e pela verificação de quaisquer situações previstas nos artigos 155 e 137, da Lei Federal n.º 14.133/2021, a Administração poderá, resguardados os procedimentos legais pertinentes, aplicar as sanções previstas na cláusula subsequente.

CLÁUSULA VIGÉSIMA SÉTIMA
DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

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

27.1.1. Deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo(a) Pregoeiro(a) durante o certame;

27.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

a) não enviar a proposta adequada ao último lance ofertado ou após a negociação;

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, quando for solicitado;

e) apresentar proposta ou amostra, quando for solicitado, em desacordo com as especificações do Edital;

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

a) recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

27.1.4. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

27.1.5. Fraudar a licitação;

27.1.6. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

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

b) induzir deliberadamente a erro no julgamento;

c) apresentar amostra, quando for solicitado, falsificada ou deteriorada;

27.1.7. Praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

27.1.8. Praticar ato lesivo previsto no art. 5º da Lei n.º 12.846/2013.

27.2. Com fulcro na Lei Federal n.º 14.133/2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

27.2.1. Advertência;

27.2.2. Multa;

27.2.3. Impedimento de licitar e contratar; e

27.2.4. Declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

27.3. Na instrução da aplicação das sanções administrativas devem ser observados os princípios do contraditório e da ampla defesa, considerando, ainda:

I - a natureza e a gravidade da infração cometida;

II - as peculiaridades do caso concreto;

III - os danos causados ao Tribunal;

IV - a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle;

V - as circunstâncias agravantes ou atenuantes;

VI - o custo e benefício da instrução do processo em relação à sanção a ser aplicada.

Parágrafo único. A pena-base deve ser fixada levando-se em consideração as circunstâncias listadas nos incisos I a IV do caput deste artigo; em seguida serão aplicadas as circunstâncias agravantes e atenuantes, respeitando-se os limites mínimo e máximo das penas previstas nos artigos 23 e 24 do Anexo VIII da Resolução n.° 64/2023 TJAM.

27.4. A aplicação das sanções previstas neste Edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

27.5. O regramento para a instauração e instrução dos processos administrativos sancionatórios e para a definição da dosimetria da aplicação da pena decorrentes da prática de condutas previstas no art. 155 da Lei Federal n.º 14.133/2021, encontra-se estabelecido no Anexo VIII da Resolução n.° 64/2023 TJAM.

27.6. As penalidades aplicadas serão obrigatoriamente divulgadas no Diário da Justiça Eletrônico, no site do Tribunal de Justiça do Amazonas e registradas no Sistema de Cadastramento Unificado de Fornecedores (SICAF).

CLÁUSULA VIGÉSIMA OITAVA
DAS DISPOSIÇÕES GERAIS

28.1. Será divulgada ata da sessão pública ou documento equivalente no sistema eletrônico e no site do Tribunal de Justiça do Amazonas.

28.2. A critério do Tribunal de Justiça do Amazonas, a presente licitação poderá ser:

28.2.1. Adiada, por conveniência do Tribunal de Justiça do Amazonas, desde que devidamente justificada;

28.2.2. Revogada, a juízo do Tribunal de Justiça do Amazonas, se considerada inoportuna ou inconveniente ao interesse público, decorrente de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta;

28.2.3. Anulada, de ofício ou mediante provocação de terceiros, sempre que presente ilegalidade insanável, mediante parecer escrito onde indicará expressamente os atos com vícios insanáveis, tornando sem efeito todos os subsequentes que deles dependam, e dará ensejo à apuração de responsabilidade de quem lhes tenha dado causa.

28.3. A anulação do procedimento licitatório induz a do contrato.

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

28.5. A participação nesta licitação implica na aceitação plena e irrevogável das normas constantes neste presente ato de convocação, independentemente de declaração expressa.

28.6. É vedada a manutenção, aditamento ou prorrogação de contrato de prestação de serviços com empresa que 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 membros ou juízes vinculados ao do Tribunal de Justiça do Amazonas.

28.7. É vedada, ainda a manutenção, aditamento ou prorrogação de contrato de prestação de serviços com empresa que tenha entre seus empregados colocados à disposição do Tribunal de Justiça do Amazonas para o exercício de funções de chefia, pessoas que incidam na vedação dos arts. 1º e 2º da Resolução nº 156/2012 CNJ, em atendimento ao disposto no art. 4º da Resolução supracitada.

28.8. Na hipótese de não constar prazo nos documentos exigidos para a participação nesta licitação, este Órgão aceitará como válidos os expedidos em até 90 (noventa) dias imediatamente anteriores à data de abertura da licitação, com exceção daqueles cuja validade seja indeterminada.

28.9. No caso de posteriores alterações das Normas Regulamentadoras (NRs) da Associação Brasileira de Normas Técnicas (ABNT) exigidas neste instrumento convocatório e seus anexos, serão consideradas para todos os efeitos cabíveis as NRs vigentes e atualizadas.

28.10. Quando houver indicação de marca, no Termo de Referência ou em qualquer dos anexos deste Edital, fica admitida a utilização de marcas similares com qualidade equivalente ou superior.

28.11. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.

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

28.13. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

28.14. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

28.15. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento, considerando-se o expediente normal deste Órgão, de segunda a sexta-feira, das 8 às 14 horas (horário de Manaus), salvo expressa disposição em contrário.

28.16. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

28.17. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

28.18. O(A) Pregoeiro(a) ou autoridade superior poderão promover diligências destinadas a elucidar ou complementar a instrução do processo, em qualquer fase da licitação, fixando prazos para atendimento.

28.19. O(A) Pregoeiro(a) poderá solicitar parecer de técnicos pertencentes ao quadro de pessoal do Tribunal de Justiça do Amazonas, ou ainda, de pessoas físicas ou jurídicas, estranhas a ele, com notórios conhecimentos na matéria em análise, para orientar suas decisões.

28.20. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico https://www.tjam.jus.br/index.php/documentos-licitacao/editais-avisos-erratas-e-docs

28.21. Os casos omissos serão dirimidos pela Presidência do Tribunal de Justiça do Amazonas.

CLÁUSULA VIGÉSIMA NONA
DOS ANEXOS

29.1. São partes integrantes deste Edital os seguintes anexos:

29.1.1. Declaração conjunta de ciência e concordância com as condições contidas no Edital, de cumprimento das condições de habilitação, de inexistência de impedimento legal para licitar ou contratar com a Administração Pública e de cumprimento ao disposto no inciso XXXIII do art. 7º da CF e no Inciso VI do art. 68 da Lei Federal n.º 14.133/2021 (Anexo I);

29.1.2. Declaração de elaboração independente de proposta (Anexo II);

29.1.3. Formulário proposta de preços (Anexo III);

29.1.4. Termo de Referência (Anexo IV);

29.1.4.1. Apêndice do Anexo V - Estudo Técnico Preliminar;

29.1.5. Minuta de Termo de Contrato (Anexo V).

CLÁUSULA TRIGÉSIMA
DO FORO

30.1. Fica eleito o foro da comarca de Manaus, capital do Estado do Amazonas, para dirimir quaisquer dúvidas decorrentes deste edital com exclusão de qualquer outro, por mais privilegiado que seja.

Manaus/AM, 07 de maio de 2026.

Desembargador JOMAR RICARDO SAUNDERS FERNANDES

Presidente do Tribunal de Justiça do Amazonas

PREGÃO ELETRÔNICO Nº. 039/2026 – TJAM

ANEXO I – Modelo de declaração conjunta de cumprimento das condições de habilitação e de inexistência de impedimento legal para licitar ou contratar com a Administração Pública.

(nome da empresa) _____, inscrito(a) no CNPJ n°. _____, por intermédio de seu representante legal o(a) Sr. (a)_____, portador(a) da Carteira de Identidade nº..... e do CPF nº ....., **DECLARA**:

1) que está ciente e concorda com as condições contidas no edital e seus anexos, e que cumpre plenamente os requisitos de habilitação definidos no edital;

2) que até a presente data inexistem fatos impeditivos para sua habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores;

3) que não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos, salvo menor, a partir de 14 (quatorze) anos, na condição de aprendiz, nos termos do inciso XXXIII do art. 7º da Constituição Federal.

Manaus, XX de XXXXX de 202X.

_____

carimbo (ou nome legível) e assinatura

PREGÃO ELETRÔNICO Nº. 039/2026 – TJAM

ANEXO II – Modelo de declaração de elaboração independente de proposta

[IDENTIFICAÇÃO COMPLETA DO REPRESENTANTE DO LICITANTE], como representante devidamente constituído de [IDENTIFICAÇÃO COMPLETA DO LICITANTE OU DO CONSÓRCIO] doravante denominado [Licitante/Consórcio], em atendimento ao disposto no edital do Pregão Eletrônico nº. XXX/202X, declara, sob as penas da lei, em especial o art. 299 do Código Penal Brasileiro, que:

a) a proposta anexa foi elaborada de maneira independente [pelo Licitante/Consórcio], e que o conteúdo da proposta anexa não foi, no todo ou em parte, direta ou indiretamente, informado a, discutido com ou recebido de qualquer outro participante potencial ou de fato do Pregão Eletrônico nº. XXX/202X, por qualquer meio ou por qualquer pessoa;

b) a intenção de apresentar a proposta anexa não foi informada a, discutido com ou recebido de qualquer outro participante potencial ou de fato do Pregão Eletrônico nº. XXX/202X, por qualquer meio ou por qualquer pessoa;

c) que não tentou, por qualquer meio ou qualquer pessoa, influir na decisão de qualquer outro participante potencial ou de fato do Pregão Eletrônico nº. XXX/202X quanto a participar ou não da referida licitação;

d) que o conteúdo da proposta anexa não será, no todo ou em parte, direta ou indiretamente, comunicado a ou discutido com qualquer outro participante potencial ou de fato do Pregão Eletrônico nº. XXX/202X antes da adjudicação do objeto da referida licitação;

e) que o conteúdo da proposta anexa não foi, no todo ou em parte, direta ou indiretamente, informado a, discutido com ou recebido de qualquer integrante do Tribunal de Justiça do Amazonas antes da abertura oficial das propostas; e

f) que está plenamente ciente do teor e da extensão desta declaração e que detém plenos poderes e informações para firmá-la.

Manaus, XX de XXXXX de 202X.

_____

carimbo (ou nome legível) e assinatura

PREGÃO ELETRÔNICO Nº. 039/2026 – TJAM

ANEXO III – Formulário de Proposta de Preços

RAZÃO SOCIAL:		
CNPJ:		**TELEFONE (S):**
E-MAIL:		
ENDEREÇO:		
BANCO:	**AGÊNCIA:**	**CONTA CORRENTE:**

GRUPO OU LOTE

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	VALOR TOTAL (R$)
VALOR TOTAL (R$)				

Valor total por extenso da Proposta de Preços.

Validade da proposta: 60 (sessenta) dias.

Observação: Estão inclusos nos preços supramencionados todos os custos diretos e indiretos, inclusive de embalagens, transportes ou fretes, e ainda os resultantes da incidência de quaisquer tributos, contribuições ou obrigações decorrentes da legislação trabalhista, fiscal e previdenciária a que estiver sujeito.

Declaro que possuo capacidade operacional e técnica para atendimento a todos os requisitos deste Edital e seus anexos.

Manaus, XX de XXXXXXXX de 202X.

_____

carimbo (ou nome legível) e assinatura

do Representante legal

PREGÃO ELETRÔNICO Nº. 039/2026 – TJAM
ANEXO IV – TERMO DE REFERÊNCIA

PREGÃO ELETRÔNICO Nº. 039/2026 – TJAM
ANEXO V – MINUTA DE TERMO DE CONTRATO

Documento assinado eletronicamente por **Jomar Ricardo Saunders Fernandes**, **Desembargador de Justiça**, em 08/05/2026, às 14:09, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjam.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2877103** e o código CRC **AC75407F**.

TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
Av. André Araújo, S/N - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tjam.jus.br

TERMO DE REFERÊNCIA

1. OBJETO DA CONTRATAÇÃO

1.1. Definição do Objeto: Contratação de empresa especializada para fornecimento de licença de uso de software de segurança de endpoint, tipo Endpoint Detection and Response (EDR), para 5.000 (cinco mil) ativos, incluindo suporte técnico especializado e um banco de 120 (cento e vinte) horas de consultoria, pelo período de 36 (trinta e seis) meses, para atender às necessidades de segurança cibernética do Tribunal de Justiça do Estado do Amazonas (TJAM). **CATSER: 27456**

1.2. Justificativa para a contratação:

1.2.1. A contratação é fundamental para garantir a continuidade e a evolução da segurança dos ativos de tecnologia da informação do TJAM, que incluem estações de trabalho, servidores e dispositivos móveis. A solução atual (Contrato nº 005/2023-FUNJEAM) está próxima do vencimento, e a sua substituição por uma solução moderna de EDR é imperativa para proteger a infraestrutura contra ameaças cibernéticas cada vez mais sofisticadas, como ransomware, ataques de dia-zero e ameaças persistentes avançadas (APTs), assegurando a integridade, a confidencialidade e a disponibilidade dos dados e dos serviços jurisdicionais e administrativos.

1.2.2. A indicação da solução Kaspersky Next EDR Optimum se justifica pela necessidade de padronização tecnológica, em conformidade com a Súmula TCU nº 270. O TJAM já utiliza a plataforma Kaspersky em seu ambiente de produção, e a manutenção da mesma plataforma tecnológica garante a compatibilidade com a infraestrutura existente, evita custos e complexidades de migração, e aproveita o conhecimento técnico já consolidado pela equipe da SETIC. A mudança de fabricante implicaria em um novo e complexo processo de implementação, treinamento e adaptação, gerando riscos operacionais e potenciais vulnerabilidades durante o período de transição.

1.2.3. O quantitativo de 5.000 licenças foi estimado com base no parque tecnológico atual de aproximadamente 4.000 ativos, acrescido de uma margem de 25% para crescimento vegetativo, novas aquisições e projetos de expansão do Tribunal ao longo dos 36 meses de vigência contratual. O banco de 120 horas de consultoria foi dimensionado para garantir suporte especializado em demandas pontuais e complexas, como análise de incidentes, otimização de políticas e configurações avançadas.

1.2.4. Os resultados esperados com a contratação são:

1.2.4.1. Garantir a proteção contínua dos ativos de Tecnologia da Informação do Tribunal de Justiça do Estado do Amazonas (TJAM) contra ameaças cibernéticas, tais como vírus, malwares, ransomwares e demais códigos maliciosos, por meio da utilização de solução de antivírus corporativa atualizada e reconhecida no mercado.

1.2.4.2. Assegurar a manutenção da confidencialidade, integridade e disponibilidade das informações institucionais, reduzindo os riscos de vazamento de dados, indisponibilidade de sistemas e comprometimento de informações sensíveis.

1.2.4.3. Manter a continuidade e a estabilidade dos serviços informatizados utilizados nas atividades administrativas e jurisdicionais do TJAM, evitando interrupções decorrentes de incidentes de segurança da informação.

1.2.4.4. Proporcionar gerenciamento centralizado da segurança dos endpoints, permitindo maior controle, visibilidade e padronização das políticas de segurança aplicadas a estações de trabalho, servidores e demais dispositivos conectados à rede institucional.

1.2.4.5. Reduzir o impacto operacional e o tempo de resposta a incidentes de segurança da informação, por meio de mecanismos avançados de detecção, resposta e mitigação de ameaças, aliados ao suporte técnico especializado da solução contratada.

1.2.4.6. Minimizar custos operacionais e riscos associados à ocorrência de incidentes de segurança, evitando gastos extraordinários com recuperação de sistemas, restauração de dados e mitigação de danos decorrentes de ataques cibernéticos.

1.2.4.7. Garantir a conformidade do ambiente tecnológico do TJAM com as melhores práticas de segurança da informação e com as diretrizes institucionais, contribuindo para o atendimento às normas internas, à legislação vigente e às recomendações dos órgãos de controle.

1.2.4.8. Preservar a padronização tecnológica já adotada pelo Tribunal, reduzindo a complexidade da administração do ambiente de TI e a necessidade de capacitação adicional da equipe técnica em soluções distintas.

1.3. Especificação técnica do Objeto e Quantitativo:

Item	Descrição	Unidade	Quantidade	Valor Estimado Unitário	Valor Estimado Anual
1	Fornecimento de Licença de uso do software antivírus KASPERSKY NEXT EDR OPTIMUM, com suporte técnico, por 36 meses.	Unidade	5000	R$	R$
2	Serviços Especializados para SUPORTE TÉCNICO E CONSULTORIA	Hora	120	R$	R$
TOTAL					**R$**

1.3.1 Do módulo de proteção de endpoint

1.3.1.1 A solução proposta deverá proteger os sistemas operacionais abaixo:

a) Windows 7;

b) Windows 8;

c) Windows 8.1;

d) Windows 10;

e) Windows 11.

1.3.1.2 Servidores:

a) Windows Small Business Server 2011;

b) Windows MultiPoint Server 2011;

c) Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022.

1.3.1.3 Servidores de terminal Microsoft:

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

1.3.1.4 Sistemas operacionais Linux de 32 bits:

a) CentOS 1.3.7 e posterior;

b) Debian GNU/Linux 11.0 e posterior;

c) Debian GNU/Linux 12.0 e posterior;

d) Red Hat Enterprise Linux 1.3.7 e posterior.

1.3.1.5 Sistemas operacionais Linux de 64 bits:

a) Amazon Linux 2;

b) CentOS 1.3.7 e mais tarde;

c) CentOS 7.2 e posterior;

d) CentOS Stream 8;

e) CentOS Stream 9;

f) Debian GNU/Linux 11.0 e posterior;

g) Debian GNU/Linux 12.0 e posterior;

h) Linux Mint 20.3 e superior;

i) Linux Mint 21.1 e posterior;

j) openSUSE Leap 15.0 e posterior;

k) Oracle Linux 7.3 e posterior;

l) Oracle Linux 8.0 e posterior;

m) Oracle Linux 9.0 e posterior;

n) Red Hat Enterprise Linux 1.3.7 e posterior;

o) Red Hat Enterprise Linux 7.2 e posterior;

p) Red Hat Enterprise Linux 8.0 e posterior;

q) Red Hat Enterprise Linux 9.0 e posterior;

r) Rocky Linux 8.5 e posterior;

s) Rocky Linux 9.1;

t) SUSE Linux Enterprise Server 12.5 ou posterior;

u) SUSE Linux Enterprise Server 15 ou posterior;

v) Ubuntu 20.04 LTS;

w) Ubuntu 22.04 LTS.

1.3.1.6 Sistemas operacionais Arm de 64 bits:

a) CentOS Stream 9;

b) SUSE Linux Enterprise Server 15;

c) Ubuntu 22.04 LTS.

1.3.1.7 Sistemas operacionais MAC OS:

a) macOS 12 – 14.

1.3.1.8 Ferramentas de virtualização MAC OS:

a) Parallels Desktop 16 para Mac Business Edition ou superior;

b) VMware Fusion 11.5 Profissional ou superior.

1.3.1.9 A solução proposta deverá suportar as seguintes plataformas virtuais:

a) VMware Workstation;

b) VMware ESXi;

c) Microsoft Hyper-V Server;

d) Citrix Virtual Apps e Desktop;

e) Citrix Provisioning.

1.3.2 Do módulo de gerenciamento avançado

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

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

a) Amazon Web Services;

b) Microsoft Azure;

c) Google Cloud.

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

a) HP (Microfoco) ArcSight;

b) IBM QRadar;

c) Splunk;

d) Kaspersky KUMA.

1.3.2.4 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.

1.3.2.5 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.

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

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

1.3.2.8 A o modulo da solução on-premisse deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

1.3.2.9 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.

1.3.2.10 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.

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

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

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

1.3.2.14 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:

a) Status do dispositivo;

b) Tag;

c) Diretório ativo;

d) Proprietários de dispositivos;

e) Hardware.

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

a) E-mail;

b) Registro de sistema;

c) SMS.

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

a) Atributos de rede;

b) Nome;

c) Domínio e/ou Sufixo de Domínio;

d) Endereço de IP;

e) Endereço IP para servidor de gerenciamento;

f) Localização no Active Directory;

g) Unidade organizacional;

h) Grupo;

i) Sistema operacional;

j) Número do pacote de serviço;

k) Arquitetura Virtual;

l) Registro de aplicativos;

m) Nome da Aplicação;

n) Versão do aplicativo;

o) Fabricante;

p) Tipo e versão;

q) Arquitetura.

1.3.2.17 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.

1.3.2.18 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.

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

a) Dispositivos Desktop/Servidores;

b) Dispositivos móveis;

c) Dispositivos de rede;

d) Dispositivos virtuais;

e) Componentes OEM;

f) Periféricos de computador;

g) Dispositivos IoT conectados;

h) Telefones VoIP;

i) Repositórios de rede.

1.3.2.20 A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:a) Nome da Aplicação;b) Caminho do aplicativo;c) Metadados do aplicativo;d) Aplicativo Certificado digital;e) Categorias de aplicativos predefinidas pelo fornecedor;f) SHA256 e MD5.

1.3.2.21 A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:a) Bluetooth;b) Dispositivos móveis;c) Modems externos;d) CD/DVD;e) Câmeras e scanners;f) MTPs;g) E a transferência de dados para dispositivos móveis.

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

1.3.2.23 A solução proposta 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.

1.3.2.24 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:a) Estruturas de domínios e grupos de trabalho do Windows;b) Estruturas de grupos do Active Directory;c) Conteúdo de um arquivo de texto criado manualmente pelo administrador.

1.3.2.25 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.

1.3.2.26 A solução proposta deve permitir realizar as seguintes ações para endpoints:a) Verificação manual;b) Verificação no acesso;c) Verificação por demanda;d) Verificação de arquivos compactados;e) Verificação de arquivos individuais, pastas e unidades;f) Bloqueio e verificação de scripts;g) Proteção contra alteração de registros;h) Proteção contra estouro de buffer;i) Verificação em segundo plano/inativa;j) Verificação de unidade removível na conexão com o sistema.

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

1.3.2.28 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.

1.3.2.29 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.

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

1.3.2.31 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.

1.3.2.32 A solução proposta deve suportar Windows Failover Cluster.

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

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

1.3.2.35 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.

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

1.3.2.37 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.

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

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

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

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

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

1.3.2.43 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 específico de prevenção de intrusão.

1.3.2.44 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.

1.3.2.45 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).

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

1.3.2.47 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.

1.3.2.48 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.

1.3.2.49 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.

1.3.2.50 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.

1.3.2.51 A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.

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

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

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

1.3.2.55 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.

1.3.2.56 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.

1.3.2.57 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.

1.3.2.58 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.

1.3.2.59 A solução proposta deve permitir ao administrador personalizar relatórios.

1.3.2.60 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.

1.3.2.61 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.

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

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

1.3.2.64 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.

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

1.3.2.66 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.

1.3.2.67 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.

1.3.2.68 A solução proposta deve suportar integração com solução APT.

1.3.2.69 A solução proposta deve suportar a integração com o serviço Managed Detection and Response.

1.3.2.70 A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:a) Windows;b) Linux.

1.3.2.71 A solução proposta deverá suportar os seguintes servidores de banco de dados:a) Windows: Microsoft SQL Server; Microsoft Banco de dados SQL do Azure; MySQL Standard e Enterprise; MariaDB; PostgreSQL.b) Linux: MySQL; MariaDB; PostgreSQL.

1.3.2.72 A solução proposta deverá suportar as seguintes plataformas virtuais:a) Windows: VMware vSphere 1.3.7 e 7.0; Estação de trabalho VMware 16 Pro; Servidor Microsoft Hyper-V 2012 de 64 bits; Servidor Microsoft Hyper-V 2012 R2 de 64 bits; Microsoft Servidor Hyper -V 2016 de 64 bits; Servidor Microsoft Hyper-V 2019 de 64 bits; Servidor Microsoft Hyper-V 2022 de 64 bits; Citrix XenServer 7.1 LTSR; Citrix XenServer 8.x; Oracle VM VirtualBox 6.x.b) Linux: VMware vSphere 1.3.7 e 7.0; VMware Desktop 16 Pro e 17 Pro; Servidor Microsoft Hyper-V 2012 de 64 bits; Servidor Microsoft Hyper-V 2012 R2 de 64 bits; Microsoft Servidor Hyper -V 2016 de 64 bits; Servidor Microsoft Hyper-V 2019 de 64 bits; Servidor Microsoft Hyper-V 2022 de 64 bits; Citrix XenServer 7.1 e 8.x; Oracle VM VirtualBox 6.x e7.x.

1.3.2.73 A solução proposta deve suportar criptografia em vários níveis:a) Criptografia completa do disco – incluindo disco do sistema;b) Criptografia de arquivos e pastas;c) Criptografia de mídia removível;d) Gerenciamento de criptografia BitLocker e MacOS Filevault2.

1.3.2.74 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:a) A criptografia de arquivos em unidades de computador locais;b) A criação de listas de criptografia de arquivos por extensão ou grupo de extensões;c) A criação de listas criptografadas de pastas em unidades de computador locais.

1.3.2.75 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:a) Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis;b) Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.

1.3.2.76 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:a) A criptografia de todos os arquivos armazenados em unidades removíveis;b) A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.

1.3.2.77 A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia.

1.3.2.78 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis.

1.3.2.79 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado.

1.3.2.80 A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.

1.3.2.81 A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais.

1.3.2.82 A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia.

1.3.2.83 A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados.

1.3.2.84 A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema.

1.3.2.85 A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado.

1.3.2.86 A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.

1.3.2.87 A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados.

1.3.2.88 A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos.

1.3.2.89 A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação.

1.3.2.90 O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados independentemente da localização e/ou usuário.

1.3.2.91 A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.

1.3.2.92 A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.

1.3.2.93 A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:a) Uso do Trusted Platform Module e configurações de senha;b) Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível;c) Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets).

1.3.2.94 A solução proposta deve suportar criptografia em Microsoft Surface Tablets.

1.3.2.95 A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:a) Instalação remota de software de terceiros;b) Relatórios sobre software e hardware existentes;c) Monitoramento para instalação de software não autorizado;d) Remoção de software não autorizado.

1.3.2.96 A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.

1.3.2.97 A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.

1.3.2.98 A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.

1.3.2.99 A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais.

1.3.2.100 A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.

1.3.2.101 A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.

1.3.2.102 O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.

1.3.2.103 A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança.

1.3.2.104 A solução proposta deve permitir ao administrador aprovar atualizações.

1.3.2.105 A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.

1.3.2.106 A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.

1.3.2.107 A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.

1.3.2.108 A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.

1.3.2.109 A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.

1.3.2.110 A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências).

1.3.2.111 A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.

1.3.2.112 A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.

1.3.2.113 A solução proposta deve incluir campos dedicados que contenham informações sobre ‘Exploração encontrada para a vulnerabilidade’.

1.3.2.114 A solução proposta deve incluir campos dedicados que contenham informações sobre “Ameaça encontrada para a vulnerabilidade”.

1.3.2.115 A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.

1.3.2.116 A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.

1.3.2.117 A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.

1.3.2.118 A solução proposta deve apoiar a implantação do sistema operacional.

1.3.2.119 A solução proposta deve suportar Wake-on LAN e UEFI.

1.3.2.120 A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server.

1.3.2.121 A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.

1.3.2.122 A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador.

1.3.2.123 A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.

1.3.2.124 A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.

1.3.2.125 A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.

1.3.2.126 A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota.

1.3.2.127 A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.

1.3.2.128 A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros.

1.3.2.129 A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:a) Inicie a instalação ao reiniciar ou desligar o computador;b) Instale o gerador necessário todos os pré-requisitos do sistema;c) Permitir a instalação de novas versões de aplicativos durante as atualizações;d) Baixe atualizações para o dispositivo sem instalá-las.

1.3.2.130 A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas.

1.3.2.131 A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.

1.3.2.132 O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:a) CEF;b) LEEF.

1.3.2.133 A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.

1.3.2.134 O relatório da solução proposta deve conter informações CVE.

1.3.2.135 A solução proposta deve suportar instalação de aplicações e software de terceiros.

1.3.3 Do módulo de gerenciamento simplificado

1.3.3.1 A solução proposta deve suportar arquitetura cloud.

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

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

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

1.3.3.5 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.

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

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

1.3.3.8 A solução proposta deve incluir informações do endpoint:a) IP público de internet;b) IP interno do dispositivo;c) Versão do agente de proteção;d) Ultima comunicação com a console, contendo data e hora;e) Informações do sistema operacional.

1.3.3.9 A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365.

1.3.3.10 A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365.

1.3.3.11 A solução proposta deve incluir treinamento em segurança cibernética.

1.3.4 Requisitos gerais

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

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

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

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

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

1.3.4.6 A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:a) Proteção contra ameaças sem arquivos (Fileless);b) Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque.

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

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

1.3.4.9 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.

1.3.4.10 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.

1.3.4.11 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.

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

1.3.4.13 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.

1.3.4.14 A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:a) Controles de aplicativos;b) Controle web e dispositivos;c) HIPS e Firewall;d) Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;e) Gerenciamento de criptografia de arquivos e discos;f) Controle adaptativo para detecção de anomalias.

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

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

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

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

1.3.4.19 A solução proposta deve incluir um módulo capaz, no mínimo, de:a) Bloqueio de aplicativos com base em sua categorização;b) Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos;c) A adição de sub-redes e a modificação de permissões de atividade.

1.3.4.20 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.

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

1.3.4.22 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.

1.3.4.23 A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:a) Modo silencioso;b) Discos rígidos e dispositivos removíveis;c) De todos as contas de usuários do dispositivo.

1.3.4.24 A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:a) Exclusão imediata de dados;b) Exclusão de dados adiada.

1.3.4.25 A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:a) Excluir usando os recursos do sistema operacional - os arquivos são excluídos;b) Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.

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

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

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

1.3.4.29 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.

1.3.4.30 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.

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

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

1.3.4.33 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.

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

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

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

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

1.3.4.38 A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.

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

1.3.4.40 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.

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

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

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

1.3.4.44 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.

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

1.3.4.46 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.

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

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

1.3.4.49 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.

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

1.3.4.51 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.

1.3.4.52 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.

1.3.4.53 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.

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

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

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

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

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

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

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

1.3.4.61 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.

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

1.3.4.63 A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:a) Filtro de anexos;b) Verificação de mensagens de email ao receber, ler e enviar.

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

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

1.3.4.66 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.).

1.3.4.67 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.

1.3.4.68 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.

1.3.4.69 A solução proposta deve incluir suporte ao protocolo IPv6.

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

1.3.4.71 A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:a) Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo;b) Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.

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

1.3.4.73 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.

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

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

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

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

1.3.4.78 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.

1.3.4.79 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.

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

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

1.3.4.82 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.

1.3.4.83 A solução proposta deve suportar endereços IPv6.

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

1.3.4.85 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.

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

1.3.4.87 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.

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

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

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

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

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

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

1.3.4.94 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.

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

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

1.3.4.97 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.

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

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

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

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

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

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

1.3.4.104 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.

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

1.3.4.106 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.

1.3.4.107 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.

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

1.3.4.109 A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:a) Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível;b) Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.

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

1.3.4.111 A solução proposta deve gerar relatoiros de vulnerabilidades encontradas nos dispositivos com sensor de end point instalado.

1.3.5 Do modulo de gerenciamento de dispositivos móveis

1.3.5.1 O modulo deve ser integrado a console de gerenciamento.

1.3.5.2 A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:a) Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition).

1.3.5.3 A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:a) iOS 10–17 ou iPadOS 13–17.

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

1.3.5.5 A solução proposta deve suportar dispositivos iOS supervisionados.

1.3.5.6 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.

1.3.5.7 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.

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

1.3.5.9 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).

1.3.5.10 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.

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

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

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

1.3.5.14 A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:a) Dados em contêineres;b) Contas de e-mail corporativo;c) Configurações para conexão à rede Wi-Fi corporativa e VPN;d) Nome do ponto de acesso (APN);e) Perfil do Android for Work;f) Recipiente KNOX;g) Chave do gerenciador de licença KNOX.

1.3.5.15 A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:a) Todos os perfis de configuração instalados;b) Todos os perfis de provisionamento;c) O perfil iOS MDM;d) Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas.

1.3.5.16 A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo.

1.3.5.17 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:a) Critérios de verificação do dispositivo;b) 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.

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

1.3.5.19 A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:a) Cartões de memória e outras unidades removíveis;b) Câmera do dispositivo;c) Conexões Wi-Fi;d) Conexões Bluetooth;e) Porta de conexão infravermelha;f) Ativação do ponto de acesso Wi-Fi;g) Conexão de área de trabalho remota;h) Sincronização de área de trabalho;i) Definir configurações da caixa de correio do Exchange;j) Configurar caixa de e-mail em dispositivos iOS MDM;k) Configure contêineres Samsung KNOX;l) Definir as configurações do perfil do Android for Work;m) Configurar e-mail/calendário/contatos;n) Defina as configurações de restrição de conteúdo de mídia;o) Definir configurações de proxy no dispositivo móvel;p) Configurar certificados e SCEP.

1.3.5.20 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.a) Portal de inscrição móvel KNOX;b) Pacotes de instalação pré-configurados independentes.

1.3.5.21 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.

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

1.3.5.23 A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:a) VMware AirWatch 9.3 ou posterior;b) MobileIron 10.0 ou posterior;c) IBM MaaS360 10.68 ou posterior;d) Microsoft Intune 1908 ou posterior;e) SOTI MobiControl 14.1.4 (1693) ou posterior.

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

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

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

1.3.5.27 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.

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

1.3.5.29 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.

1.3.5.30 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.

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

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

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

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

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

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

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

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

1.3.6 Do módulo de EDR

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

1.3.6.2 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.

1.3.6.3 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.

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

1.3.6.5 Deve apresentar informações detalhadas contendo:a) Usuário que executou a ação;b) Informações acesso privilegiado.

1.3.6.6 A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.

1.3.6.7 A solução proposta deve suportar integração com serviço de reputação em nuvem.

1.3.6.8 A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado. (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações, etc.)

1.3.6.9 O agente EDR deve ter integração com o aplicativo de proteção de endpoint(agente único).

1.3.6.10 Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas.

1.3.6.11 A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.

1.3.6.12 A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção.

1.3.6.13 A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.

1.3.6.14 A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.

1.3.6.15 A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.

1.3.6.16 A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.

1.3.6.17 A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas.

1.3.6.18 A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC.

1.3.6.19 A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.

1.3.6.20 A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:a) Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque);b) Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional;c) Informações gerais sobre a detecção, incluindo modo de detecção;d) Alterações no registro associadas à detecção;e) Histórico da presença de arquivos no dispositivo;f) Ações de resposta executadas pela aplicação.

1.3.6.21 O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc.

1.3.6.22 A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:a) Processo;b) Conexões de rede;c) Alterações no registro;d) Detalhes do download de objeto.

1.3.6.23 A solução proposta deve fornecer orientação de resposta (resposta guiada).

1.3.6.24 A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente.

1.3.6.25 A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:a) Impedir a execução de objetos;b) Isolamento de host;c) Excluir objeto do host ou grupo de hosts;d) Encerrar um processo no dispositivo;e) Colocar um objeto em quarentena;f) Execute a verificação do sistema;g) Execução remota de programa/processo/comando;h) Iniciar a varredura IoC para um grupo de hosts.

1.3.7 Requisitos para documentação da solução.

1.3.7.1 A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:a) Ajuda on-line para administradores;b) Ajuda on-line para melhores práticas de implementação;c) Ajuda on-line para proteção de servidores de administração.

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

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

1.3.8 SERVIÇOS DE CONSULTORIA E SUPORTE ESPECIALIZADO

1.3.8.1. Serviços de Suporte Técnico Especializado e Consultoria para Plataforma Kaspersky, que deverão ser prestados através de Banco de Horas (120h):

1.3.8.1.1. A CONTRATADA prestará serviços de consultoria e suporte técnico especializado nas soluções Kaspersky implantadas na CONTRATANTE, com foco em proteção de endpoints e funcionalidades EDR.

1.3.8.1.2. Os serviços serão realizados por meio de um banco de 120(cento e vinte) horas técnicas, disponibilizadas ao longo da vigência contratual, mediante solicitação da CONTRATANTE.

1.3.8.2. Das condições de execução dos serviços:

1.3.8.2.1. As horas poderão ser utilizadas sob demanda, mediante solicitação formal da CONTRATANTE, via chamado telefônico ou e-mail, entre 9h e 18h, de segunda a sexta-feira (horário de Brasília);

1.3.8.2.2. Os serviços poderão ser executados remotamente;

1.3.8.2.3. O suporte incluirá:

1.3.8.2.3.1. Esclarecimento de dúvidas de utilização, administração e operação das soluções Kaspersky fornecidas;

1.3.8.2.3.2. Orientação sobre atualizações, correções e melhorias;

1.3.8.2.3.3. Envio de procedimentos e boas práticas para operação segura e eficiente da solução;

1.3.8.2.3.4. Apoio em incidentes e contenção de ameaças;

1.3.8.2.3.5. Auditoria, revisão e análise de logs.

1.3.8.3. Da abrangência dos serviços de consultoria:

1.3.8.3.1. Os serviços contemplam, entre outros:

1.3.8.3.1.1. Análise, planejamento e implantação de projetos relacionados a soluções antivírus, EDR e proteção em nuvem Kaspersky;

1.3.8.3.1.2. Auxílio na gestão de políticas de segurança, incluindo prevenção e combate a ameaças como vírus, spywares, ransomwares e rootkits;

1.3.8.3.1.3. Avaliação de vulnerabilidades e recomendações de mitigação;

1.3.8.3.1.4. Instalação e configuração de atualizações de versão e patches;

1.3.8.3.1.5. Parametrização de filtros, regras e mecanismos de bloqueio para ameaças sem vacina;

1.3.8.3.1.6. Apoio na análise de logs e investigação de eventos de segurança.

1.3.8.4. Das condições operacionais e SLA:

1.3.8.4.1. O suporte será prestado por equipe com certificação oficial Kaspersky;

1.3.8.4.2. O atendimento ocorrerá em regime 8x5 com tempos de resposta conforme prioridade: a) Conforme tabela de SLA no item 1.3.8.6.

1.3.8.5. Da gestão e controle do banco de horas:

1.3.8.5.1. A CONTRATADA enviará até o dia 10 de cada mês o extrato das horas utilizadas no mês anterior;

1.3.8.5.2. A CONTRATANTE terá até 5 (cinco) dias úteis para validar ou contestar os relatórios enviados;

1.3.8.5.3. A CONTRATADA poderá emitir Nota Fiscal somente após o aceite das horas executadas.

1.3.8.5.4. O pagamento das horas será efetuado no prazo máximo de até 30 (trinta) dias, podendo ser de forma integral ou parcelada, através de conta corrente da CONTRATADA, no banco e conta corrente por ela indicados pela contratada.

1.3.8.6. Disposições finais

1.3.8.6.1. Este serviço não substitui a implantação inicial das soluções já contempladas nos documentos técnicos de EDR Optimum;

1.3.8.6.2. O banco de horas é válido durante a vigência contratual e pode ser utilizado conforme necessidade da CONTRATANTE.

DUVIDA	**SOLICITAÇÃO DE SERVIÇOS**	**INCIDENTE**			
PADRÃO	**PADRÃO**	**CRÍTICO**	**ALTO**	**MÉDIO**	**BAIXO**
Primeiro atendimento em até: 08 horas	Primeiro atendimento em até: 04 horas	Primeiro atendimento em até: 01 hora	Primeiro atendimento em até: 04 horas	Primeiro atendimento em até: 24 horas	Incidentes que criam restrições à operação da Solução.
Tempo para resolução em até: 72 horas	Tempo para resolução em até: 48 horas	Tempo para solução ou contorno em até: 04 horas	Tempo para solução ou contorno em até: 08 horas	Primeiro atendimento em até: 24 horas	Incidentes que criam restrições à operação da Solução.
Solicitações de dúvida sobre a plataforma ou sobre os serviços contratados.	Solicitações de novos serviços relacionado s ao produto contratado, como exemplo: Novas configurações, novos relatórios, novas parametrizações, entre outros.	Incidente crítico que paralise totalmente os serviços do ambiente de produção com impacto direto no negócio.	Incidente grave que prejudique a operação da solução ou limite severamente suas funcionalidades com a paralisação parcial do serviço.	Incidentes que criam restrições à operação da Solução.	Incidentes que criam restrições à operação da Solução.

1.4. Caracterização do Objeto:

1.4.1. O objeto do presente Termo de Referência enquadra-se no conceito de serviços comuns, nos termos do inciso XIII, Art. 6º, da Lei nº 14.133/2021.

1.5. Fundamentação Legal:

1.5.1. A contratação deverá obedecer, no que couber, ao disposto na legislação a seguir:

a) Lei nº 14.133, de 1º de abril de 2021;

b) Resolução n.º 64/2023, de 5 de dezembro de 2023;

c) Gui Prático de Critérios de Sustentabilidade - TJAM / 2022.

1.5.2. Legislações aplicáveis ao objeto a ser contratado, no que couber:

a) Resolução CNJ nº 468/2022 (Diretrizes para contratações de TIC);

b) Resolução CNJ nº 396/2021 (Estratégia Nacional de Segurança Cibernética do Poder Judiciário);

c) Decreto nº 9.637/2018 (Política Nacional de Segurança da Informação);

1.6. Indicação de necessidade de apresentação de amostras, catálogos, manuais, folders ou prospectos:

1.6.1. Para este certame, não será exigida apresentação de amostras, catálogos, manuais, folders ou prospectos.

1.7. Valor estimado da contratação:

1.7.1. A estimativa de valor da contratação será discriminada no Mapa de Preços a ser elaborado pela Divisão de Compras e Operações.

1.8. Adequação orçamentária:

1.8.1. A contratação pretendida está prevista no Plano de Contratação Anual 2026, sob o Código **SETIC-2026-72.**

2. CONDIÇÕES GERAIS DA CONTRATAÇÃO

2.1. O objeto deste Termo de Referência caracteriza-se como situação prevista na modalidade Pregão, sob a forma Eletrônica, nos termos do artigo 28, inciso I da, Lei nº 14.133/2021.

2.2. A presente contratação adotará como regime de execução a Empreitada por Preço unitário.

2.3. O procedimento para a contratação pretendida neste instrumento não será regido pelo Sistema de Registro de Preços, conforme apontado na escolha da solução do Estudo Técnico Preliminar.

2.4. O critério de julgamento será o de **MENOR PREÇO.**

2.5. O critério de adjudicação da contratação será GLOBAL, levando em consideração que o objeto configura um sistema único e integrado, sendo inviável ter o domínio principal sendo atendido por uma empresa de acessibilidade e os subdomínios por outra, o que geraria inconsistência de experiência para o usuário e aumentaria os custos e a complexidade de gestão do contrato

2.6. Participação de consórcios de empresas:

2.6.1. A participação de consórcios no certame que se originará do presente Termo de Referência não será permitida, em razão da complexidade e o vulto do objeto não limitarem a participação de fornecedores aptos a executar o objeto. Os potenciais fornecedores, em sua maioria, dispõem de condições de participar isoladamente do certame e prestar a integralidade do objeto, não sendo o caso de permitir a junção de esforços de 2 (duas) ou mais empresas para a execução da contratação pretendida. Nesse caso, a possibilidade de participação de consórcios poderia limitar a competitividade do certame, uma vez que se admitiria que empresas se associassem e não disputassem individualmente o objeto da licitação.

2.7. Não será permitida a subcontratação do objeto deste Termo de Referência.

2.8. Tratamento diferenciado para Microempresas, Empresas de Pequeno Porte ou Cooperativas:

2.8.1. Aplicam-se a este certame, no que couber, as disposições constantes dos arts. 42 a 49 da Lei Complementar nº 123, de 14 de dezembro de 2006.

3. REQUISITOS DO FORNECEDOR

3.1. Vistoria:

3.1.1. Para a execução do objeto, não será necessária realização de vistoria.

3.2. Qualificação Técnica:

3.2.1. Qualificação técnico-profissional:

3.2.1.1. Para o objeto a ser contratado, fica dispensada a apresentação de documento relativo à qualificação técnico-profissional por não guardar relação ao objeto contratado.

3.2.2.Qualificação técnico-operacional:

3.2.2.1. Para o objeto a ser licitado, será necessária a apresentação dos seguintes documentos relativos a qualificação técnico-operacional:

3.2.2.1.1. A licitante deverá apresentar Atestado(s) de Capacidade Técnica, emitido(s) por pessoa jurídica de direito público ou privado, que comprove(m) a execução satisfatória de serviços de implantação, configuração e operação de solução de segurança do tipo *Endpoint Protection*, em quantidade mínima de 50% para o Item 1, sendo admitido o somatório de atestados.

3.2.2.1.2. A licitante deverá apresentar obrigatoriamente, no momento da habilitação, carta de autorização emitida pelo fabricante da solução ofertada, que comprove a qualificação e credenciamento da empresa vencedora junto ao fabricante, citando nominalmente este processo licitatório.

3.2.2.1.3. No caso de pessoa jurídica de direito público, o(s) atestado(s) ou certidão(ões) deverá(ão) ser assinado(s) pelo responsável do setor competente do órgão, preferencialmente munidos de mecanismos de verificação ou autenticação.

3.2.2.1.4. No caso de pessoa jurídica de direito privado, o(s) atestado(s) ou certidão(ões) deverá(ão) conter dados suficientes para identificação civil do declarante, com referência ao cargo/função que ocupa na empresa e formas de contato, ou munidos de mecanismos de verificação ou autenticação.

3.2.2.1.5. Os documentos apresentados poderão ser objeto de diligências, a critério da Administração.

3.2.3. As exigências e condições estabelecidas são pertinentes e razoáveis para a garantia de que o objeto licitado tenha a qualidade desejada.

3.2.4. As exigências relativas à capacidade técnica, seja ela de caráter técnico-profissional ou técnico-operacional, guardam amparo constitucional e não constituem, por si só, restrição indevida ao caráter competitivo de uma licitação.

4. MODELO DE GESTÃO

4.1. A fiscalização do objeto será realizada pelo Secretaria de Tecnologia da Informação e Comunicação - SETIC

4.1.1. A execução do objeto deverá ser acompanhada e fiscalizada por servidor designado como responsável ou por seu substituto.

4.1.2. A SETIC será responsável pela avaliação da conformidade dos serviços, e anotará em registro próprio todas as ocorrências relacionadas à falhas ou problemas observados, determinando o que for necessário à regularização das mesmas.

4.1.3. A existência da fiscalização de nenhum modo diminui ou altera a responsabilidade do fornecedor na total execução do objeto.

4.1.4. Deverá ser mantido preposto, aceito pela CONTRATANTE, durante o período de execução do objeto, para representá-lo sempre que for necessário.

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

4.3. Indicação de instrumento para efetivar a contratação:

4.3.1 Será necessária a formalização de contrato para a execução do serviço objeto desse termo.

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

4.4. Vigência contratual:

4.4.1 A vigência do contrato a ser firmado será de 36 (trinta e seis) meses, podendo ser prorrogado na forma do art. 111 da Lei nº 14.133/21.

4.5. Índice de reajuste:

4.5.1. Os preços contratados poderão ser reajustados, após solicitação da CONTRATADA, observado o interregno mínimo de 12 (doze) meses, tendo como limite máximo a variação do Índice de Custos de Tecnologia da Informação - ICTI, ocorrida nos últimos 12 (doze) meses.

4.5.2. O interregno mínimo de 12 (doze) meses será contado a partir da data orçamento estimado, assim considerada a data de conclusão da apuração do valor estimado da contratação, ou, da planilha orçamentária, independentemente da data da tabela ou sistema referencial de custos utilizado.

4.5.3. Nos reajustamentos subsequentes ao primeiro, o interregno mínimo de 12 (doze) meses será contado da data de início dos efeitos financeiros do último reajustamento ocorrido.

4.5.4. O reajuste deverá ser solicitado antes do término da atual vigência deste Contrato, sob pena de preclusão.

4.5.5. Demais condições de repactuação estarão descritas na Minuta Contratual.

5. OBRIGAÇÕES DA CONTRATADA E DO CONTRATANTE.

5.1. São obrigações e responsabilidades do CONTRATANTE:

5.1.1. Efetuar os pagamentos nas condições e preços pactuados.

5.1.2. Promover o acompanhamento e a fiscalização da execução do objeto, sob os aspectos quantitativos e qualitativos, anotando em registro próprio as faltas detectadas e comunicando à empresa as ocorrências de qualquer fato que, a seu critério, exija medidas por parte daquela.

5.1.3. Rejeitar, no todo ou em parte, os materiais entregues em desacordo com as exigências deste Termo.

5.1.4. Notificar por escrito a ocorrência de eventuais imperfeições na execução do objeto, fixando prazo para a sua correção.

5.1.5. Proporcionar todas as facilidades para que ocorra a correta execução do objeto.

5.1.6. Comunicar qualquer irregularidade ou ilegalidade encontrada no fornecimento do objeto.

5.1.7. Prestar as informações e os esclarecimentos atinentes à execução do objeto que venham a ser solicitados.

5.1.8. Solicitar o fornecimento do objeto deste Termo de Referência.

5.1.9. Manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassados em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

5.1.10. Demais obrigações estipuladas no Contrato.

5.2. São obrigações e responsabilidades da CONTRATADA:

5.2.1. Executar o objeto desta contratação, atendendo às especificações estabelecidas neste Termo de Referência e as quantidades indicadas no instrumento contratual.

5.2.2. Manter todas as condições de habilitação e qualificação exigidas na licitação em compatibilidade com as obrigações assumidas.

5.2.3. Responsabilizar-se única e exclusivamente pelo pagamento de todos os encargos e demais despesas, diretas ou indiretas, decorrentes da execução do objeto do presente Termo de Referência, tais como impostos, taxas, contribuições fiscais, previdenciárias, trabalhistas, fundiárias; enfim, por todas as obrigações e responsabilidades, sem qualquer ônus adicional ao CONTRATANTE.

5.2.4. Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho quando, em caso de ocorrência, forem vítimas seus empregados no desempenho dos serviços ou em conexão com eles, ainda que ocorridos nas dependências do CONTRATANTE.

5.2.5. Cumprir os normativos e os procedimentos definidos pelo CONTRATANTE.

5.2.6. Primar pelo bom planejamento das atividades, utilizar as boas práticas e técnicas de governança, avaliar previamente a viabilidade técnica, os riscos e os impactos de suas ações.

5.2.7. Realizar a entrega do objeto em conformidade com os horários e períodos determinados pelo CONTRATANTE.

5.2.8. Submeter seus profissionais aos regulamentos de segurança e disciplina instituídos pelo CONTRATANTE, durante o tempo de permanência nas suas dependências.

5.2.9. Comunicar às unidades do CONTRATANTE responsáveis pela fiscalização do objeto, por escrito, qualquer anormalidade, bem como atender prontamente o que lhe for solicitado e exigido.

5.2.10. Responder por todas as despesas decorrentes do fornecimento.

5.2.11. Refazer todos os serviços que, a juízo do representante do CONTRATANTE, não forem considerados satisfatórios, sem que caiba qualquer acréscimo no custo contratado.

5.2.12. Não realizar, promover e incentivar a divulgação de qualquer dado ou informação do ambiente do CONTRATANTE.

5.2.13. Obedecer às normas internas do CONTRATANTE, relativas à segurança, à identificação, ao trânsito e à permanência de pessoas em suas dependências.

5.2.14. Manter sigilo e ciência das normas de segurança e privacidade vigentes no órgão, se responsabilizando por todos os seus empregados diretamente envolvidos na contratação.

5.2.15. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto deste contrato, devendo orientar seus profissionais nesse sentido.

5.2.16. Tratar todas as informações a que tenha acesso, em caráter de estrita confidencialidade, não podendo, sob qualquer pretexto, divulgar, revelar, reproduzir, ou delas dar conhecimento a terceiros estranhos a esta contratação, bem como utilizá-las para fins diferentes dos previstos na presente contratação.

5.2.17. Acatar as determinações feitas pela fiscalização do CONTRATANTE no que tange ao cumprimento do objeto.

5.2.18. Prestar, de imediato, todos os esclarecimentos solicitados pela fiscalização do CONTRATANTE no que diz respeito a execução do objeto.

5.2.19. Fornecer os materiais, observadas rigorosamente as especificações constantes no Termo de Referência.

5.2.20. Observar conduta adequada na utilização dos materiais, equipamentos, ferramentas e utensílios.

5.2.21. Responder pelos vícios e defeitos dos materiais e serviços e assumir os gastos e as despesas que se fizerem necessários para adimplemento das obrigações decorrentes da execução do objeto.

5.2.22. Responsabilizar-se por danos causados ao patrimônio do CONTRATANTE, ou de terceiros, ocasionados por seus profissionais, em virtude de dolo ou culpa, durante a execução do objeto.

5.2.23. Notificar, formal e tempestivamente, a CONTRANTE sobre quaisquer irregularidades e inconformidades observadas durante a execução do objeto, bem como qualquer ocorrência relativa ao comportamento de seus empregados, quando em atendimento, que venha a ser considerada prejudicial ou

inconveniente para a CONTRATADA.

5.2.24. Prestar as informações e os esclarecimentos que venham a ser solicitados pelo CONTRATANTE necessários à perfeita execução do objeto.

5.2.25. Manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassados em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

5.2.26. Demais obrigações estipuladas no Contrato.

6. REGIME DE EXECUÇÃO

6.1. A execução do objeto deste Termo de Referência será integral.

6.2. A solicitação para início da execução dos serviços será com a assinatura do contrato. A comunicação será realizada por e-mail.

6.3. A entrega das licenças de software deverá ocorrer no prazo máximo de 30 (trinta) dias corridos a contar da assinatura do contrato, podendo ser prorrogado, excepcionalmente, desde que justificado previamente pela CONTRATADA e autorizado pelo CONTRATANTE.

6.3.1. Quando da entrega, a CONTRATADA deverá comprovar, através de acesso ao site do fabricante ou entrega de documentação oficial do fabricante, a aquisição das licenças de software em nome do TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS.

6.4. A necessidade de manter a padronização da infraestrutura de segurança da informação do Tribunal de Justiça do Amazonas (TJAM) justifica a dispensa do levantamento de mercado para esta contratação. O Tribunal utiliza, de forma contínua, desde o ano de 2020, a solução de antivírus corporativo da fabricante Kaspersky, a qual se encontra plenamente integrada ao ambiente tecnológico institucional, atendendo de forma satisfatória aos requisitos de proteção de endpoints, servidores e estações de trabalho. Tal justificativa encontra respaldo no art. 41, inciso I, alíneas “a” e “b”, da Lei nº 14.133/2021, que permite a indicação de marcas e modelos específicos quando necessária a manutenção da padronização e da compatibilidade com soluções já adotadas pela Administração.

6.5. O objeto deste Termo de referência será recebido da seguinte forma:

6.5.1. **Provisoriamente**, no prazo de 05 dias, pelo responsável por seu acompanhamento e fiscalização, após a validação da ativação do produto disponibilizado para uso do TRIBUNAL, mediante termo detalhado, quando verificado o cumprimento das exigências de caráter técnico.

6.5.2. **Definitivamente**, no prazo de 15 dias, por servidor ou comissão designada pela autoridade competente, mediante termo detalhado que comprove o atendimento das exigências contratuais, após a apresentação do relatório de disponibilidade pela contratada.

6.5.3. O objeto será recusado caso não atenda as especificações técnicas solicitadas no Termo de Referência, devendo a empresa providenciar os ajustes necessários para adequação, em um prazo de 03 dias corridos contados a partir da comunicação, quando do não aceite.

6.5.4. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

6.5.5. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do objeto.

6.6. 6.5. Garantia ou assistência técnica: conforme estabelecido no item 1.3.8.

7. PENALIDADES POR DESCUMPRIMENTO CONTRATUAL

7.1. Comete infração administrativa, nos termos dos artigos 155 da Lei nº 14.133 de 2021, a CONTRATADA que incorrer nas seguintes infrações:

a) dar causa à inexecução parcial do contrato;

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

c) dar causa à inexecução total do contrato;

d) deixar de entregar a documentação exigida para o certame;

e) não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

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

g) ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

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

i) fraudar a licitação ou praticar ato fraudulento na execução do contrato;

j) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

l) praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

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

n) Inobservância dos prazos contratuais;

o) Inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia, quando houver previsão contratual de sua exigência.

7.2. Poderão ser aplicadas à CONTRATADA que incorrer nas infrações previstas neste Termo de Referência as seguintes sanções:

a) Advertência;

b) Impedimento de licitar e contratar;

c) Declaração de inidoneidade para licitar e contratar;

d) Multa de 0,5% a 30% do valor do contrato.

7.3. Na aplicação das sanções serão considerados, conforme o art. 156, §1º, da Lei nº 14.133, de 2021:

a) A natureza e a gravidade da infração cometida;

b) As peculiaridades do caso concreto;

c) As circunstâncias agravantes ou atenuantes;

d) Os danos que dela provierem para o Tribunal;

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

7.4. As infrações e sanções administrativas observarão os termos de cláusula específica da Minuta Contratual.

8. ADOÇÃO DE IMR OU ANS

8.1. Não se aplica.

9. FORMA DE PAGAMENTO

9.1. O pagamento será efetuado em até 30 (trinta) dias, mediante apresentação da Nota Fiscal/Fatura, após ser devidamente atestada a sua conformidade pelo Fiscal designado para acompanhar e fiscalizar a execução.

9.2. O pagamento será efetuado por meio de Ordem Bancária Eletrônica em conta corrente indicada na Nota Fiscal/Fatura, devendo, para isso, ficar explícito o nome do banco, agência, localidade e número da conta corrente em que deverá ser efetivado o crédito.

9.3. Caso a CONTRATADA seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES, a mesma deverá apresentar, juntamente com a Nota Fiscal/Fatura, a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor.

9.4. Para a efetivação do pagamento deverão ser mantidas as mesmas condições iniciais de habilitação, cumpridos os seguintes requisitos: Comprovação da regularidade fiscal da CONTRATADA para com a Fazenda Federal, Estadual e Municipal; Comprovação da regularidade fiscal da CONTRATADA relativa à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço (FGTS), demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei; Comprovação de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de Certidão Negativa de Débitos Trabalhistas (CNDT); Comprovação de regularidade junto ao Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis); e o Cadastro Nacional de Empresas Punidas (Cnep).

9.5. A Nota Fiscal/Fatura correspondente será examinada diretamente pelo Fiscal designado pela CONTRATANTE, o qual somente atestará a prestação do serviço contratado e liberará a referida Nota Fiscal/Fatura para pagamento quando cumpridas, pela CONTRATADA, todas as condições pactuadas.

9.6. Havendo erro na Nota Fiscal/Fatura ou circunstância que impeça a liquidação da despesa, aquela será devolvida pelo Fiscal à CONTRATADA e o pagamento ficará pendente até que a mesma providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento será interrompido e reiniciado a partir da regularização da situação ou reapresentação do documento fiscal, não acarretando qualquer ônus para o CONTRATANTE.

9.7. O pagamento observará, ainda, as demais disposições contidas em Cláusula específica da Minuta Contratual.

10. GARANTIA CONTRATUAL

10.1. A CONTRATADA deverá apresentar ao CONTRATANTE, em até 05 (cinco) dias úteis, contados da assinatura do contrato, comprovante de garantia, no valor correspondente a 5% (cinco por cento) do valor total do contrato, cabendo-lhe optar por uma das modalidades de garantia prevista no art. 96, § 1º da Lei n.º 14.133/2021.

10.2. A garantia deverá ser prestada com vigência de 03 (três) meses após o término da vigência do Contrato e será restituída automaticamente, ou por solicitação, no prazo de até 60 (sessenta) dias contados do final da vigência do contrato ou da rescisão, somente após comprovação de que a empresa pagou todas as verbas rescisórias trabalhistas decorrentes da contratação.

10.2.1. Caso a CONTRATADA não efetive o cumprimento das obrigações previstas no subitem anterior, a garantia será utilizada para o pagamento dessas verbas trabalhistas diretamente pelo CONTRATANTE.

10.3. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

10.3.1. Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

10.3.2. Multas moratórias e punitivas aplicadas pela Administração à contratada; e

10.3.3. Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo contratado, quando couber.

10.4. Quando a garantia for apresentada em dinheiro, ela será atualizada monetariamente, conforme os critérios estabelecidos pela instituição bancária em que for realizado o depósito.

10.5. Quando a opção da garantia for a modalidade de seguro-garantia, a apólice deverá conter cláusulas específicas, oferecendo cobertura para despesas com obrigações contratuais e riscos trabalhistas, bem como multas que tenham caráter punitivo.

10.6. Aditado o Contrato, prorrogado o prazo de sua vigência ou alterado o seu valor, fica a CONTRATADA obrigada a apresentar garantia complementar ou substituí-la, no mesmo percentual e modalidades constantes desta cláusula. Nesses casos, a garantia será liberada após a apresentação da nova garantia e da assinatura do termo aditivo ao Contrato.

10.7. Nas hipóteses em que a garantia for utilizada total ou parcialmente – como para corrigir quaisquer imperfeições na execução do objeto do contrato ou para reparar danos decorrentes da ação ou omissão da CONTRATADA, de seu preposto ou de quem em seu nome agir, ou ainda nos casos de multas aplicadas depois de esgotado o prazo recursal – a CONTRATADA deverá, no prazo de 03 (três) dias, recompor o valor total dessa garantia, sob pena de aplicação de penalidades previstas neste Contrato.

10.8. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

11. CLÁUSULAS DE SUSTENTABILIDADE

11.1. Desenvolvimento Nacional Sustentável

11.1.1. A CONTRATADA deverá pautar sua atuação pela promoção do desenvolvimento nacional sustentável, em conformidade com a Constituição Federal (arts. 170 e 225), Lei nº 14.133/2021 (art. 5º) e Resoluções CNJ nº 400/2021 e 641/2025.

11.1.2. A CONTRATADA assume responsabilidade ambiental integral pela execução do contrato, adotando melhores práticas de gestão para prevenir e mitigar impactos ambientais, sociais e econômicos, mantendo conformidade com legislação federal, estadual e municipal.

11.2. Redução de Emissões de Gases de Efeito Estufa (GEE)

11.2.1. Otimização de rotas de transporte e logística;

11.2.2. Adoção de fontes de energia renovável;

11.2.3. Implementação de programas de eficiência energética;

11.2.4. Redução de consumo de materiais e economia circular;

11.3. Eficiência no Uso de Recursos Naturais

11.3.1. Recomenda-se à CONTRATADA adotar práticas para uso racional de água e energia elétrica, utilizando equipamentos de menor consumo e implementando programas internos de conscientização.

11.4. Responsabilidade Social e Governança

11.4.1. Recomenda-se adoção de políticas internas de inclusão e diversidade, promovendo equidade de gênero, raça e acessibilidade, com cumprimento de cotas legais para PCD e aprendizes.

11.4.2. A CONTRATADA deverá manter integridade e transparência, abstendo-se de práticas de corrupção, fraude, conluio ou coação.

12. RESPONSÁVEIS PELO TERMO DE REFERÊNCIA

12.1. Subscrevem o Termo de Referência os servidores responsáveis por sua elaboração, nos moldes e parâmetros estabelecidos pelo Tribunal de Justiça do Estado do Amazonas. Além da exigência legal da aprovação da autoridade competente, o instrumento em tela carece da ratificação de que retrata o que fora ordenado aos responsáveis por sua elaboração.

13. DOS ANEXOS

13.1. São partes integrantes deste Termo de Referência os seguintes anexos:

a) Mapa de Gerenciamento de Riscos na Contratação;

b) Estudo Técnico Preliminar;

c) Mapa de Preços.

Manaus, *data do sistema*

assinado digitalmente
Matheus Barreto dos Santos

Seção de Elaboração de Artefatos da Contratação

Documento assinado eletronicamente por **Karla Rozeana Bau Zarth**, **Servidor**, em 23/04/2026, às 13:02, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjam.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2845378** e o código CRC **D5C9E413**.

TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
Av. André Araújo, S/N - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tjam.jus.br

ANEXO

MAPA DE GERENCIAMENTO DE RISCOS

Processo SEI nº 2026/000002456-00 — Contratação de Solução Antivírus/EDR Kaspersky Next EDR Optimum

ID	EVENTO DE RISCO	CAUSA	CONSEQUÊNCIA	PROBABILIDADE (1-5)	IMPACTO (1-5)	NÍVEL DO RISCO	AÇÕES PREVENTIVAS (MITIGAÇÃO)	AÇÕES DE CONTINGÊNCIA (CORREÇÃO)	RESPONSÁVEL
R01	Atraso na disponibilização das licenças e acesso ao console de gerenciamento	Problemas logísticos, burocráticos ou técnicos na ativação das licenças pelo fornecedor	Descontinuidade da proteção dos endpoints e vulnerabilidade da infraestrutura do TJAM	2	5	ELEVADO	Exigir prazo de entrega de 15 dias no TR; incluir penalidades específicas por atraso na ativação; exigir plano de contingência do fornecedor	Acionar o suporte emergencial do fabricante; prorrogar temporariamente o contrato vigente; notificar a contratada formalmente e iniciar contagem de multa	Fiscal Técnico / DVITIC
R02	Fornecimento de licenças inautênticas, piratas ou em desconformidade	Empresa contratada não é revendedora autorizada do fabricante; fraude na cadeia de fornecimento	Risco jurídico e de segurança; bloqueio das licenças pelo fabricante; interrupção total da proteção	2	5	ELEVADO	Exigir declaração de parceiro/revendedor autorizado na habilitação; verificar o status no portal oficial do fabricante antes da assinatura do contrato	Rescindir o contrato; acionar o fabricante; registrar ocorrência policial; acionar o seguro-garantia	Fiscal Técnico / DVITIC
R03	Descumprimento dos Níveis de Serviço (SLA) para incidentes críticos	Falta de equipe técnica certificada; sobrecarga do fornecedor; ausência de estrutura de suporte adequada	Incidentes cibernéticos sem resposta tempestiva; propagação de ameaças; danos à reputação e à continuidade dos serviços	3	4	ELEVADO	Definir SLAs claros no Anexo I (1h para críticos); exigir relatório mensal de SLA; incluir penalidades por descumprimento; exigir certificação do fabricante para a equipe	Acionar diretamente o suporte do fabricante; aplicar glosa proporcional; emitir notificação formal; instaurar processo de apuração de responsabilidade	Fiscal Técnico / DVITIC
R04	Incidente cibernético grave (ransomware, APT) não detectado pela solução	Configuração inadequada das políticas de segurança; falha na solução; ameaça de dia-zero sem assinatura disponível	Comprometimento de dados sigilosos do Poder Judiciário; interrupção de serviços jurisdicionais; danos à imagem institucional	2	5	ELEVADO	Exigir módulo EDR com análise comportamental e sandbox em nuvem; exigir atualização automática de assinaturas; contratar banco de horas para otimização contínua das políticas	Acionar o Plano de Resposta a Incidentes do TJAM; isolar os ativos comprometidos; acionar o CSIRT do CNJ; acionar a contratada para suporte emergencial prioritário	Gestor do Contrato / SETIC
R05	Incompatibilidade técnica com a infraestrutura existente do TJAM	Versão da solução incompatível com sistemas operacionais legados; conflito com outros softwares instalados	Falhas de funcionamento nos endpoints; necessidade de adequações não previstas; atrasos na implantação	2	3	MODERADO	Exigir catálogos técnicos detalhando compatibilidade com Windows, Linux, macOS e versões legadas; realizar Prova de Conceito (PoC) antes do aceite definitivo	Acionar o banco de horas de consultoria para resolução; solicitar atualização de compatibilidade ao fabricante; avaliar exceções para ativos legados	Fiscal Técnico / DVITIC
R06	Vazamento de dados de logs e monitoramento de endpoints (LGPD)	Acesso indevido da contratada a dados pessoais de servidores; falha de segurança no console de gerenciamento em nuvem	Violação da LGPD; sanções administrativas; danos à imagem do TJAM	2	4	MODERADO	Incluir cláusula de confidencialidade e LGPD no contrato; exigir que o console em nuvem esteja em data center com certificação ISO 27001; exigir relatório de conformidade LGPD	Notificar a ANPD; acionar o DPO do TJAM; rescindir o contrato se houver violação grave; aplicar as penalidades contratuais	Gestor do Contrato / DPO-TJAM
R07	Perda do credenciamento ou autorização do fabricante pela contratada durante a vigência	Descumprimento de requisitos do programa de parceiros do fabricante; mudanças societárias na contratada	Impossibilidade de renovação de licenças; perda de acesso ao suporte técnico de nível superior; risco de licenças inválidas	1	5	MODERADO	Incluir cláusula contratual exigindo manutenção do status de parceiro autorizado durante toda a vigência; exigir comprovação anual	Notificar a contratada; conceder prazo para regularização; rescindir o contrato e realizar nova licitação emergencial se não houver regularização	Fiscal Técnico / DVITIC

LEGENDA — NÍVEIS DE RISCO E MATRIZ DE PROBABILIDADE × IMPACTO

TABELA DE NÍVEIS DE RISCO

NÍVEL	COR	FAIXA DE PONTUAÇÃO (Prob × Impacto)	DESCRIÇÃO	AÇÃO REQUERIDA	PRAZO
EXTREMO	■ EXTREMO	≥ 15	Risco inaceitável. Ameaça crítica à continuidade dos serviços.	Ação imediata da Alta Gestão	Imediato
ELEVADO	■ ELEVADO	8 a 14	Risco significativo. Requer atenção prioritária.	Ação do Gestor do Contrato	Até 15 dias
MODERADO	■ MODERADO	4 a 7	Risco tolerável com monitoramento contínuo.	Ação do Fiscal do Contrato	Até 30 dias
BAIXO	■ BAIXO	1 a 3	Risco aceitável. Monitoramento periódico suficiente.	Monitoramento rotineiro	Contínuo

MATRIZ DE PROBABILIDADE × IMPACTO

PROBABILIDADE ↓ / IMPACT →	Muito Baixo (1)	Baixo (2)	Médio (3)	Alto (4)	Muito Alto (5)
Muito Alta (5)	5	10	15	20	25
Alta (4)	4	8	12	16	20
Média (3)	3	6	9	12	15
Baixa (2)	2	4	6	8	10
Muito Baixa (1)	1	2	3	4	5

Documento assinado eletronicamente por **Matheus Barreto dos Santos**, **Servidor**, em 12/03/2026, às 14:13, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjam.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2769454** e o código CRC **20020268**.

2026/000002456-00 2769454v2

TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
Av. André Araújo, S/N - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tjam.jus.br

ESTUDO TÉCNICO PRELIMINAR - TJ/AM/SETIC/DVITIC

Responsáveis pela elaboração:

Diogo Mendonça de Sousa

Rafael Araújo da Silva

Contato: (92) 99239-1948

Número de identificação do ETP: 2735870

Categoria do Objeto: Serviços de licenciamento de uso de softwares e suporte técnico

CATSER: 27456

1. PREVISÃO NO PLANO DE CONTRATAÇÕES ANUAL

1.1 O objeto da pretensa contratação está previsto no PCA (Plano de Contratações Anual) / 2026, conforme **RESOLUÇÃO Nº 30, DE 11 DE NOVEMBRO DE 2025,** disponibilizado no painel *BI* disponível NESTE LINK, sob o código **SETIC-2026-72**, totalizando **R$ 2.400.000,00** de recurso disponível.

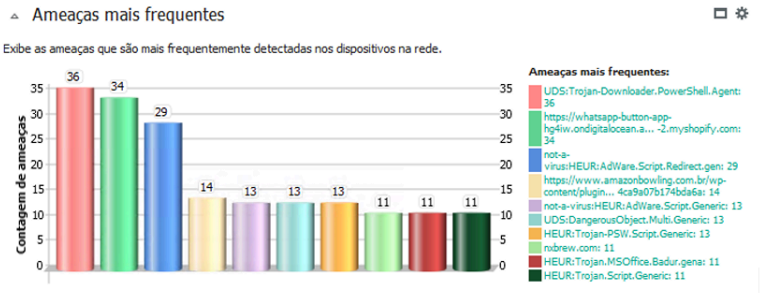
2. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1 Fundamentação e descrição da necessidade da contratação:

Considerando que as licenças do software antivírus atualmente em uso pelo TJAM, bem como os serviços de suporte técnico, terão sua validade expirada em 26/03/2026 e que, consequentemente, passarão a não ter mais atualizações das bases de dados de vírus e correções de erros, os sistemas que dependem dos respectivos softwares passarão a ficar vulneráveis a novas ameaças que surgirem, por isso se faz necessária a aquisição desses softwares em suas versões mais atuais, com o respectivo suporte técnico, para garantir o perfeito funcionamento dos dispositivos que deles são dependentes. Considerando a importância vital que os sistemas e serviços de TI adquiriram para as organizações e a constante diversificação e desenvolvimento de novas ameaças cibernéticas ao longo do tempo, torna-se mandatório o uso de uma solução de antivírus e a disponibilidade de apoio técnico especializado na ferramenta para atingir as metas de segurança da informação, garantir a continuidade dos serviços essenciais e que esteja totalmente alinhada ao ambiente e às melhores práticas de segurança da Informação.

2.2 Evidências técnicas do ambiente em produção:

A necessidade da presente contratação fundamenta-se nas evidências técnicas extraídas da solução de segurança Kaspersky atualmente em produção no ambiente do Tribunal de Justiça do Estado do Amazonas (TJAM). Conforme resultados extraídos da ferramenta de gerenciamento da solução, referente aos últimos 30 (trinta) dias de operação, foram detectadas e bloqueadas diversas tentativas de ameaças cibernéticas, demonstrando a exposição contínua do ambiente institucional a riscos de segurança da informação. Os dados consolidados, apresentados por meio de gráfico ilustrativo, evidenciam a efetividade da solução na mitigação dessas ameaças.



2.3 Evolução e complexidade das ameaças cibernéticas:

Observa-se, de forma contínua, a evolução, diversificação e aumento da complexidade das ameaças cibernéticas, incluindo malwares avançados, ransomwares, ataques direcionados, exploração de vulnerabilidades e tentativas de acesso não autorizado. Tal cenário exige a utilização de soluções de antivírus corporativas robustas, constantemente atualizadas e alinhadas às melhores práticas de segurança da informação, capazes de atuar de forma preventiva, corretiva e reativa diante de incidentes de segurança.

2.4 Padronização, gerenciamento e suporte técnico:

A contratação da solução de antivírus com suporte técnico ativo permitirá manter a padronização do ambiente tecnológico já adotado pelo TJAM, reduzir riscos operacionais e facilitar o gerenciamento centralizado da segurança dos endpoints. Ademais, o suporte técnico especializado é fundamental para auxiliar a equipe interna de TI na correta administração da solução, na rápida resolução de incidentes e na aplicação adequada das políticas de segurança da informação, contribuindo para a continuidade dos serviços essenciais e para a preservação da confidencialidade, integridade e disponibilidade das informações institucionais.

2.11 As normas vigentes aplicáveis a esta contratação incluem, mas não se limitam a:

2.11.1 Lei nº 14.133/2021: Lei de Licitações e Contratos da Administração Pública.

2.11.2 Resolução CNJ nº 468/2022: Diretrizes para contratações de Soluções de Tecnologia da Informação e Comunicação (STIC) pelos órgãos do Poder Judiciário.

2.11.3 Resolução CNJ nº 370/2021: Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

3. UNIDADE DEMANDANTE

3.1 A unidade demandante responsável pelo desenvolvimento e acompanhamento deste estudo será a Secretaria de Tecnologia da Informação e Comunicação - SETIC.

4. REQUISITOS DA CONTRATAÇÃO

4.1 A contratação não é de natureza contínua.

4.2 O contrato terá duração de 36 meses, podendo ser prorrogado nos termos dos arts. 105 e seguintes da Lei n.° 14.133/21.

4.3 Sugere-se que a licitação seja realizada na modalidade Pregão Eletrônico por menor preço global.

4.4 Quando da entrega, a CONTRATADA deverá comprovar, através de acesso ao site do fabricante ou entrega de documentação oficial do fabricante, a aquisição das licenças de software em nome do TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS.

4.5 A entrega das licenças de software deverá ocorrer no prazo máximo de 30 (trinta) dias corridos a contar da assinatura do contrato, podendo ser prorrogado, excepcionalmente, desde que justificado previamente pela CONTRATADA e autorizado pelo CONTRATANTE.

4.6 Considerando a complexidade e o impacto das soluções a serem implantadas, ficam estabelecidos os seguintes requisitos de capacitação técnica, em conformidade com o disposto no art. 67 da Lei nº 14.133/2021, que autoriza a exigência de comprovação de qualificação técnico-profissional e técnico-operacional:

4.6.1 A licitante deverá apresentar Atestado(s) de Capacidade Técnica, emitido(s) por pessoa jurídica de direito público ou privado, que comprove(m) a execução satisfatória de serviços de implantação, configuração e operação de solução de segurança do tipo *Endpoint Protection*, em quantidade mínima de 50% da quantidade objeto deste edital.

4.6.2 Para assegurar a autenticidade, procedência e regularidade técnica da solução de segurança EDR (Endpoint Detection and Response), a licitante deverá apresentar obrigatoriamente, no momento da habilitação, carta de autorização emitida pelo fabricante da solução ofertada, que comprove a qualificação e credenciamento da empresa vencedora junto ao fabricante, citando nominalmente este processo licitatório.

5. LEVANTAMENTO DE MERCADO E JUSTIFICATIVA DA ESCOLHA DO TIPO DE SOLUÇÃO A CONTRATAR

5.1 A necessidade de manter a padronização da infraestrutura de segurança da informação do Tribunal de Justiça do Amazonas (TJAM) justifica a dispensa do levantamento de mercado para esta contratação. O Tribunal utiliza, de forma contínua, desde o ano de 2020, a solução de antivírus corporativo da fabricante Kaspersky, a qual se encontra plenamente integrada ao ambiente tecnológico institucional, atendendo de forma satisfatória aos requisitos de proteção de endpoints, servidores e estações de trabalho. Tal justificativa encontra respaldo no art. 41, inciso I, alíneas “a” e “b”, da Lei nº 14.133/2021, que permite a indicação de marcas e modelos específicos quando necessária a manutenção da padronização e da compatibilidade com soluções já adotadas pela Administração.

5.2 A adoção de solução antivírus distinta da atualmente utilizada poderia acarretar impactos negativos relevantes, tais como aumento dos custos operacionais, necessidade de reconfiguração de políticas de segurança, migração de agentes, readequação de processos internos e capacitação adicional da equipe técnica. Além disso, a substituição da tecnologia vigente poderia comprometer temporariamente o nível de proteção do ambiente computacional, contrariando os princípios da eficiência, da economicidade e da continuidade do serviço público.

5.3 A padronização da solução de antivírus corporativo contribui para a redução da complexidade na administração da segurança da informação, facilita o gerenciamento centralizado, mantém a curva de aprendizado da equipe técnica em patamar adequado e assegura a plena compatibilidade com os sistemas e procedimentos já estabelecidos no TJAM. Esse alinhamento atende ao disposto no art. 47, inciso I, da Lei nº 14.133/2021, que determina a observância do princípio da padronização, visando à compatibilidade técnica e ao desempenho adequado das soluções contratadas.

5.4 A continuidade da utilização da solução Kaspersky minimiza riscos operacionais, preserva a estabilidade do ambiente computacional e garante a manutenção dos níveis de segurança já alcançados, sem a necessidade de adaptações técnicas complexas ou investimentos adicionais desnecessários. Dessa forma, a dispensa do levantamento de mercado se justifica não apenas pela manutenção da padronização tecnológica do TJAM, mas também pelo respaldo legal conferido pela Lei nº 14.133/2021, assegurando eficiência, economicidade e continuidade dos serviços públicos.

5.5 Ressalta-se, ainda, que a solução Kaspersky não se caracteriza como produto de fornecedor exclusivo, sendo comercializada por diversas empresas autorizadas no território nacional. A fabricante mantém um amplo ecossistema de parceiros e revendedores credenciados, o que assegura a competitividade na futura contratação e possibilita à Administração a obtenção da proposta mais vantajosa, afastando qualquer restrição indevida à ampla concorrência.

6. DESCRIÇÃO DA SOLUÇÃO ESCOLHIDA

6.1 Do módulo de proteção de endpoint

6.1.1 A solução proposta deverá proteger os sistemas operacionais abaixo:
a) Windows 7;

b) Windows 8;
c) Windows 8.1;
d) Windows 10;
e) Windows 11.

6.1.2 Servidores:
a) Windows Small Business Server 2011;
b) Windows MultiPoint Server 2011;
c) Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022.

6.1.3 Servidores de terminal Microsoft:
a) Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022.

6.1.4 Sistemas operacionais Linux de 32 bits:
a) CentOS 6.7 e posterior;
b) Debian GNU/Linux 11.0 e posterior;
c) Debian GNU/Linux 12.0 e posterior;
d) Red Hat Enterprise Linux 6.7 e posterior.

6.1.5 Sistemas operacionais Linux de 64 bits:
a) Amazon Linux 2;
b) CentOS 6.7 e mais tarde;
c) CentOS 7.2 e posterior;
d) CentOS Stream 8;
e) CentOS Stream 9;
f) Debian GNU/Linux 11.0 e posterior;
g) Debian GNU/Linux 12.0 e posterior;
h) Linux Mint 20.3 e superior;
i) Linux Mint 21.1 e posterior;
j) openSUSE Leap 15.0 e posterior;
k) Oracle Linux 7.3 e posterior;
l) Oracle Linux 8.0 e posterior;
m) Oracle Linux 9.0 e posterior;
n) Red Hat Enterprise Linux 6.7 e posterior;
o) Red Hat Enterprise Linux 7.2 e posterior;
p) Red Hat Enterprise Linux 8.0 e posterior;
q) Red Hat Enterprise Linux 9.0 e posterior;
r) Rocky Linux 8.5 e posterior;
s) Rocky Linux 9.1;
t) SUSE Linux Enterprise Server 12.5 ou posterior;
u) SUSE Linux Enterprise Server 15 ou posterior;
v) Ubuntu 20.04 LTS;
w) Ubuntu 22.04 LTS.

6.1.6 Sistemas operacionais Arm de 64 bits:
a) CentOS Stream 9;
b) SUSE Linux Enterprise Server 15;
c) Ubuntu 22.04 LTS.

6.1.7 Sistemas operacionais MAC OS:
a) macOS 12 – 14.

6.1.8 Ferramentas de virtualização MAC OS:
a) Parallels Desktop 16 para Mac Business Edition ou superior;
b) VMware Fusion 11.5 Profissional ou superior.

6.1.9 A solução proposta deverá suportar as seguintes plataformas virtuais:
a) VMware Workstation;
b) VMware ESXi;
c) Microsoft Hyper-V Server;
d) Citrix Virtual Apps e Desktop;
e) Citrix Provisioning.

6.2 Do módulo de gerenciamento avançado

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

6.2.2 A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:
a) Amazon Web Services;
b) Microsoft Azure;
c) Google Cloud.

6.2.3 A solução proposta deve incluir as seguintes opções de integração SIEM:
a) HP (Microfoco) ArcSight;
b) IBM QRadar;
c) Splunk;
d) Kaspersky KUMA.

6.2.4 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.

6.2.5 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.

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

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

6.2.8 A o modulo da solução on-premisse deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

6.2.9 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.

6.2.10 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.

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

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

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

6.2.14 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:
a) Status do dispositivo;
b) Tag;
c) Diretório ativo;
d) Proprietários de dispositivos;
e) Hardware.

6.2.15 A solução proposta deve suportar os seguintes canais de entrega de notificação:
a) E-mail;
b) Registro de sistema;
c) SMS.

6.2.16 A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:
a) Atributos de rede;
b) Nome;
c) Domínio e/ou Sufixo de Domínio;
d) Endereço de IP;
e) Endereço IP para servidor de gerenciamento;
f) Localização no Active Directory;
g) Unidade organizacional;
h) Grupo;
i) Sistema operacional;
j) Número do pacote de serviço;
k) Arquitetura Virtual;
l) Registro de aplicativos;
m) Nome da Aplicação;
n) Versão do aplicativo;
o) Fabricante;
p) Tipo e versão;
q) Arquitetura.

6.2.17 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.

6.2.18 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.

6.2.19 As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:
a) Dispositivos Desktop/Servidores;
b) Dispositivos móveis;
c) Dispositivos de rede;
d) Dispositivos virtuais;
e) Componentes OEM;

f) Periféricos de computador;
g) Dispositivos IoT conectados;
h) Telefones VoIP;
i) Repositórios de rede.

6.2.20 A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:
a) Nome da Aplicação;
b) Caminho do aplicativo;
c) Metadados do aplicativo;
d) Aplicativo Certificado digital;
e) Categorias de aplicativos predefinidas pelo fornecedor;
f) SHA256 e MD5.

6.2.21 A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:
a) Bluetooth;
b) Dispositivos móveis;
c) Modems externos;
d) CD/DVD;
e) Câmeras e scanners;
f) MTPs;
g) E a transferência de dados para dispositivos móveis.

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

6.2.23 A solução proposta 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.

6.2.24 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:
a) Estruturas de domínios e grupos de trabalho do Windows;
b) Estruturas de grupos do Active Directory;
c) Conteúdo de um arquivo de texto criado manualmente pelo administrador.

6.2.25 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.

6.2.26 A solução proposta deve permitir realizar as seguintes ações para endpoints:
a) Verificação manual;
b) Verificação no acesso;
c) Verificação por demanda;
d) Verificação de arquivos compactados;
e) Verificação de arquivos individuais, pastas e unidades;
f) Bloqueio e verificação de scripts;
g) Proteção contra alteração de registros;
h) Proteção contra estouro de buffer;
i) Verificação em segundo plano/inativa;
j) Verificação de unidade removível na conexão com o sistema.

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

6.2.28 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.

6.2.29 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.

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

6.2.31 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.

6.2.32 A solução proposta deve suportar Windows Failover Cluster.

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

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

6.2.35 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.

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

6.2.37 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.

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

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

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

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

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

6.2.43 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 específico de prevenção de intrusão.

6.2.44 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.

6.2.45 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).

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

6.2.47 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.

6.2.48 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.

6.2.49 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.

6.2.50 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.

6.2.51 A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.

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

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

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

6.2.55 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.

6.2.56 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.

6.2.57 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.

6.2.58 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.

6.2.59 A solução proposta deve permitir ao administrador personalizar relatórios.

6.2.60 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.

6.2.61 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.

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

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

6.2.64 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.

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

6.2.66 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.

6.2.67 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.

6.2.68 A solução proposta deve suportar integração com solução APT.

6.2.69 A solução proposta deve suportar a integração com o serviço Managed Detection and Response.

6.2.70 A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:
a) Windows;
b) Linux.

6.2.71 A solução proposta deverá suportar os seguintes servidores de banco de dados:
a) Windows: Microsoft SQL Server; Microsoft Banco de dados SQL do Azure; MySQL Standard e Enterprise; MariaDB; PostgreSQL.
b) Linux: MySQL; MariaDB; PostgreSQL.

6.2.72 A solução proposta deverá suportar as seguintes plataformas virtuais:
a) Windows: VMware vSphere 6.7 e 7.0; Estação de trabalho VMware 16 Pro; Servidor Microsoft Hyper-V 2012 de 64 bits; Servidor Microsoft Hyper-V 2012 R2 de 64 bits; Microsoft Servidor Hyper -V 2016 de 64 bits; Servidor Microsoft Hyper-V 2019 de 64 bits; Servidor Microsoft Hyper-V 2022 de 64 bits; Citrix XenServer 7.1 LTSR; Citrix XenServer 8.x; Oracle VM VirtualBox 6.x.

b) Linux: VMware vSphere 6.7 e 7.0; VMware Desktop 16 Pro e 17 Pro; Servidor Microsoft Hyper-V 2012 de 64 bits; Servidor Microsoft Hyper-V 2012 R2 de 64 bits; Microsoft Servidor Hyper -V 2016 de 64 bits; Servidor Microsoft Hyper-V 2019 de 64 bits; Servidor Microsoft Hyper-V 2022 de 64 bits; Citrix XenServer 7.1 e 8.x; Oracle VM VirtualBox 6.x e7.x.

6.2.73 A solução proposta deve suportar criptografia em vários níveis:
a) Criptografia completa do disco – incluindo disco do sistema;
b) Criptografia de arquivos e pastas;
c) Criptografia de mídia removível;
d) Gerenciamento de criptografia BitLocker e MacOS Filevault2.

6.2.74 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:
a) A criptografia de arquivos em unidades de computador locais;
b) A criação de listas de criptografia de arquivos por extensão ou grupo de extensões;
c) A criação de listas criptografadas de pastas em unidades de computador locais.

6.2.75 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:
a) Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis;
b) Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.

6.2.76 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:
a) A criptografia de todos os arquivos armazenados em unidades removíveis;
b) A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.

6.2.77 A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia.

6.2.78 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis.

6.2.79 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado.

6.2.80 A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.

6.2.81 A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais.

6.2.82 A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia.

6.2.83 A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados.

6.2.84 A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema.

6.2.85 A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado.

6.2.86 A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.

6.2.87 A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados.

6.2.88 A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos.

6.2.89 A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação.

6.2.90 O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados independentemente da localização e/ou usuário.

6.2.91 A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.

6.2.92 A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.

6.2.93 A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:
a) Uso do Trusted Platform Module e configurações de senha;
b) Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível;
c) Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets).

6.2.94 A solução proposta deve suportar criptografia em Microsoft Surface Tablets.

6.2.95 A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:
a) Instalação remota de software de terceiros;
b) Relatórios sobre software e hardware existentes;
c) Monitoramento para instalação de software não autorizado;
d) Remoção de software não autorizado.

6.2.96 A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.

6.2.97 A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.

6.2.98 A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.

6.2.99 A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais.

6.2.100 A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.

6.2.101 A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.

6.2.102 O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.

6.2.103 A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança.

6.2.104 A solução proposta deve permitir ao administrador aprovar atualizações.

6.2.105 A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.

6.2.106 A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.

6.2.107 A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.

6.2.108 A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.

6.2.109 A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.

6.2.110 A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências).

6.2.111 A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.

6.2.112 A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.

6.2.113 A solução proposta deve incluir campos dedicados que contenham informações sobre ‘Exploração encontrada para a vulnerabilidade’.

6.2.114 A solução proposta deve incluir campos dedicados que contenham informações sobre “Ameaça encontrada para a vulnerabilidade”.

6.2.115 A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.

6.2.116 A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.

6.2.117 A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.

6.2.118 A solução proposta deve apoiar a implantação do sistema operacional.

6.2.119 A solução proposta deve suportar Wake-on LAN e UEFI.

6.2.120 A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server.

6.2.121 A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.

6.2.122 A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador.

6.2.123 A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.

6.2.124 A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.

6.2.125 A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.

6.2.126 A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota.

6.2.127 A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.

6.2.128 A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros.

6.2.129 A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:
a) Inicie a instalação ao reiniciar ou desligar o computador;
b) Instale o gerador necessário todos os pré-requisitos do sistema;
c) Permitir a instalação de novas versões de aplicativos durante as atualizações;
d) Baixe atualizações para o dispositivo sem instalá-las.

6.2.130 A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas.

6.2.131 A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.

6.2.132 O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:
a) CEF;
b) LEEF.

6.2.133 A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.

6.2.134 O relatório da solução proposta deve conter informações CVE.

6.2.135 A solução proposta deve suportar instalação de aplicações e software de terceiros.

6.3 Do módulo de gerenciamento simplificado

6.3.1 A solução proposta deve suportar arquitetura cloud.

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

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

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

6.3.5 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.

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

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

6.3.8 A solução proposta deve incluir informações do endpoint:
a) IP público de internet;
b) IP interno do dispositivo;
c) Versão do agente de proteção;
d) Ultima comunicação com a console, contendo data e hora;
e) Informações do sistema operacional.

6.3.9 A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365.

6.3.10 A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365.

6.3.11 A solução proposta deve incluir treinamento em segurança cibernética.

6.4 Requisitos gerais

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

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

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

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

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

6.4.6 A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:
a) Proteção contra ameaças sem arquivos (Fileless);
b) Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque.

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

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

6.4.9 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.

6.4.10 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.

6.4.11 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.

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

6.4.13 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.

6.4.14 A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:
a) Controles de aplicativos;
b) Controle web e dispositivos;
c) HIPS e Firewall;
d) Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;
e) Gerenciamento de criptografia de arquivos e discos;
f) Controle adaptativo para detecção de anomalias.

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

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

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

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

6.4.19 A solução proposta deve incluir um módulo capaz, no mínimo, de:
a) Bloqueio de aplicativos com base em sua categorização;
b) Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos;
c) A adição de sub-redes e a modificação de permissões de atividade.

6.4.20 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.

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

6.4.22 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.

6.4.23 A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:
a) Modo silencioso;
b) Discos rígidos e dispositivos removíveis;
c) De todos as contas de usuários do dispositivo.

6.4.24 A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:
a) Exclusão imediata de dados;
b) Exclusão de dados adiada.

6.4.25 A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:
a) Excluir usando os recursos do sistema operacional - os arquivos são excluídos;
b) Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.

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

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

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

6.4.29 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.

6.4.30 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.

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

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

6.4.33 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.

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

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

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

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

6.4.38 A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.

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

6.4.40 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.

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

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

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

6.4.44 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.

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

6.4.46 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.

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

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

6.4.49 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.

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

6.4.51 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.

6.4.52 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.

6.4.53 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.

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

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

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

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

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

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

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

6.4.61 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.

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

6.4.63 A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:
a) Filtro de anexos;
b) Verificação de mensagens de email ao receber, ler e enviar.

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

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

6.4.66 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.).

6.4.67 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.

6.4.68 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.

6.4.69 A solução proposta deve incluir suporte ao protocolo IPv6.

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

6.4.71 A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:
a) Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo;
b) Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.

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

6.4.73 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.

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

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

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

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

6.4.78 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.

6.4.79 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.

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

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

6.4.82 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.

6.4.83 A solução proposta deve suportar endereços IPv6.

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

6.4.85 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.

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

6.4.87 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.

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

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

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

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

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

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

6.4.94 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.

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

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

6.4.97 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.

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

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

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

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

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

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

6.4.104 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.

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

6.4.106 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.

6.4.107 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.

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

6.4.109 A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:
a) Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível;
b) Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.

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

6.4.111 A solução proposta deve gerar relatoiros de vulnerabilidades encontradas nos dispositivos com sensor de end point instalado.

6.5 Do modulo de gerenciamento de dispositivos móveis

6.5.1 O modulo deve ser integrado a console de gerenciamento.

6.5.2 A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:
a) Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition).

6.5.3 A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:
a) iOS 10–17 ou iPadOS 13–17.

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

6.5.5 A solução proposta deve suportar dispositivos iOS supervisionados.

6.5.6 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.

6.5.7 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.

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

6.5.9 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).

6.5.10 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.

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

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

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

6.5.14 A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:
a) Dados em contêineres;
b) Contas de e-mail corporativo;
c) Configurações para conexão à rede Wi-Fi corporativa e VPN;

d) Nome do ponto de acesso (APN);
e) Perfil do Android for Work;
f) Recipiente KNOX;
g) Chave do gerenciador de licença KNOX.

6.5.15 A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:
a) Todos os perfis de configuração instalados;
b) Todos os perfis de provisionamento;
c) O perfil iOS MDM;
d) Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas.

6.5.16 A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo.

6.5.17 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:
a) Critérios de verificação do dispositivo;
b) 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.

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

6.5.19 A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:
a) Cartões de memória e outras unidades removíveis;
b) Câmera do dispositivo;
c) Conexões Wi-Fi;
d) Conexões Bluetooth;
e) Porta de conexão infravermelha;
f) Ativação do ponto de acesso Wi-Fi;
g) Conexão de área de trabalho remota;
h) Sincronização de área de trabalho;
i) Definir configurações da caixa de correio do Exchange;
j) Configurar caixa de e-mail em dispositivos iOS MDM;
k) Configure contêineres Samsung KNOX;
l) Definir as configurações do perfil do Android for Work;
m) Configurar e-mail/calendário/contatos;
n) Defina as configurações de restrição de conteúdo de mídia;
o) Definir configurações de proxy no dispositivo móvel;
p) Configurar certificados e SCEP.

6.5.20 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.
a) Portal de inscrição móvel KNOX;
b) Pacotes de instalação pré-configurados independentes.

6.5.21 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.

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

6.5.23 A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:
a) VMware AirWatch 9.3 ou posterior;
b) MobileIron 10.0 ou posterior;
c) IBM MaaS360 10.68 ou posterior;
d) Microsoft Intune 1908 ou posterior;
e) SOTI MobiControl 14.1.4 (1693) ou posterior.

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

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

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

6.5.27 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.

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

6.5.29 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.

6.5.30 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.

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

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

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

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

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

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

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

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

6.6 Do módulo de EDR

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

6.6.2 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.

6.6.3 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.

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

6.6.5 Deve apresentar informações detalhadas contendo:
a) Usuário que executou a ação;
b) Informações acesso privilegiado.

6.6.6 A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.

6.6.7 A solução proposta deve suportar integração com serviço de reputação em nuvem.

6.6.8 A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado. (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações, etc.)

6.6.9 O agente EDR deve ter integração com o aplicativo de proteção de endpoint(agente único).

6.6.10 Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas.

6.6.11 A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.

6.6.12 A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção.

6.6.13 A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.

6.6.14 A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.

6.6.15 A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.

6.6.16 A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.

6.6.17 A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas.

6.6.18 A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC.

6.6.19 A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.

6.6.20 A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:
a) Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque);
b) Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional;
c) Informações gerais sobre a detecção, incluindo modo de detecção;
d) Alterações no registro associadas à detecção;
e) Histórico da presença de arquivos no dispositivo;
f) Ações de resposta executadas pela aplicação.

6.6.21 O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc.

6.6.22 A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:
a) Processo;
b) Conexões de rede;
c) Alterações no registro;
d) Detalhes do download de objeto.

6.6.23 A solução proposta deve fornecer orientação de resposta (resposta guiada).

6.6.24 A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente.

6.6.25 A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:
a) Impedir a execução de objetos;
b) Isolamento de host;

c) Excluir objeto do host ou grupo de hosts;
d) Encerrar um processo no dispositivo;
e) Colocar um objeto em quarentena;
f) Execute a verificação do sistema;
g) Execução remota de programa/processo/comando;
h) Iniciar a varredura IoC para um grupo de hosts.

6.7 Requisitos para documentação da solução.

6.7.1 A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:
a) Ajuda on-line para administradores;
b) Ajuda on-line para melhores práticas de implementação;
c) Ajuda on-line para proteção de servidores de administração.

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

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

6.8 **SERVIÇOS DE CONSULTORIA E SUPORTE ESPECIALIZADO**

6.8.1. Serviços de Suporte Técnico Especializado e Consultoria para Plataforma Kaspersky, que deverão ser prestados através de Banco de Horas (120h):

6.8.1.1. A CONTRATADA prestará serviços de consultoria e suporte técnico especializado nas soluções Kaspersky implantadas na CONTRATANTE, com foco em proteção de endpoints e funcionalidades EDR.

6.8.1.2. Os serviços serão realizados por meio de um banco de 120(cento e vinte) horas técnicas, disponibilizadas ao longo da vigência contratual, mediante solicitação da CONTRATANTE.

6.8.2. Das condições de execução dos serviços:

6.8.2.1. As horas poderão ser utilizadas sob demanda, mediante solicitação formal da CONTRATANTE, via chamado telefônico ou e-mail, entre 9h e 18h, de segunda a sexta-feira (horário de Brasília);

6.8.2.2. Os serviços poderão ser executados remotamente;

6.8.2.3. O suporte incluirá:

6.8.2.3.1. Esclarecimento de dúvidas de utilização, administração e operação das soluções Kaspersky fornecidas;

6.8.2.3.2. Orientação sobre atualizações, correções e melhorias;

6.8.2.3.3. Envio de procedimentos e boas práticas para operação segura e eficiente da solução;

6.8.2.3.4. Apoio em incidentes e contenção de ameaças;

6.8.2.3.5. Auditoria, revisão e análise de logs.

6.8.3. Da abrangência dos serviços de consultoria:

6.8.3.1. Os serviços contemplam, entre outros:

6.8.3.1.1. Análise, planejamento e implantação de projetos relacionados a soluções antivírus, EDR e proteção em nuvem Kaspersky;

6.8.3.1.2. Auxílio na gestão de políticas de segurança, incluindo prevenção e combate a ameaças como vírus, spywares, ransomwares e rootkits;

6.8.3.1.3. Avaliação de vulnerabilidades e recomendações de mitigação;

6.8.3.1.4. Instalação e configuração de atualizações de versão e patches;

6.8.3.1.5. Parametrização de filtros, regras e mecanismos de bloqueio para ameaças sem vacina;

6.8.3.1.6. Apoio na análise de logs e investigação de eventos de segurança.

6.8.4. Das condições operacionais e SLA:

6.8.4.1. O suporte será prestado por equipe com certificação oficial Kaspersky;

6.8.4.2. O atendimento ocorrerá em regime 8x5 com tempos de resposta conforme prioridade: a) Conforme tabela de SLA no item 6.8.6.

6.8.5. Da gestão e controle do banco de horas:

6.8.5.1. A CONTRATADA enviará até o dia 10 de cada mês o extrato das horas utilizadas no mês anterior;

6.8.5.2. A CONTRATANTE terá até 5 (cinco) dias úteis para validar ou contestar os relatórios enviados;

6.8.5.3. A CONTRATADA poderá emitir Nota Fiscal somente após o aceite das horas executadas.

6.8.5.4. O pagamento das horas será efetuado no prazo máximo de até 30 (trinta) dias, podendo ser de forma integral ou parcelada, através de conta corrente da CONTRATADA, no banco e conta corrente por ela indicados pela contratada.

6.8.6. Disposições finais

6.8.6.1. Este serviço não substitui a implantação inicial das soluções já contempladas nos documentos técnicos de EDR Optimum;

6.8.6.2. O banco de horas é válido durante a vigência contratual e pode ser utilizado conforme necessidade da CONTRATANTE.

DUVIDA	SOLICITAÇÃO DE SERVIÇOS	INCIDENTE			
PADRÃO	PADRÃO	CRÍTICO	ALTO	MÉDIO	BAIX
Primeiro atendimento em até: 08 horas	Primeiro atendimento em até: 04 horas	Primeiro atendimento em até: 01 hora	Primeiro atendimento em até: 04 horas	Primeiro atendimento em até: 24 horas	Incidentes que cria operação da S
Tempo para resolução em até: 72 horas	Tempo para resolução em até: 48 horas	Tempo para solução ou contorno em até: 04 horas	Tempo para solução ou contorno em até: 08 horas	Primeiro atendimento em até: 24 horas	Incidentes que cria operação da S
Solicitações de dúvida sobre a plataforma ou sobre os serviços contratados.	Solicitações de novos serviços relacionado s ao produto contratado, como exemplo: Novas configurações, novos relatórios, novas parametrizações, entre outros.	Incidente crítico que paralise totalmente os serviços do ambiente de produção com impacto direto no negócio.	Incidente grave que prejudique a operação da solução ou limite severamente suas funcionalidades com a paralisação parcial do serviço.	Incidentes que criam restrições à operação da Solução.	Incidentes que cria operação da S

7. DA NECESSIDADE DE FORMALIZAÇÃO DE CONTRATO

7.1 Deverá ser formalizado contrato para os serviços previstos neste Estudo Técnico Preliminar (ETP), tendo em vista as características do objeto a ser contratado, com a existência de obrigações futuras, incluindo a garantia, continuidade e confiabilidade do mesmo.

7.2 Não é admitida a subcontratação do objeto contratual.

8. ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO

8.1 Atualmente, o Tribunal de Justiça do Estado do Amazonas (TJAM) utiliza aproximadamente 4.000 (quatro mil) licenças da solução de antivírus corporativo, quantidade necessária para atender à proteção das estações de trabalho, servidores e demais dispositivos computacionais em operação no ambiente institucional.

8.2 A estimativa atual considera o parque tecnológico existente, abrangendo equipamentos utilizados nas atividades administrativas e jurisdicionais, distribuídos entre a sede, fóruns, comarcas do interior e demais unidades vinculadas ao TJAM.

8.3 Considerando a expansão gradual do parque tecnológico do Tribunal, decorrente da ampliação de unidades administrativas, modernização de equipamentos, substituição de ativos obsoletos e eventual incremento de novos serviços e sistemas informatizados, projeta-se um crescimento na quantidade de dispositivos que necessitarão de proteção ao longo do período contratual.

8.4 Diante desse cenário, estima-se necessária a contratação de 5.000 (cinco mil) licenças da solução de antivírus, quantidade que contempla uma margem de crescimento planejada, permitindo absorver novas demandas sem a necessidade de aditivos contratuais ou novas contratações durante a vigência do contrato.

Item	Descrição	Unidade	Quantidade
01	Fornecimento de Licença de uso do software antivírus KASPERSKY NEXT EDR OPTIMUM, com suporte técnico, por 36 meses.	Unidade	5000
02	Serviços Especializados para SUPORTE TÉCNICO E CONSULTORIA	Horas	120

9. ESTIMATIVA DE PREÇOS

9.1.

Item	Descrição	Unidade	Quantidade	Valor Estimado Unitário	Valor Estimado Anual
1	Fornecimento de Licença de uso do software antivírus KASPERSKY NEXT EDR OPTIMUM, com suporte técnico, por 36 meses.	Unidade	5000	R$ 465,60	R$ 2.328.000,00
2	Serviços Especializados para SUPORTE TÉCNICO E CONSULTORIA	Hora	120	R$ 600,00	R$ 72.000,00
				TOTAL	**R$ 2.400.000,00**

10. JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DA CONTRATAÇÃO

10.1 Não se aplica, pois trata-se de um item único.

11. CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

11.1 A contratação proveniente deste ETP visa substituir o Contrato Administrativo 005/2023-FUNJEAM.

12. RESULTADOS PRETENDIDOS

12.1 Garantir a proteção contínua dos ativos de Tecnologia da Informação do Tribunal de Justiça do Estado do Amazonas (TJAM) contra ameaças cibernéticas, tais como vírus, malwares, ransomwares e demais códigos maliciosos, por meio da utilização de solução de antivírus corporativa atualizada e reconhecida no mercado.

12.2 Assegurar a manutenção da confidencialidade, integridade e disponibilidade das informações institucionais, reduzindo os riscos de vazamento de dados, indisponibilidade de sistemas e comprometimento de informações sensíveis.

12.3 Manter a continuidade e a estabilidade dos serviços informatizados utilizados nas atividades administrativas e jurisdicionais do TJAM, evitando interrupções decorrentes de incidentes de segurança da informação.

12.4 Proporcionar gerenciamento centralizado da segurança dos endpoints, permitindo maior controle, visibilidade e padronização das políticas de segurança aplicadas a estações de trabalho, servidores e demais dispositivos conectados à rede institucional.

12.5 Reduzir o impacto operacional e o tempo de resposta a incidentes de segurança da informação, por meio de mecanismos avançados de detecção, resposta e mitigação de ameaças, aliados ao suporte técnico especializado da solução contratada.

12.6 Minimizar custos operacionais e riscos associados à ocorrência de incidentes de segurança, evitando gastos extraordinários com recuperação de sistemas, restauração de dados e mitigação de danos decorrentes de ataques cibernéticos.

12.7 Garantir a conformidade do ambiente tecnológico do TJAM com as melhores práticas de segurança da informação e com as diretrizes institucionais, contribuindo para o atendimento às normas internas, à legislação vigente e às recomendações dos órgãos de controle.

12.8 Preservar a padronização tecnológica já adotada pelo Tribunal, reduzindo a complexidade da administração do ambiente de TI e a necessidade de capacitação adicional da equipe técnica em soluções distintas.

13. PROVIDÊNCIAS PARA ADEQUAÇÃO DO AMBIENTE DO ÓRGÃO

13.1 O objeto deste ETP não enseja nenhuma adequação no ambiente.

14. IMPACTOS AMBIENTAIS

14.1 Aplicar, no que couber, a Resolução CNJ nº 400 de 16 de junho de 2021 que dispõe sobre a política de sustentabilidade no âmbito do Poder Judiciário.

15. SERVIÇOS DE MANUTENÇÃO E ASSISTÊNCIA TÉCNICA

15.1 Os Serviços de Manutenção e Suporte Técnicos estão evidenciados no Item 6.8

16. DECLARAÇÃO DE VIABILIDADE (OU NÃO) DA CONTRATAÇÃO

16.1 Considerando todo o exposto, a Secretaria de Tecnologia da Informação e Comunicação (SETIC), por meio da Divisão de Infraestrutura de TIC (SETIC/DVITIC), declara que a contratação de uma solução de proteção de endpoints contra softwares maliciosos é viável e indispensável para garantir a segurança, a integridade e a disponibilidade dos serviços jurisdicionais e administrativos essenciais do TJAM.

17. OBRIGAÇÕES PERTINENTES À LEI GERAL DE PROTEÇÃO DE DADOS

17.1 O objeto desta pretensa contratação, por si só, não está diretamente vinculada à Lei Geral de Proteção de Dados (LGPD). Portanto, esta aquisição não exige cláusulas específicas de proteção de dados.

18. MAPEAMENTO DE RISCOS

FASE: ESTUDO TÉCNICO PRELIMINAR												
ID	**CAUSA (DEVIDO A)**	**EVENTO (PODERÁ OCORRER)**	**CONSEQUÊNCIA (O QUE PODERÁ LEVAR A)**	**PROB.**	**IMPACTO**	**NÍVEL**	**RESPOSTA**	**MEDIDAS PREVENTIVAS (PARA EVITAR QUE OCORRA)**	**MEDIDAS DE CONTINGÊNCIA (SE OCORRER, O QUE DEVE SER FEITO)**	**RESPONSÁVEL**	**PRAZO**	**MONITORAMENTO**
R1	Falta de alinhamento entre a necessidade e o escopo técnico do ETP	Elaboração de requisitos técnicos incompletos ou divergentes	Atrasos na contratação e necessidade de revisão do ETP	3	4	Alto	Revisar constantemente os requisitos	Reuniões de alinhamento entre a SETIC e as unidades demandantes	Ajustar rapidamente os requisitos técnicos	SETIC	Durante a elaboração do ETP	Acompanhamento das atas de reunião e validações
R2	Subestimação dos custos e da abrangência da solução	Estimativas de valores abaixo dos preços praticados no mercado	Restrição orçamentária e necessidade de revisão do estudo técnico	2	4	Moderado	Revisão detalhada das estimativas de custo	Pesquisa de preços de mercado atualizada e ampla	Readequar o escopo e as estimativas orçamentárias	SETIC	Durante a elaboração do ETP	Revisão contínua das informações de mercado
R3	Incompleta identificação das necessidades institucionais	Definição inadequada do objeto da contratação	Necessidade de reabertura do processo ou revisão do ETP	1	4	Baixo	Revisão da descrição das necessidades	Consulta ampla às áreas usuárias e análise do planejamento estratégico	Ajustar o objeto da contratação antes da conclusão do ETP	SETIC	Durante a elaboração do ETP	Validação da necessidade com os gestores

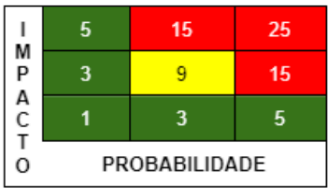
NÍVEL DE RISCO

Alto: Obrigatoriedade de tratamento do risco por meio de ação, monitoramento, e controle efetivo.

Moderado: Recomendável o tratamento do risco por meio de ação, monitoramento, e controle.

Baixo: Não há obrigatoriedade de tratamento do risco, cabendo uma reavaliação no ciclo posterior e/ou decisão da alta direção do TJAM quanto à emissão de ação, após a análise do tema em questão.

Baixo	Menor e/ou igual a 5.
Moderado	Entre 6 e 9.
Alto	Maior que 9.



Manaus- AM, data registrada no sistema.

Rafael Araújo da Silva	**Diogo Mendonça de Sousa**	**Breno Figueiredo Corado**
Fiscal Técnico do Contrato Administrativo 005/2023-FUNJEAM SETIC/DVITIC	Diretor da Divisão de Infraestrutura de TIC SETIC/DVITIC	Secretário de Tecnologia da Informação e Comunicação SETIC

Documento assinado eletronicamente por **Rafael Araújo da Silva**, **Servidor**, em 04/03/2026, às 14:31, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **DIOGO MENDONCA DE SOUSA**, **Diretor(a)**, em 04/03/2026, às 14:35, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **BRENO FIGUEIREDO CORADO**, **Secretário(a)**, em 04/03/2026, às 15:23, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjam.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2735870** e o código CRC **5975A851**.

TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
Av. André Araújo, S/N - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tjam.jus.br

MAPA DE PREÇOS

ITEM	SERVIÇO	UND.	QUANT.	VALOR UNITÁRIO ESTIMADO		MÉDIA	DESVIO PADRÃO	LIMITE INFERIOR	LIMITE SUPERIOR	VALOR UNITÁRIO ESTIMADO A LICITAR	VALOR ANUAL ESTIMADO A LICITAR - TOTAL	VALOR ESTIMADO PARA 36 MESES	METODOLOGIA DE CÁLCULO APLICADA
1	Fornecimento de Licença de uso do software antivírus KASPERSKY NEXT EDR OPTIMUM, com suporte técnico, por 36 meses.	Unidade	5.000	FORNECEDOR 01 - ARP 22026 TJMA - NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA; CNPJ: 05.250.796/0001-54	R$ 323,00	R$ 461,90	R$ 240,78	R$ 221,12	R$ 702,68	R$ 372,08	R$ 1.860.400,00	R$ 5.581.200,00	DESVIO PADRÃO
				FORNECEDOR 02 - CT 039/2025 - TJRN - NETWORK SECURE SEGURANCA DA INFORMAÇÃO LTDA; CNPJ: 05.250.796/0001-54	R$ 226,00								
				FORNECEDOR 03 - ARP 002/2025 - FUNARTE - 4FSOLUÇÕES EM TECNOLOGIA LTDA; 30.357.688/0001-22	R$ 358,00								
				FORNECEDOR 04	R$ 445,00								
				FORNECEDOR 05	R$ 508,42								
				FORNECEDOR 06	R$ 911,00								
2	Serviços Especializados para SUPORTE TÉCNICO E CONSULTORIA	Hora	120	FORNECEDOR 04	R$ 490,00	R$ 706,33	R$ 349,04	R$ 357,29	R$ 1.055,37	R$ 505,00	R$ 60.600,00	R$ 181.800,00	DESVIO PADRÃO
				FORNECEDOR 05	R$ 520,00								
				FORNECEDOR 06	R$ 1.109,00								
										TOTAL ESTIMADO	**R$ 1.921.000,00**	**R$ 5.763.000,00**	

OBS: OS VALORES ESTIMADOS FORAM PROVENIENTES DE PESQUISA DE MERCADO COM FORNECEDORES ESPECIALIZADOS E PREÇOS PÚBLICOS COM CONTRATAÇÕES SEMELHANTES REALIZADAS POR ESTE TRIBUNAL, SENDO APLICADO NO CÁLCULO O DESVIO PADRÃO DAS AMOSTRAS DOS PREÇOS OBTIDOS, CAPÍTULO III, ART. 4 º RESOLUÇÃO N. 064/2023-TJAM.

FORNECEDOR 1: ARP 22026 TJMA - NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA; CNPJ: 05.250.796/0001-54

FORNECEDOR 02: CT 039/2025 - TJRN - NETWORK SECURE SEGURANCA DA INFORMAÇÃO LTDA; CNPJ: 05.250.796/0001-54

FORNECEDOR 03: ARP 002/2025 - FUNARTE - 4FSOLUÇÕES EM TECNOLOGIA LTDA; CNPJ: 30.357.688/0001-22

FORNECEDOR 04: IP TRUST ADVANCE TECNOLOGIA DA INFORMAÇÃO LTDA; CNPJ: 18.753.084/0001-18

FORNECEDOR 05: QUALITEK TECNOLIGIA LTDA CNPJ: 10.224.281/0001-10

FORNECEDOR 06: XP ON CONSULTORIA LTDACNPJ: 23.518.065/0001-29

Hélida Valéria Muneymne Telles de Souza
Chefe Seção Cotações e Compras
Thiago Lima dos Santos
Divisão de Compras e Operações

Documento assinado eletronicamente por **THIAGO LIMA DOS SANTOS**, **Servidor**, em 14/04/2026, às 10:06, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **HELIDA VALERIA MUNEYMNE TELLES DE SOUZA**, **Chefe de Setor**, em 14/04/2026, às 10:35, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjam.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2826847** e o código CRC **1E05F536**.

TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
Av. André Araújo, S/N - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tjam.jus.br
CONTRATO - SECOP/DVCC/ATJ

*** MINUTA DE DOCUMENTO**

PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
DIVISÃO DE CONTRATOS E CONVÊNIOS

CONTRATO ADMINISTRATIVO Nº ___/20__-FUNJEAM

CONTRATO ADMINISTRATIVO Nº ___/20__-FUNJEAM, que entre si celebram o **TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS,** por intermédio do **FUNDO DE MODERNIZAÇÃO E REAPARELHAMENTO DO PODER JUDICIÁRIO ESTADUAL-FUNJEAM,** e a empresa _____, na forma abaixo.

O **TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS**, por intermédio do **FUNDO DE MODERNIZAÇÃO E REAPARELHAMENTO DO PODER JUDICIÁRIO ESTADUAL-FUNJEAM**, sediado na Cidade de Manaus, Estado do Amazonas, à Avenida André Araújo, s/nº, Aleixo, inscrito no CNPJ/MF sob nº 04.301.769/0001-09, neste ato representado por seu Presidente, Desembargador **JOMAR RICARDO SAUNDERS FERNANDES**, neste instrumento simplesmente denominado **CONTRATANTE**, e do outro lado, a empresa XXXXXXXXXXXXXX, pessoa jurídica de direito privado, com seus atos constitutivos devidamente registrados na Junta Comercial do Estado XXXXXXX, em XX/XX/XXXX, sob o nº XXX, inscrita no CNPJ/MF sob nº XXXXXXX, estabelecida na Cidade de XXXXXXX, Estado XXXXXXX, à XXXXXXX, neste ato representada pelo(a) Sr(a). XXXXXXX, daqui por diante simplesmente denominada **CONTRATADA**, em consequência da licitação na modalidade XXXXXXXX, sob o nº XXX/2026-COLIC/TJAM, cuja homologação foi publicada no Diário da Justiça Eletrônico, Ano XXX, Edição nº XXX, Caderno Administrativo, em XX/XX/XXXX, à pág. XX, tendo em vista o que consta do Processo Administrativo Digital nº 2026/000002456-00, doravante referido apenas por **PROCESSO**, celebram, na presença das testemunhas adiante nominadas, o presente **CONTRATO ADMINISTRATIVO Nº XXXX/2026- FUNJEAM**, que se regerá pelas normas instituídas pela Lei 14.133/21 e suas alterações, bem como pela Resolução nº 64/2023 TJAM, ou a norma que a substituir, que a regulamenta, pelas cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a contratação de serviço de **licença de uso de software de segurança de endpoint**, tipo Endpoint Detection and Response (EDR), para 5.000 (cinco mil) ativos, incluindo suporte técnico especializado e um banco de 120 (cento e vinte) horas de consultoria, nas condições estabelecidas no Termo de Referência.

1.2. Objeto da contratação:

ITEM	OBJETO	UND.	QUANT.	VALOR UNITÁRIO	VALOR TOTAL ANUAL	VALOR TOTAL GLOBAL
1	Fornecimento de Licença de uso do software antivírus KASPERSKY NEXT EDR OPTIMUM, com suporte técnico, por 36 meses.	unidade	5000			
2	Serviços Especializados para SUPORTE TÉCNICO E CONSULTORIA	hora	120			

1.3. Vinculam esta contratação, independentemente de transcrição, o Termo de Referência, o Edital da Licitação, a Proposta da **CONTRATADA** e os eventuais anexos destes documentos.

1.4. Estão inclusos no objeto desta contratação todo o aparato necessário à execução do objeto contratual, como o fornecimento de materiais, mão de obra, acessórios e insumos inerentes à sua execução, observando-se tipo, especificações, quantidades e condições descritas no Termo de Referência.

1.5. O regime de execução é o de empreitada por preço unitário.

CLÁUSULA SEGUNDA – LEGISLAÇÃO APLICÁVEL

2.1. O presente Contrato rege-se por toda a legislação aplicável à espécie e ainda pelas disposições que a complementarem, alterarem ou regulamentarem, cujas normas, desde já, entendem-se como integrantes do presente Termo, especialmente às normas constantes da Lei 14.133/21, a Resolução nº 64/2023 deste Tribunal de Justiça, ou outra que vier a substituí-la, e demais normas legais pertinentes.

2.2. A **CONTRATADA** declara conhecer todas essas normas e concorda em se sujeitar às estipulações, sistemas de penalidades e demais regras delas constantes, mesmo que não expressamente transcritas no presente instrumento.

CLÁUSULA TERCEIRA – VIGÊNCIA E PRORROGAÇÃO

3.1. O prazo de vigência da contratação é de **36 (trinta e seis) meses**, contados da lavratura deste contrato, na forma do art. 105 da Lei 14.133/21.

3.2. O prazo de vigência será automaticamente prorrogado, independentemente de termo aditivo, quando o objeto não for concluído no período firmado acima, ressalvadas as providências cabíveis no caso de culpa do contratado, previstas neste instrumento, conforme art. 111 da Lei 14.133/21.

3.3. É vedada a manutenção, aditamento ou prorrogação de contrato de prestação de serviços com empresa que 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 membros ou juízes vinculados ao **CONTRATANTE**, nos termos do art. 3.º da Resolução CNJ n.º 07/2005

CLÁUSULA QUARTA – PREÇO

4.1. O valor estimado anual da contratação é de R$ XXXXX,XX (XXXXXX), perfazendo o valor estimado global de R$ XXXXX,XX (XXXXXX).

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

4.3. No interesse da **CONTRATANTE** o valor deste Contrato poderá ser aumentado ou suprimido até o limite de 25% (vinte e cinco por cento), conforme disposto no artigo 125 da Lei nº 14.133/2021.

4.4. A **CONTRATADA** fica obrigada a aceitar, nas mesmas condições, os acréscimos e supressões que se fizerem necessários, até o limite ora previsto, não podendo os mesmos excederem o limite estabelecido no parágrafo anterior.

4.5. O valor acima é meramente estimativo, de forma que os pagamentos devidos ao contratado dependerão dos quantitativos efetivamente fornecidos.

CLÁUSULA QUINTA – MODELO DE EXECUÇÃO, MODELO DE GESTÃO CONTRATUAL E REEQUILÍBRIO ECONÔMICO-FINANCEIRO

5.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

5.2. O objeto contratual deverá ser executado no prazo de vigência do Contrato, conforme Termo de Referência.

5.3. Fica estabelecida a comunicação, preferencialmente, formal, eletrônica e escrita entre as partes, devendo a **CONTRATANTE**, sempre que comunicar/notificar a parte **CONTRATADA**, indicar prazo para acusação de recebimento do documento.

5.4 Transcorrido o prazo indicado no parágrafo anterior, presumir-se-á comunicada/notificada a **CONTRATADA** para todos os efeitos jurídicos.

5.5. A recomposição do equilíbrio econômico financeiro do contrato, além de obedecer aos requisitos previstos na Lei Federal nº 14.133/2021, será proporcional ao desequilíbrio efetivamente suportado, cuja existência e extensão deverão ser comprovados pela **CONTRATADA** ou pelo **CONTRATANTE**, conforme o caso, e darão ensejo à alteração do valor do contrato para mais ou para menos, respectivamente.

5.6. O pleito da recomposição do equilíbrio econômico-financeiro não será acolhido quando a parte interessada falhar em comprovar os requisitos previstos no item anterior, em especial nas seguintes hipóteses:
5.6.1. A efetiva elevação dos encargos não resultar em onerosidade excessiva ou não restar comprovada e quantificada por memória de cálculo a ser apresentada pela parte interessada;
5.6.2. O evento que houver dado causa ao desequilíbrio houver ocorrido em data anterior à entrega de proposta ou posterior à expiração da vigência do contrato;
5.6.3. Não for comprovado o nexo de causalidade entre o evento e a majoração dos encargos suportados pela parte interessada;
5.6.4. A parte interessada houver, direta ou indiretamente, contribuído para a majoração de seus próprios encargos, seja pela previsibilidade do evento, seja pela possibilidade de evitar a sua ocorrência;
5.6.5. A elevação dos encargos decorrer exclusivamente de variação inflacionária, hipótese já contemplada nos critérios de reajuste previstos neste instrumento.

5.7. Havendo a revisão contratual em razão da recomposição do equilíbrio econômico-financeiro, a formalização será realizada por meio de Termo Aditivo.

CLÁUSULA SEXTA – REAJUSTAMENTO

6.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, conforme art. 92, §3º, da Lei 14.133/2021.

6.2. Após o interregno de um ano, desde que haja pedido da **CONTRATADA**, os preços iniciais serão **reajustados**, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI, ocorrida nos últimos 12 (doze) meses, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

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

6.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

6.5. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

6.6. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

6.7. O reajuste poderá ser realizado por apostilamento.

CLÁUSULA SÉTIMA – RECEBIMENTO

7.1. Os **serviços** serão **recebidos provisoriamente**, no prazo de 05 (cinco) dias, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico, conforme Termo de Referência.

7.1.1. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda da **CONTRATADA** com a comprovação da prestação dos serviços a que se refere a parcela a ser paga.

7.2. A **CONTRATADA** fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

7.2.1. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

7.2.2. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

7.3. Os serviços serão **recebidos definitivamente** no prazo de 15 (quinze) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado.

7.4. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

7.5. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pela **CONTRATADA**, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

7.6. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

CLÁUSULA OITAVA - PAGAMENTO E DO ÍNDICE DE MEDIÇÃO DE RESULTADO (IMR)

8.1. O pagamento será efetuado **mensalmente** à **CONTRATADA**, em até 30 (trinta) dias, mediante apresentação da Nota Fiscal/Fatura, pelos serviços efetivamente prestados, após ser devidamente atestada a sua conformidade pelo Fiscal designado para acompanhar e fiscalizar a execução contratual.

8.2. O pagamento será efetuado por meio de **Ordem Bancária Eletrônica** em conta corrente indicada na Nota Fiscal/Fatura, devendo, para isso, ficar explícito o nome do banco, agência, localidade e número da conta corrente em que deverá ser efetivado o crédito.

8.3. Caso a **CONTRATADA** seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES, a mesma deverá apresentar, juntamente com a Nota Fiscal/Fatura, a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor.

8.4. Para a efetivação do pagamento deverão ser mantidas as mesmas condições iniciais de habilitação, cumpridos os seguintes requisitos: Comprovação da **regularidade fiscal** da **CONTRATADA** para com a **Fazenda Federal**, **Estadual** e **Municipal**; Comprovação da **regularidade fiscal** da **CONTRATADA** relativa à **Seguridade Social** e ao **Fundo de Garantia por Tempo de Serviço (FGTS)**, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei; Comprovação de **inexistência de débitos inadimplidos perante a Justiça do Trabalho**, mediante a apresentação de **Certidão Negativa de Débitos Trabalhistas (CNDT)**; Comprovação de regularidade junto ao Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis); e o Cadastro Nacional de Empresas Punidas (Cnep).

8.5. A **CONTRATADA** deverá encaminhar ao **CONTRATANTE**, através do e-mail contratos@tjam.jus.br: a Nota Fiscal/Fatura acompanhada dos documentos previstos nesta Cláusula, bem como das certidões que comprovem a regularidade fiscal da **CONTRATADA, relatórios técnicos e fotográficos que comprovem a execução do objeto, se for o caso,** a fim de que sejam adotadas as medidas inerentes ao pagamento.

8.6. A Nota Fiscal/Fatura correspondente será examinada diretamente pelo Fiscal designado pela **CONTRATANTE**, o qual somente atestará a prestação do serviço contratado e liberará a referida Nota Fiscal/Fatura para pagamento quando cumpridas, pela **CONTRATADA**, todas as condições pactuadas.

8.6.1 Em nenhuma hipótese será efetuado pagamento de Nota Fiscal/Fatura com o número do CNPJ/MF diferente do que foi apresentado na proposta de preços, mesmo que sejam empresas consideradas matriz e filial ou vice versa, ou pertencentes ao mesmo grupo ou conglomerado.

8.7. Havendo erro na Nota Fiscal/Fatura ou circunstância que impeça a liquidação da despesa, aquela será devolvida pelo Fiscal à **CONTRATADA** e o pagamento ficará pendente até que a mesma providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento será interrompido e reiniciado a partir da regularização da situação ou reapresentação do documento fiscal, não acarretando qualquer ônus para o **CONTRATANTE**.

8.8. A não disponibilização das informações e/ou documentos exigidos nesta cláusula caracteriza descumprimento de cláusula contratual, sujeitando a **CONTRATADA** à aplicação de penalidade(s) prevista(s) neste contrato.

8.9. O **CONTRATANTE** pode deduzir do montante a pagar os valores correspondentes a multas ou indenizações devidas pela **CONTRATADA**, nos termos deste contrato.

8.10. Ocorrendo atraso no pagamento, e desde que para tal não tenha concorrido de alguma forma a **CONTRATADA**, **haverá incidência de atualização monetária sobre o valor devido, pela variação acumulada do Índice de Preço ao Consumidor Amplo (IPCA)**, publicado pelo Instituto Brasileiro de Geografia e Estatística – IBGE, ocorrida entre a data final prevista para o pagamento e a data de sua efetiva realização.

CLÁUSULA NONA - DOTAÇÃO ORÇAMENTÁRIA

9.1. As despesas com a prestação de serviços do presente Contrato serão custeadas, no exercício em curso, por conta do Programa de Trabalho _____, Elemento de Despesa _____, Fonte de Recurso _____, Unidade Orçamentária _____ (_____), **Nota de Empenho _____**, de __/__/_____, no valor de **R$ _____ (_____)**.

CLÁUSULA DÉCIMA - OBRIGAÇÕES DAS PARTES

10.1. São obrigações da **CONTRATANTE**:

a)Exigir o cumprimento de todas as obrigações assumidas pela **CONTRATADA**, de acordo com o contrato e seus anexos;

b)Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

c)Notificar a **CONTRATADA**, por escrito, sobre vícios, defeitos ou incorreções verificadas na execução do objeto, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas, fixando prazo para a sua correção, certificando-se de que as soluções por ele propostas sejam as mais adequadas;

d)Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pela **CONTRATADA**;

e)Efetuar o pagamento à **CONTRATADA** do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e seus anexos;

f)Aplicar à **CONTRATADA** as sanções previstas na lei e neste Contrato;

g)Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste, no prazo de 30 dias, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período;

h)Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 30 dias, admitida a prorrogação motivada, por igual período;

i)Prestar esclarecimentos e fornecer por escrito as informações necessárias para a execução do objeto do contrato.

j)Não responder por quaisquer compromissos assumidos pela **CONTRATADA** com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do **CONTRATADO**, de seus empregados, prepostos ou subordinados;

k)Rejeitar, no todo ou em parte, serviço ou fornecimento executado em desacordo com este contrato e com o Termo de Referência;

10.2. São obrigações da **CONTRATADA**:

a)A **CONTRATADA** deve cumprir todas as obrigações constantes deste Contrato e em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

b)Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior e prestar todo esclarecimento ou informação solicitadas;

c)Informar imediatamente à **CONTRATANTE** qualquer ocorrência anormal, acidentes, condições inadequadas, quaisquer atos ou fatos que possam ser causa de prejuízos ou transtornos à perfeita execução do objeto;

d)Comunicar, por escrito, eventual atraso ou interrupção da execução do objeto, apresentando razões justificadoras que serão objeto de apreciação pelo **CONTRATANTE**, sem prejuízo das eventuais sanções cabíveis;

e)Prestar todas as informações e esclarecimentos solicitadas pela **CONTRATANTE** no prazo por ela estabelecido, inclusive, facilitando a ação da Fiscalização na inspeção da execução dos serviços, quando for o caso, em qualquer dia ou hora;

f)Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os bens e/ou serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

g)Efetuar comunicação ao **CONTRATANTE**, assim que tiver ciência da impossibilidade de entrega do bem ou realização/finalização do serviço no prazo estabelecido, para adoção de ações de contingência cabíveis;

h)Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo **CONTRATANTE**, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos, consoante art. 120 da Lei 14.133/2021;

i)Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas, previdenciárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao contratante e não poderá onerar o objeto do contrato, consoante art. 121 da Lei 14.133/2021;

j)Responsabilizar-se, integral e exclusivamente, pelas obrigações com mão de obra, materiais, transporte, refeições, uniformes, ferramentas, equipamentos, encargos sociais, trabalhistas, previdenciários, fiscais, cíveis e criminais, resultantes da execução do Contrato, inclusive no tocante aos seus empregados, dirigentes e prepostos;

k)Apresentar, sempre que solicitado, as seguintes informações e/ou os documentos listados: **Nota Fiscal/Fatura**; Comprovação da **regularidade fiscal** da **CONTRATADA** para com a **Fazenda Federal**, **Estadual** e **Municipal**; Comprovação da **regularidade fiscal** da **CONTRATADA** relativa à **Seguridade Social** e ao **Fundo de Garantia por Tempo de Serviço (FGTS)**, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei; Comprovação de **inexistência de débitos inadimplidos perante a Justiça do Trabalho**, mediante a apresentação de **Certidão Negativa de Débitos Trabalhistas (CNDT)**; Comprovação de regularidade junto ao **Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e o Cadastro Nacional de Empresas Punidas (Cnep);**

l)Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

m)Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz, conforme art. 116, da Lei n.º 14.133, de 2021;

n)Cumprir a reserva de cargos para menores aprendizes, nos termos do art. 92, XVII da Lei 14.133/2021, do art. 429 do Decreto-Lei nº 5.452/1943, da Resolução 64/2023 deste Tribunal de Justiça do Amazonas ou daquelas normas que vierem a substituí-las. O seu descumprimento poderá resultar nas sanções previstas nos normativos citados e neste Contrato Administrativo;

o)Cumprir a reserva de cargos para reabilitados da previdência social, nos termos do art. 92, XVII da Lei 14.133/2021, do art. 93 da Lei nº 8.213/91, da Resolução 64/2023 deste Tribunal de Justiça do Amazonas ou daquelas normas que vierem a substituí-las. O seu descumprimento poderá resultar nas sanções previstas nos normativos citados e neste Contrato Administrativo;

p)No início da contratação, quando da eventual prorrogação contratual ou sempre que a **CONTRATANTE** entender necessário, o cumprimento das reservas de cargos para menores aprendizes e para reabilitados da previdência social serão verificadas com emissão de certidão eletrônica junto ao Ministério do Trabalho e Emprego ou, caso necessário, pelo envio de declaração da **CONTRATADA**;

q)Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

r)É expressamente vedada à **CONTRATADA** a veiculação de publicidade acerca da contratação, salvo se houver prévia autorização do **CONTRATANTE**;

s)Sempre que a natureza da execução do objeto exigir, esta Administração promoverá reunião inicial com participação obrigatória da **CONTRATADA** para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

t)Cumprir e atender às normas relativas à Política de Prevenção e Enfrentamento do Assédio Moral, do Assédio Sexual e da Discriminação, a fim de promover o trabalho digno, saudável, seguro e sustentável no âmbito do Poder Judiciário instituidas pela Resolução nº 518 de 31/08/2023 do Conselho Nacional de Justiça (CNJ);

u)Manter preposto aceito pela Administração para representá-lo na execução do contrato;

v)A indicação ou a manutenção do preposto da empresa poderá ser recusada por este Tribunal de Justiça do Amazonas, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade;

w)Informar contatos (e-mails, telefones e endereços de correspondência) do(s) preposto(s) técnico e administrativo, previamente aceito pela **CONTRATANTE** para representar a **CONTRATADA** sempre que for necessário;

x)Observar e cumprir todas as demais obrigações previstas no Termo de Referência não descritas nesta cláusula.

CLÁUSULA DÉCIMA PRIMEIRA - OBRIGAÇÕES PERTINENTES À LEI GERAL DE PROTEÇÃO DE DADOS

11.1. As cláusulas seguintes são aplicáveis ao tratamento de dados pessoais, conforme especificado no Termo de Referência.

11.2. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados), quanto a todos os dados pessoais a que tenham acesso em razão deste Contrato Administrativo, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

11.3. A **CONTRATADA** terá acesso aos dados pessoais que estão de posse da **CONTRATANTE** apenas para as finalidades definidas pela **CONTRATANTE**, conforme especificado no Termo de Referência.

11.4. A **CONTRATADA** deve tratar os dados pessoais que tiver acesso apenas de acordo com as instruções documentadas da **CONTRATANTE**, durante a vigência do contrato, e em conformidade com estas cláusulas, e que, na eventualidade, não conseguir seguir as instruções ou de não mais poder cumprir estas obrigações, por qualquer razão, deve oficiar de modo formal este fato imediatamente à **CONTRATANTE**, sob pena de rescisão do contrato que terá o direito de rescindir o contrato sem qualquer ônus, multa ou encargo.

11.5. É dever da **CONTRATADA** orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da Lei Geral de Proteção de Dados.

11.6. A **CONTRATADA** deverá exigir de suboperadores e subcontratados, se houver, o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

11.7. A **CONTRATADA** ao tomar conhecimento de que os dados pessoais que recebeu são imprecisos ou desatualizados, deve informar a **CONTRATANTE**, sem demora injustificada. Neste caso, o **CONTRATANTE** deve apoiar a **CONTRATADA** para apagar ou retificar os dados.

11.8. No caso de uma violação de dados pessoais relativos a dados pessoais tratados pela **CONTRATADA** sob este contrato, a **CONTRATADA** deve tomar as medidas apropriadas para lidar com a violação, incluindo medidas para mitigar seus efeitos adversos. A **CONTRATADA** também deve notificar a **CONTRATANTE** sem demora injustificada, e no prazo de 24 horas, logo após tomar conhecimento da violação. Esta notificação deve conter os detalhes de um ponto de contato, onde mais informações podem ser obtidas, uma descrição da natureza da violação (incluindo, sempre que possível, categorias e número aproximado de titulares de dados e registros de dados pessoais em questão), suas prováveis consequências e as medidas tomadas ou propostas para resolver a violação, incluindo, quando apropriado, medidas para mitigar seus possíveis efeitos adversos.

11.9. A **CONTRATADA** deve apoiar e auxiliar a **CONTRATANTE** para permitir que a mesma cumpra suas obrigações nos termos da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), em particular para notificar a Autoridade Nacional de Proteção de Dados – ANPD e os titulares de dados afetados, levando em consideração a natureza do tratamento e as informações disponíveis para a **CONTRATADA**.

11.10. As Partes concordam que, a **CONTRATADA** ou o **CONTRATANTE** que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo, e as demais hipóteses em relação a responsabilidade e ressarcimento de danos serão regidos pelos arts. 42 a 45 e seus incisos da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

11.11. O **CONTRATANTE** poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo a **CONTRATADA** atender prontamente eventuais pedidos de comprovação formulados, esclarecimentos e/ou informações, no prazo estipulado pela **CONTRATANTE**.

11.12. Ao encerrar as atividades que fazem tratamento de dados pessoais, a **CONTRATADA** deve, à escolha do **CONTRATANTE**, apagar ou devolver os Dados Pessoais em sua posse, e apagar as cópias existentes. O tratamento pela **CONTRATADA** deve ocorrer apenas pelo período especificado no Termo de Referência. Até que os dados sejam apagados ou devolvidos, a **CONTRATADA** continuará a garantir o cumprimento do contrato, sem óbice de realização de posterior auditoria pela **CONTRATANTE.**

11.13. Quando necessário, a **CONTRATANTE** exigirá a apresentação de evidência técnica documentada (relatórios, logs, hash, screenshots) que comprove a eliminação correta dos dados pessoais tratados pela **CONTRATADA**.

11.14 O tratamento incorreto de dados pessoais ou a inobservância desta cláusula poderá implicar nas sanções administrativas previstas neste Contrato Administrativo e nas legislações pertinentes.

CLÁUSULA DÉCIMA SEGUNDA - SUBCONTRATAÇÃO

12.1. Não será admitida a subcontratação do objeto contratual.

CLÁUSULA DÉCIMA TERCEIRA - GARANTIA DE EXECUÇÃO

13.1. A **CONTRATADA** deverá apresentar ao **CONTRATANTE**, em até 05 (cinco) dias úteis, contados da assinatura do contrato, comprovante de garantia, no valor correspondente a **5% (cinco por cento) do valor total do contrato**, cabendo-lhe optar por uma das modalidades de garantia prevista no art. 96, § 1º

da Lei n.º 14.133/2021.

13.2. A garantia deverá ser prestada com vigência de 03 (três) meses após o término da vigência do Contrato e será restituída automaticamente, ou por solicitação, **no prazo de até 60 (sessenta) dias contados do final da vigência do contrato ou da rescisão**, somente após comprovação de que a empresa pagou todas as verbas rescisórias trabalhistas decorrentes da contratação.

13.2.1. Caso a **CONTRATADA** não efetive o cumprimento das obrigações previstas no subitem anterior, **a garantia será utilizada para o pagamento dessas verbas trabalhistas diretamente pelo CONTRATANTE**.

13.3. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

13.3.1. Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

13.3.2. Multas moratórias e punitivas aplicadas pela Administração à contratada; e

13.3.3. Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo contratado, quando couber.

13.4. Quando a garantia for apresentada em dinheiro, ela será atualizada monetariamente, conforme os critérios estabelecidos pela instituição bancária em que for realizado o depósito.

13.5. Quando a opção da garantia for a modalidade de seguro-garantia, a apólice deverá conter cláusulas específicas, oferecendo cobertura para despesas com obrigações contratuais e riscos trabalhistas, bem como multas que tenham caráter punitivo e, ainda, deverá ser apresentada em no mínimo de 1 (um) mês, contado da data de homologação da licitação e anterior à assinatura do contrato conforme art. 96. §3º da Lei 14.133/2021.

13.6. Aditado o Contrato, prorrogado o prazo de sua vigência ou alterado o seu valor, fica a **CONTRATADA** obrigada a apresentar garantia complementar ou substituí-la, no mesmo percentual e modalidades constantes desta cláusula. Nesses casos, a garantia será liberada após a apresentação da nova garantia e da assinatura do termo aditivo ao Contrato.

13.7. Nas hipóteses em que a garantia for utilizada total ou parcialmente – como para corrigir quaisquer imperfeições na execução do objeto do contrato ou para reparar danos decorrentes da ação ou omissão da **CONTRATADA**, de seu preposto ou de quem em seu nome agir, ou ainda nos casos de multas aplicadas depois de esgotado o prazo recursal – a **CONTRATADA** deverá, no prazo de 03 (três) dias, recompor o valor total dessa garantia, sob pena de aplicação de penalidades previstas neste Contrato.

13.8. Além da garantia de que tratam os arts. 96 e seguintes da Lei nº 14.133/21, a presente contratação possui previsão de **garantia técnica** do serviço a ser fornecido, incluindo manutenção e assistência técnica, conforme condições estabelecidas no Termo de Referência.

13.9. A garantia de execução é independente de eventual garantia do produto prevista especificamente no Termo de Referência.

CLÁUSULA DÉCIMA QUARTA - ALTERAÇÕES CONTRATUAIS

14.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021, bem como pela Resolução nº 64/2023, ou outra que vier a substituí-la, e seu anexo VI deste Tribunal de Justiça do Amazonas.

14.2. 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.

CLÁUSULA DÉCIMA QUINTA - FISCALIZAÇÃO

15.1. A existência e a atuação da fiscalização pelo **CONTRATANTE** em nada restringem a responsabilidade, única, integral e exclusiva da **CONTRATADA**, no que concerne à execução do objeto do contrato.

15.2. Ficam reservados à Fiscalização o direito e a autoridade para resolver todo e qualquer caso singular, duvidoso ou omisso, não previstos neste Contrato, no Edital de Licitação e seus anexos, e em tudo mais que, de qualquer forma, se relacione direta ou indiretamente, com objeto em questão, podendo determinar o que for necessário à regularização das faltas ou defeitos observados.

15.3 As atribuições da Fiscalização são aquelas constantes na Resolução n° 64-TJAM de 05 de dezembro de 2023, ou outra que vier a substituí-la, e no Manual de Gestão e Fiscalização de Contratos.

15.4 Compete à fiscalização técnica além de outras atribuições:

a) Participação em reuniões iniciais, de trabalho e de conclusão da execução contratual;

b) Verificação da conformidade da entrega de material, execução de obra ou prestação de serviço com as especificações, valor unitário ou total, quantidade e prazos estabelecidos no contrato;

c) Registro de todas as ocorrências relacionadas à execução do contrato, indicando o necessário para regularização de falhas ou defeitos;

d) Monitoramento constante da qualidade dos serviços, intervindo para solicitar à contratada a correção de faltas, falhas e irregularidades identificadas, mediante envio de SEP - Solicitação de Esclarecimentos e Providências ou Notificação Contratual.

e) Registro e comunicação à Seção de Gestão Contratual das atividades realizadas e pendências observadas na execução do contrato;

f) Manifestação sobre solicitações da contratada para prorrogação da execução/entrega do objeto contratual, abordando interesse na continuidade, prejuízos ao Tribunal decorrentes de atrasos e justificativas para a prorrogação de prazos;

g) Elaboração e assinatura do termo de recebimento provisório, detalhando o cumprimento das exigências técnicas referentes a aquisições, obras ou serviços conforme as regras contratuais;

h) Análise, em conjunto com o fiscal administrativo, dos documentos apresentados para pagamento, submetendo-os ao Fiscal para ateste ou notificação da contratada para regularização de impropriedades;

i) Comunicação imediata à gestão contratual e à Assessoria Técnica de Fiscalização, sobre qualquer ocorrência ou incapacidade técnica da empresa contratada que possa prejudicar a execução nas datas estabelecidas;

j) Proposição à Seção de Gestão Contratual e à Assessoria Técnica de Fiscalização, em caso de descumprimento contratual, da aplicação de sanções à contratada, conforme as regras do ato convocatório e/ou contrato, seguindo os procedimentos estabelecidos na Resolução n° 64, de 05 de

dezembro de 2023, ou outra que vier a substituí-la;

k) Elaboração, quando necessário, de relatórios, laudos e pareceres referentes às atividades de fiscalização técnica da execução do contrato;

l) Realização de vistorias, atestando o cumprimento de orientações técnicas e indicações de segurança;

m) Assistência à Seção de Gestão Contratual com informações necessárias para elaborar o documento comprobatório da avaliação realizada na fiscalização do cumprimento de obrigações assumidas pelo contratado;

n) Execução de outras atribuições derivadas das cláusulas e especificidades contratuais.

CLÁUSULA DÉCIMA SEXTA - INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

16.1. O processamento e julgamento das infrações e sanções administrativas que incorrer a **CONTRATADA** tramitarão na forma de Processo Administrativo Sancionatório (PAS), consoante as normas previstas no Anexo VIII da Resolução 64/2023 deste Tribunal de Justiça do Amazonas, ou outra que vier a substituí-la.

16.2. Poderão ser aplicadas à **CONTRATADA** que incorrer nas infrações previstas neste Contrato as seguintes sanções:

a) **Advertência**;
b) **Impedimento de licitar e contratar**;
c) **Declaração de inidoneidade para licitar e contratar**;
d) **Multa** de 0,5% a 30% do valor do contrato.

16.3. Comete infração administrativa, nos termos dos artigos 155 e 156 da Lei nº 14.133, de 2021, a **CONTRATADA** que incorrer nas seguintes infrações, cabendo-a as respectivas sanções:

a) **Der causa à inexecução parcial do contrato**;
Sanções: Advertência **e/ou** Multa compensatória de 20% (vinte por cento) sobre o valor da parcela não cumprida, observando que o valor final apurado não poderá ser inferior a 0,5% do valor total do contrato.

b) **Der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo**;
Sanções: Impedimento de licitar/contratar **ou** Declaração de inidoneidade para licitar/contratar **e/ou** Multa compensatória de 20% (vinte por cento) sobre o valor da parcela não cumprida, observando que o valor final apurado não poderá ser inferior a 0,5% do valor total do contrato.

c) **Der causa à inexecução total do contrato;**
Sanções: Impedimento de licitar/contratar **ou** Declaração de inidoneidade para licitar/contratar **e/ou** Multa compensatória de 30% do valor do contrato.

d) **Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;**
Sanções: Impedimento de licitar/contratar **ou** Declaração de inidoneidade para licitar/contratar **e/ou** Multa compensatória.

e) **Apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;**
Sanções: Declaração de inidoneidade para licitar/contratar **e/ou** Multa compensatória.

f) **Praticar ato fraudulento na execução do contrato;**
Sanções: Declaração de inidoneidade para licitar/contratar **e/ou** Multa compensatória.

g) **Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;**
Sanções: Declaração de inidoneidade para licitar/contratar **e/ou** Multa compensatória.

h) **Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013;**
Sanções: Declaração de inidoneidade para licitar/contratar **e/ou** Multa compensatória.

i) **Inobservância dos prazos contratuais;**
Sanção: Multa moratória, nos percentuais previstos no art. 18 do Anexo VIII da Resolução 64/2023 deste Tribunal de Justiça do Amazonas, ou outra que vier a substituí-la.

f) **Inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia, quando houver previsão contratual de sua exigência.**
Sanção: Multa moratória, nos percentuais previstos no art. 18 do Anexo VIII da Resolução 64/2023 deste Tribunal de Justiça do Amazonas, ou outra que vier a substituí-la.

16.4. Na aplicação das sanções serão considerados, conforme o art. 156, §1º, da Lei nº 14.133, de 2021):

a) A natureza e a gravidade da infração cometida;
b) As peculiaridades do caso concreto;
c) As circunstâncias agravantes ou atenuantes;
d) Os danos que dela provierem para o Tribunal;
e) A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle;

16.5. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa à **CONTRATADA**, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

16.6. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, conforme art. 157, da Lei nº 14.133, de 2021.

16.7. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo **CONTRATANTE** à **CONTRATADA**, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente, conforme art. 156, §8º, da Lei nº 14.133, de 2021.

16.8. Excepcionalmente, *ad cautelam*, o **CONTRATANTE** poderá efetuar a retenção do valor presumido da multa, antes da instauração do regular procedimento administrativo. Nesta hipótese, instaurará o procedimento em até 30 (trinta) dias contados da retenção.

16.9. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia, conforme art. 160, da Lei nº 14.133, de 2021.

16.10. O **CONTRATANTE** deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal, conforme art. 161, da Lei nº 14.133, de 2021.

16.11. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

CLÁUSULA DÉCIMA SÉTIMA - EXTINÇÃO CONTRATUAL

17.1. O contrato se extingue quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado para tanto.

17.2. Se as obrigações não forem cumpridas no prazo estipulado, a vigência ficará prorrogada até a conclusão do objeto, caso em que deverá a Administração providenciar a readequação do cronograma fixado para o contrato.

17.3. Quando a não conclusão do contrato referida no item anterior decorrer de culpa da **CONTRATADA**:

17.3.1. ficará ela constituída em mora, sendo-lhe aplicáveis as respectivas sanções administrativas; e

17.3.2. poderá a Administração optar pela extinção do contrato e, nesse caso, adotará as medidas admitidas em lei para a continuidade da execução contratual.

17.4. O contrato pode ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

17.4.1. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

17.4.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a rescisão se não restringir sua capacidade de concluir o contrato.

17.4.2.1 Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

17.5. O termo de rescisão, sempre que possível, será precedido:

17.5.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

17.5.2. Relação dos pagamentos já efetuados e ainda devidos;

17.5.3. Indenizações e multas.

17.6. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, desde que o pedido ainda tenha ocorrido enquanto vigente a contratação, hipótese em que será concedida indenização por meio de termo indenizatório, conforme art. 131, *caput,* da Lei n.º 14.133, de 2021.

CLÁUSULA DÉCIMA OITAVA - CASOS OMISSOS

18.1. Os casos omissos serão decididos pelo **CONTRATANTE**, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis 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.

CLÁUSULA DÉCIMA NONA - PUBLICAÇÃO

19.1. Incumbirá ao **CONTRATANTE** a publicação do **instrumento contratual** no **Portal Nacional de Contratações Públicas (PNCP)**, na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo **sítio oficial na Internet (Portal Eletrônico do TJAM)**, em atenção ao art. 8º, §2º, da Lei n. 12.527, de 2011, sendo, ainda, facultativa a publicação do **extrato deste Contrato no Diário da Justiça Eletrônico**, conforme dispõe o art. 4º, da Lei nº 11.419, de 19 de dezembro de 2006.

CLÁUSULA VIGÉSIMA - OS MEIOS ALTERNATIVOS DE RESOLUÇÃO E PREVENÇÃO DE CONFLITOS

20.1. As partes submetem-se aos dispostos na Resolução 48/2024 do Tribunal de Justiça do Amazonas que regulamenta os meios alternativos de prevenção e solução de controvérsias no âmbito dos Contratos Administrativos deste Poder, bem como outras normas que vierem alterá-la ou substituí-la.

20.2. Na busca pela autocomposição, nas demandas originadas da execução dos contratos administrativos de competência do Poder Judiciário Amazonense, será utilizada a mediação como instrumento de solução adequada de controvérsias, para prevenir ou resolver todo o conflito, ou apenas parte dele que será conduzido pelo Comitê de Prevenção e Resolução Administrativa de Conflitos em matéria de Contratos Administrativos - CPRAC deste Tribunal de Justiça do Amazonas.

20.2.1 A autocomposição a que se refere o caput desta cláusula poderá ser adotada quanto a totalidade ou parcela de quaisquer direitos patrimoniais disponíveis no âmbito dos conflitos em matéria de contrato administrativo, **incluindo-se** as **questões relacionadas ao restabelecimento do equilíbrio econômico-financeiro do contrato**, ao i**nadimplemento de obrigações contratuais por quaisquer das partes**, ao **cálculo de indenizações**, ou, ainda, a **celebração de negócio jurídico processual no Processo Administrativo Sancionatório (PAS)**.

20.3. A solicitação de submissão de conflito ao CPRAC, iniciada por pessoa física ou jurídica interessada deverá ser encaminhada à Divisão de Contratos e Convênios, que instruirá o pedido com toda a documentação necessária à compreensão do caso e remeterá os autos à ao Desembargador Coordenador do Comitê para análise de admissibilidade.

20.4. As propostas, os documentos e as informações apresentados no âmbito do CPRAC serão confidenciais e não poderão ser utilizados pelas partes como meio de defesa e/ou prova em processo judicial.

CLÁUSULA VIGÉSIMA PRIMEIRA - FORO

21.1. Obriga-se a **CONTRATADA**, por si e seus sucessores, ao fiel cumprimento de todas as cláusulas e condições do presente Contrato e elege seu domicílio contratual, o da Comarca de Manaus, capital do Estado do Amazonas, para dirimir eventuais dúvidas originadas pelo presente Termo, com expressa renúncia a qualquer outro, por mais privilegiado que seja, consoante 92, §1º, da Lei 14.133 de 2021.

E assim, por estarem às partes justas e contratadas, foi lavrado o presente instrumento contratual, que lido e achado conforme pelas partes, vai por elas assinado para que produza todos os efeitos de Direito, na presença das testemunhas abaixo identificadas.

Desembargador(a) XXXXXXXX
Presidente do Tribunal de Justiça do Estado do Amazonas
CONTRATANTE

Sr. _____
Representante Legal da Empresa
CONTRATADA

TESTEMUNHAS:

Nome: _____ Nome: _____

Matrícula: _____ Matrícula: _____

Documento assinado eletronicamente por **Aldemir da Silva Menezes Medeiros**, **Diretor(a)**, em 24/04/2026, às 11:12, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjam.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2845913** e o código CRC **FBF3AACE**.