CONTRATO Nº 19.16.3901.0049402/2025-45

CONTRATO SIAD Nº 9470652

CONTRATO DE PRESTAÇÃO DE SERVIÇOS QUE ENTRE SI CELEBRAM O MINISTÉRIO PÚBLICO DO ESTADO DE MINAS GERAIS, POR INTERMÉDIO DA PROCURADORIA-GERAL DE JUSTIÇA, E BRASOFTWARE INFORMÁTICA LTDA., NA FORMA AJUSTADA.

CONTRATANTE: Ministério Público do Estado de Minas Gerais, por intermédio da **Procuradoria-Geral de Justiça**, com sede na Av. Álvares Cabral, nº 1690, bairro Santo Agostinho, nesta Capital, CEP 30.170-008, inscrita no CNPJ sob o nº 20.971.057/0001-45, neste ato representado pelo Procuradora-Geral de Justiça Adjunta Administrativa, **Iraídes de Oliveira Marques**.

CONTRATADO(A): Brasoftware Informática Ltda., inscrita no CNPJ sob o nº 57.142.978/0001-05, com sede na rua Marina La Regina, nº 227, 3º andar, salas 11 a 15, Centro, Poá/SP, CEP 08.550-210, neste ato representada por **Walter F. da S. Júnior**, inscrito no CPF sob o nº ***.434.428-**.

As partes acima qualificadas celebram o presente contrato, com observância ao **Processo SEI n.º 19.16.1937.0123734/2024-83**, nos termos da Lei Federal nº 14.133, de 1º de abril de 2021, da Resolução PGJ nº 02/2023, além das demais disposições legais aplicáveis e do disposto no Edital do Processo Licitatório SIAD nº 22/2025 devidamente adjudicado, homologado e publicado, na forma da Lei, observados os Anexos I e II (Anexos II e IV do Edital) e respectivas atas de abertura e julgamento, mediante as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA – Do Objeto

O objeto da presente licitação é a prestação de serviços de empresa especializada em tecnologia da informação para subscrição de licenciamento de solução de segurança e antivírus, conforme especificações, exigências e quantidades estabelecidas no Termo de Referência.

CLÁUSULA SEGUNDA – Da Vigência

O prazo de vigência do presente contrato é de 36 (trinta e seis) meses, contados a partir da data da publicação do instrumento, podendo ser prorrogado por meio de termos aditivos, desde que respeitada a vigência máxima decenal, com fulcro nos arts. 106 e 107, ambos da Lei Federal nº 14.133/21.

Subcláusula Primeira: A cada exercício, o Contratante atestará a existência de créditos orçamentários vinculados à contratação e a vantagem em sua manutenção.

Subcláusula Segunda: A prorrogação de que trata o caput desta cláusula será condicionada ao ateste, da autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o(a) Contratado(a).

CLÁUSULA TERCEIRA – Dos Modelos de Execução e Gestão Contratuais

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.

CLÁUSULA QUARTA – Das Obrigações do Contratante

São obrigações do Contratante, além de outras previstas neste contrato e no Termo de Referência (Anexo II):

4.1. Efetuar o pagamento dos valores devidos, no prazo e condições pactuadas;

4.2. Acompanhar e fiscalizar a execução contratual, por intermédio do responsável pelo(s) setor(es) constante(s) do Anexo II deste instrumento, indicado pelo respectivo Órgão/Entidade ou por servidor designado por este, que deverá anotar todas as ocorrências relacionadas à referida execução, determinando o que for necessário à regularização das falhas ou defeitos detectados, e comunicar, antes de expirada a vigência contratual, as irregularidades apuradas aos superiores e aos órgãos competentes, caso haja necessidade de imposição de sanções ou as medidas corretivas a serem adotadas estejam fora do seu âmbito de competência;

4.3. Comunicar ao(à) Contratado(a), por escrito, a respeito da supressão ou acréscimo contratuais mencionados neste instrumento, encaminhando o respectivo termo aditivo para ser assinado;

4.4. Decidir sobre eventuais alterações neste contrato, nos limites permitidos por lei, para melhor adequação de seu objeto;

4.5. 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;

4.5.1. Concluída a instrução do requerimento, a Administração terá o prazo de 60 (sessenta) dias para decidir, admitida a prorrogação motivada por igual período.

4.6. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo(a) Contratado(a) no prazo de 90 (noventa) dias, contados da conclusão da instrução do requerimento, admitida a prorrogação motivada por igual período;

4.7. Notificar os emitentes das garantias quanto ao início de processo administrativo de responsabilização de fornecedores (PARF) para apuração de descumprimento de cláusulas contratuais.

CLÁUSULA QUINTA – Das Obrigações do(a) Contratado(a)

São obrigações do(a) Contratado(a), além de outras previstas neste contrato e em seu Anexo II (Termo de Referência):

5.1. Fornecer o objeto em perfeito estado, e prestar o serviço pertinente, no prazo, local, quantidade, qualidade e condições estabelecidos, cumprindo fielmente todas as disposições constantes deste contrato e seu(s) anexo(s);

5.2. Arcar com todas as despesas pertinentes à execução do objeto ora contratado, tais como tributos, fretes, embalagens, custos com mobilização, quando for o caso, e também os salários, encargos previdenciários, trabalhistas e sociais relacionados à execução do objeto, bem como os demais custos e encargos inerentes a tal execução, mantendo em dia os seus recolhimentos;

5.3. Responder integralmente pelos danos causados diretamente ao Contratante ou a terceiros, por culpa ou dolo decorrentes da execução deste contrato, não havendo exclusão ou redução de responsabilidade decorrente da fiscalização ou do acompanhamento contratual exercido pelo Contratante;

5.4. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, Lei Federal nº 14.133/21,submetendo suas justificativas à apreciação do Contratante, para análise e deliberação a respeito de eventual necessidade de adequação contratual;

5.5. Comunicar ao Contratante, imediatamente e por escrito, qualquer alteração que possa comprometer a execução dos serviços ou a comunicação entre as partes;

5.6. Submeter à apreciação do Contratante, antes de expirado o prazo previsto para entrega do objeto contratado, solicitação de prorrogação, se assim entender necessário, demonstrada a ausência de culpa do(a) Contratado(a), sob pena de ser constituída em mora e demais sanções administrativas;

5.7. Manter, durante toda a vigência contratual, as mesmas condições de regularidade fiscal e de qualificação exigidas e apresentadas na fase de habilitação do processo licitatório e/ou assinatura do presente contrato, inclusive as relativas à regularidade para com o INSS, FGTS, Justiça do Trabalho, Fazenda Municipal, bem como à regularidade tributária perante a Fazenda de Minas Gerais e, quando for o caso, perante a Fazenda Estadual do domicílio do(a) Contratado(a), conservando atualizadas as informações no Cadastro Geral de Fornecedores – CAGEF e apresentando à Superintendência de Gestão Administrativa do Contratante as certidões referentes às condições supramencionadas sempre que tiverem suas validades vencidas e quando solicitadas;

5.8. Informar, no corpo da nota fiscal (ou documento equivalente), seus dados bancários, a fim de possibilitar ao Contratante a realização dos depósitos pertinentes;

5.9. Manter o sigilo sobre todos os dados, informações e documentos fornecidos por este Órgão ou obtidos em razão da execução contratual, sendo vedada toda e qualquer reprodução destes, durante a vigência deste contrato e mesmo após o seu término;

5.10. Comunicar ao Contratante quaisquer operações de reorganização empresarial, tais como fusão, cisão e incorporação, as quais, quando caracterizarem a frustração das regras disciplinadoras da licitação, poderão ensejar a rescisão contratual;

5.11. Comunicar à Secretaria da Receita Federal, nos termos do art. 30 da Lei Complementar Federal nº 123/06, o eventual desenquadramento da situação de microempresa, empresa de pequeno porte ou equiparada em decorrência da execução deste contrato, encaminhando cópia da comunicação ao Contratante, para ciência.

5.12 Cumprir, ao longo de toda a execução contratual, se aplicável, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas em outras normas específicas (art. 116 da Lei 14.133/2021).

5.12.1 Comprovar o cumprimento da reserva de cargos a que se refere o item 5.12, sempre que solicitado pela Administração, com a indicação dos empregados que preencherem as referidas vagas (art. 116, parágrafo único).

CLÁUSULA SEXTA – Da Proteção de Dados Pessoais

6.1. É dever das partes observar e cumprir as regras impostas pela Lei Geral de Proteção de Dados (Lei n.º 13.709/18), suas alterações e regulamentações posteriores, bem como as diretrizes estabelecidas pela Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no Ministério Público (Resolução n.º 281/2023, do Conselho Nacional do Ministério Público – CNMP), devendo ser observadas, no tratamento de dados, a respectiva finalidade específica e a consonância ao interesse público.

6.2. No presente contrato, o Contratante assume o papel de controlador, nos termos do artigo 5º, VI, da Lei n.º 13.709/2018, e o(a) Contratado(a) assume o papel de operador, nos termos do artigo 5º, VII, da Lei n.º 13.709/2018.

6.3. O(A) Contratado(a) deverá guardar sigilo sobre os dados pessoais compartilhados pelo Contratante e só poderá fazer uso dos dados exclusivamente para fins de cumprimento do objeto deste contrato, sendo-lhe vedado, a qualquer tempo, o compartilhamento desses dados sem a expressa autorização do Contratante, ou o tratamento dos dados de forma incompatível com as finalidades e prazos acordados, sob pena de responsabilização administrativa, civil e criminal.

6.4. É dever do(a) Contratado(a) orientar e treinar seus empregados e colaboradores sobre os deveres, requisitos e responsabilidades decorrentes das leis e regulamentos de proteção de dados pessoais.

6.5. O(A) Contratado(a) se compromete a adequar todos os procedimentos internos e adotar as medidas de

segurança técnicas, administrativas e operacionais necessárias a resguardar os dados pessoais que lhe serão confiados, levando em conta as diretrizes de órgãos reguladores, padrões técnicos e boas práticas existentes, incluindo as diretrizes da Resolução CNMP n.º 281/2023.

6.6. Quando solicitado, o(a) Contratado(a) fornecerá ao Contratante todas as informações necessárias para comprovar a sua conformidade com as obrigações referentes à proteção de dados pessoais, incluindo registros cronológicos ou outros métodos eficazes que demonstrem a licitude do tratamento e garantam a integridade e a segurança dos dados pessoais, devendo atender prontamente eventuais pedidos de comprovação formulados, respeitando-se o sigilo empresarial e as demais proteções legais.

6.7. O(A) Contratado(a) cooperará com o Contratante no cumprimento das obrigações referentes ao exercício dos direitos dos titulares previstos na LGPD e nas leis e regulamentos de proteção de dados em vigor e, também, no atendimento de requisições de autoridades competentes ou quaisquer outros legítimos interessados.

6.8. Os dados pessoais obtidos a partir do presente contrato serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, sendo permitida a conservação para as finalidades estabelecidas no artigo 16 da Lei n.º 13.709/2018.

6.9. O(A) Contratado(a) deverá comunicar ao Contratante, no prazo máximo de 72 (setenta e duas) horas, contados do seu conhecimento, qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Subcláusula Única: A comunicação mencionada no item 6.9 desta Cláusula deverá ser enviada para o e-mail: encarregado@mpmg.mp.br, devendo trazer em seu bojo, no mínimo, as seguintes informações:

I - a descrição e a natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, observados os casos de sigilo legal e institucional;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

CLÁUSULA SÉTIMA – Cláusula Declaratória e Compromissória Anticorrupção

7.1. O(A) Contratado(a) declara, por si e por seus administradores, funcionários, representantes e outras pessoas que agem em seu nome, direta ou indiretamente, estar ciente dos dispositivos contidos na Lei nº 12.846/2013.

7.2. O(A) Contratado(a) se obriga a tomar todas as providências para fazer com que seus administradores, funcionários e representantes tomem ciência quanto ao teor da mencionada Lei nº 12.846/2013.

Subcláusula Primeira: O(A) Contratado(a), no desempenho das atividades objeto deste contrato, compromete-se perante o Contratante a abster-se de praticar ato(s) que possa(m) constituir violação à legislação aplicável ao presente instrumento pactual, incluindo aqueles descritos na Lei nº 12.846/2013, em especial no seu artigo 5º.

Subcláusula Segunda: O(A) Contratado(a) se compromete a não contratar como empregados ou firmarem qualquer forma de relacionamento com pessoa física ou jurídica envolvida em atividades criminosas, em especial pessoas investigadas por ilícitos da Lei Anticorrupção, Lei de Improbidade Administrativa, de Lavagem de Dinheiro e delitos da legislação penal.

Subcláusula Terceira: O(A) Contratado(a) se obriga a notificar o Contratante, imediatamente e por escrito, sobre qualquer suspeita ou violação à legislação vigente, como casos em que tiver ciência acerca de prática de atos de suborno, corrupção ou fraudes em geral.

Subcláusula Quarta: O(A) Contratado(a) obriga-se a conduzir os seus negócios e práticas comerciais de forma ética e íntegra em conformidade com os preceitos legais vigentes no país.

Subcláusula Quinta: O descumprimento pelo(a) Contratado(a) das normas legais anticorrupção e das dispostas neste contrato será considerada infração grave e ensejará a possibilidade de rescisão do instrumento contratual pelo Contratante, sem qualquer ônus ou penalidade, respondendo o(a) Contratado(a), ainda, sobre eventuais perdas e danos.

CLÁUSULA OITAVA – Da Subcontratação

O(A) Contratado(a) não poderá subcontratar, ceder ou transferir, total ou parcialmente, o objeto deste ajuste.

CLÁUSULA NONA – Do Preço

O valor total da contratação é de **R$ 1.048.676,00** (um milhão, quarenta e oito mil, seiscentos e setenta e seis reais).

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

CLÁUSULA DÉCIMA – Da Dotação Orçamentária

As despesas com a execução deste instrumento correrão à conta da dotação orçamentária n° 1091.03.122.703.2009.0001.3.3.90.40.02.0 - Fonte 10.1, com os respectivos valores reservados, e suas equivalentes nos exercícios seguintes quando for o caso.

CLÁUSULA DÉCIMA PRIMEIRA – Da Forma de Pagamento

A forma de pagamento do objeto contratado e demais condições a ela referentes encontram-se definidos no Termo de Referência, anexo a este contrato.

CLÁUSULA DÉCIMA SEGUNDA – Do Reajuste

A periodicidade para o reajuste do objeto será de 12 (doze) meses, contados da data do orçamento estimado, em 31/01/2025, no caso de primeiro reajuste, ou da data do reajuste anterior, na hipótese de reajustes posteriores, com base no Índice Nacional de Preços ao Consumidor Amplo (IPCA-IBGE) ou em outro que venha substituí-lo.

Subcláusula Primeira: A concessão de reajuste será efetuada independentemente de pedido do(a) Contratado(a).

Subcláusula Segunda: A redução do valor do reajuste estabelecido no caput desta cláusula ou sua dispensa poderão ainda ser objeto de acordo entre as partes.

Subcláusula Terceira*:* Em regra, o reajuste será realizado por apostilamento.

CLÁUSULA DÉCIMA TERCEIRA – Do reequilíbrio econômico-financeiro

O reconhecimento de desequilíbrio econômico-financeiro dependerá de expresso requerimento da parte interessada, devendo ser formulado durante a vigência deste contrato e antes de eventual prorrogação, nos termos da alínea 4.6 da cláusula quarta deste instrumento.

Subcláusula Única: Uma vez preenchidos os requisitos do caput, a extinção do contrato não configurará óbice para o reconhecimento da situação de desequilíbrio, hipótese na qual será concedida indenização por meio de termo indenizatório.

CLÁUSULA DÉCIMA QUARTA – Das Alterações Contratuais

O(A) Contratado(a) fica obrigado(a) a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que o Contratante, a seu critério e de acordo com sua disponibilidade orçamentária e financeira, determinar, até o limite de 25% do valor inicial atualizado do contrato.

Subcláusula Primeira: O limite para acréscimo, nos termos do caput desta cláusula, será de 50% do valor inicial atualizado do contrato quando o objeto contratado consistir em reforma de edifício ou de equipamento, conforme art. 125 da Lei Federal nº 14.133/21.

Subcláusula Segunda: As demais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei Federal nº 14.133/21.

CLÁUSULA DÉCIMA QUINTA – Da Garantia do Objeto

A garantia será prestada de acordo com o estabelecido na Proposta e no Termo de Referência, independentemente do término da vigência contratual.

CLÁUSULA DÉCIMA SEXTA – Da Garantia de Execução Contratual

Não haverá exigência de garantia contratual da execução.

CLÁUSULA DÉCIMA SÉTIMA – Das Infrações e Sanções Administrativas

A inadimplência do(a) Contratado(a), sem justificativa aceita pelo Contratante, no cumprimento de qualquer cláusula ou condição prevista neste contrato, inclusive quando configurar o cometimento de infrações, a sujeitará às sanções discriminadas no Termo de Referência, anexo a este contrato, as quais serão aplicadas de acordo com a natureza e a gravidade da infração, as peculiaridades do caso concreto, as circunstâncias agravantes ou atenuantes, os danos que dela provierem para o Contratante, a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle, bem como eventual extinção unilateral do contrato, mediante processo administrativo de responsabilização de fornecedores (PARF), observada a aplicação da Lei Federal nº 14.133/2021 e da Resolução PGJ nº 02/2023.

CLÁUSULA DÉCIMA OITAVA – Da Extinção Contratual

18.1. 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 Federal nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

18.1.1. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

18.1.2. 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.

18.1.2.1. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

18.2. O termo de extinção, sempre que possível, será precedido de:

18.2.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

18.2.2. Relação dos pagamentos já efetuados e ainda devidos;

18.2.3. Indenizações e multas.

18.3. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, conforme Subcláusula Única da Cláusula Décima Terceira**.**

CLÁUSULA DÉCIMA NONA – Da Publicação

O Contratante fará publicar no Diário Oficial Eletrônico do Ministério Público de Minas Gerais – DOMP/MG e no Portal Nacional de Contratações Públicas, bem como no respectivo sítio oficial do

MPMG, o resumo do presente contrato, nos termos e condições previstas na Lei Federal nº 14.133/21.

CLÁUSULA VIGÉSIMA – Do Foro

É competente o foro da Comarca de Belo Horizonte/MG para dirimir quaisquer questões oriundas deste instrumento que não possam ser compostos pela conciliação, nos termos do art. 92, §1º, da Lei Federal nº 14.133/21.

CLÁUSULA VIGÉSIMA PRIMEIRA – Dos Documentos Integrantes

Integram o presente contrato, independentemente de transcrição, para todos os efeitos, o Termo de Referência; o Edital da Licitação; a Proposta do(a) Contratado(a) e eventuais anexos dos documentos supracitados.

CLÁUSULA VIGÉSIMA SEGUNDA – Dos Casos Omissos

Os casos omissos serão decididos pelo Contratante, segundo as disposições contidas na Lei Federal nº 14.133/21e em normas e princípios gerais dos contratos.

ANEXO I

PLANILHA DE PREÇOS

Processo Licitatório nº 22/2025

Objeto: O objeto da presente licitação é a prestação de serviços de empresa especializada em tecnologia da informação para subscrição de licenciamento de solução de segurança e antivírus, conforme especificações, exigências e quantidades estabelecidas no Termo de Referência.

1) IDENTIFICAÇÃO DO LICITANTE: Conforme preâmbulo do Contrato.

2) DAS EXIGÊNCIAS DA PROPOSTA:

2.1) PRAZO DE VALIDADE DA PROPOSTA: 60 DIAS, contados da data de sua apresentação;

2.2) PRAZO DE ENTREGA/EXECUÇÃO DOS SERVIÇOS:

2.2.1) DO PRAZO DE ENTREGA DAS LICENÇAS DE SUBSCRIÇÃO: 15 DIAS CORRIDOS, contados do recebimento, pela Contratada, da Ordem de Serviço;

2.2.2) **DO PRAZO PARA A CAPACITAÇÃO:** 40 DIAS CORRIDOS, contados a partir do recebimento pela contratada da ordem de serviço;

2.3) PRAZO DE SUBSTITUIÇÃO / REFAZIMENTO: 7 DIAS CORRIDOS, contados do recebimento da solicitação;

2.4) PRAZO DE GARANTIA

2.4.1) O FABRICANTE da solução do software oferecerá a garantia durante todo o período da vigência contratual, estabelecida no item 15.1 do Termo de Referência (Anexo IV do Edital).

2.5) PRESTAÇÃO DA GARANTIA: Se o prazo de garantia for superior ao legal, o licitante deverá, no ato da entrega da nota fiscal (ou documento equivalente), repassar à contratante **termo ou certificado de garantia**, constando a cobertura de todo o objeto, pelo período definido no item 2.4 desta proposta;

2.5.1) A garantia inclui todos os seus acessórios e será oferecida pelo FABRICANTE;

2.5.2) Os custos com transporte para fins de execução de serviços relativos à garantia, inclusive quando realizados fora da RMBH, serão arcados exclusivamente pela contratada;

2.5.3) A garantia será prestada por empresa credenciada pelo fabricante, preferencialmente situada na Região Metropolitana de Belo Horizonte (RMBH – LC Nº 63/02), sendo indicada(s):

Empresa (razão social): BRASOFTWARE INFORMÁTICA LTDA.	
CNPJ: 57.142.978/0001-05	
Endereço: Rua Marina La Regina, nº 227 – 3º. Andar – Salas 11 a 15 – Centro – Poá/ SP – CEP 08.550-210	
Telefone: (11) 3179-6100	E-mail: operacoesgoverno@brasoftware.com.br

2.6) DECLARAÇÕES: deverão ser apresentadas, juntamente com esta Proposta, declarações conforme modelo constante do Anexo V do Edital;

2.7) Deverá(ão) ser apresentado(s), juntamente com a proposta: O licitante deverá apresentar, junto com a proposta, catálogo, prospecto ou folder, para permitir a verificação da compatibilidade do fabricante da solução, do modelo/versão da licença e do tipo de licenciamento com as especificações técnicas exigidas no edital.

3) O PREÇO E AS ESPECIFICAÇÕES MÍNIMAS:

LOTE 1 – Solução de Proteção de Endpoint com funcionalidade EDR									
Brasoftware Informática Ltda.									
Item	**QTD**	**UND**	**Especificações do Item**	**COD. SIAD**	**Preço**		**Preço deduzido ICMS(*)**		**Marca/ modelo**
					Unitário	**Total**	**Unitário**	**Total**	
1	9.700	Un	Solução de Proteção de Endpoint com funcionalidade EDR (36 meses)	119750	R$85,40	R$828.380,00	--	--	KASPERSKY
PREÇO TOTAL DO LOTE									
R$ 828.380,00 (oitocentos e vinte e oito mil, trezentos e oitenta reais)									

(*)Caso aplicável, informar valor com e sem ICMS. É de responsabilidade do licitante o conhecimento da carga tributária aplicável à presente contratação.

LOTE 2 – Solução de Proteção de Endpoint com serviço gerenciado de Detecção e Resposta (MDR)									
Brasoftware Informática Ltda.									
Item	**QTD**	**UND**	**Especificações do Item**	**COD. SIAD**	**Preço**		**Preço deduzido ICMS(*)**		**Marca/ modelo**
					Unitário	**Total**	**Unitário**	**Total**	

1	300	Un	Solução de Proteção de Endpoint com serviço gerenciado de Detecção e Resposta (MDR) - **para estações de trabalho** (36 meses)	135267	R$550,74	R$165.222,00	--	--	KASPERSKY
2	100	Un	Solução de Proteção de Endpoint com serviço gerenciado de Detecção e Resposta (MDR) - **para servidores** (36 meses)	119768	R$550,74	R$55.074,00	--	--	KASPERSKY
PREÇO TOTAL DO LOTE									
R$ 220.296,00 (duzentos e vinte mil, duzentos e noventa e seis reais)									

(*)Caso aplicável, informar valor com e sem ICMS. É de responsabilidade do licitante o conhecimento da carga tributária aplicável à presente contratação.

ANEXO II
TERMO DE REFERÊNCIA

PROCESSO LICITATÓRIO Nº 22/2025

DOCUMENTO DE FORMALIZAÇÃO DE DEMANDA (DFD): 196/2023 e 606/2024

PROCESSO SEI: 19.16.1937.0123734/2024-83

1 - DO OBJETO:

1.1 - DESCRIÇÃO DO OBJETO:

Prestação de serviços de empresa especializada em tecnologia da informação para subscrição de licenciamento de solução de segurança e antivírus, conforme especificações, exigências e quantidades estabelecidas neste Termo de Referência.

1.2 - DESCRIÇÃO DETALHADA DA SOLUÇÃO ESCOLHIDA:

1.2.1. A CONTRATADA deverá observar os seguintes requisitos gerais para os LOTES 1 e 2:

1.2.1.1. A Solução fornecida deve ser baseada na arquitetura cliente/servidor, sendo composta por componente de gerência centralizada e agentes de detecção de malware com funcionalidade EDR (E*ndpoint Detection and Response*).

1.2.1.2. A solução de gerenciamento centralizado deve ser fornecida, preferencialmente, através da nuvem. Caso o fornecedor opte por oferecer o serviço de gerenciamento centralizado de forma local, deverá disponibilizá-lo por meio de um *appliance* virtual do mesmo fabricante da solução fornecida, ou a Contratada deverá realizar a instalação e configuração dos servidores necessários no ambiente disponibilizado, sem custo adicional para a Contratante. Os componentes da solução devem ser compatíveis com o ambiente tecnológico do MPMG.

1.2.1.3. A solução deve ser fornecida pronta para utilização imediata, sem necessidade de desenvolvimento adicional após a contratação. A solução deve ser de um único fabricante, sem incluir módulos, softwares, scripts ou plug-ins de terceiros, exceto módulos nativos do sistema operacional.

1.2.1.4. A solução deve oferecer proteção contra malwares. Deverá ser capaz de prevenir ou detectar e adotar ação de contenção, emitindo o respectivo alerta, quando for detectada alguma ameaça.

1.2.1.5. Deverá efetuar, preferencialmente, proteção permanente e em tempo real dos processos em memória.

1.2.1.6. Proporcionar proteção contra ameaças, tais como vírus, ransomwares, trojans, spywares, worms, keylogers, dentre outros malwares.

1.2.1.7. Ser capaz de reconhecer ataques e ações maliciosas por análise comportamental, que poderá ser complementada com detecção de assinaturas e por análise heurística.

1.2.1.8. Permitir determinar ações como quarentena, restauração e exclusão de arquivos infectados.

1.2.1.9. Possibilitar a restauração manual de arquivos quarentenados, quando aplicável.

1.2.1.10. Permitir a criação de listas de exclusão ou exceções para aplicativos específicos.

1.2.1.11. Os mecanismos de proteção deverão ser executados sem comprometer o desempenho dos computadores, de forma que não seja perceptível aos seus usuários nem influenciem negativamente no rendimento de aplicações.

1.2.1.12. Permitir a criação de políticas para bloqueio ou varredura automática de dispositivos de armazenamento externos, caso aplicável.

1.2.1.13. Apresentar interface para investigação ou análise das características da ameaça detectada nos equipamentos em análise.

1.2.1.14. Deverá oferecer mecanismo de bloqueio automático da ameaça baseado nas capacidades de detecção e resposta.

1.2.1.15. Deve prover uma visão do fluxo do ataque identificado e informações sobre os comportamentos detectados.

1.2.1.16. A Solução deverá efetuar a proteção permanente, em tempo real, quando arquivos forem acessados, lidos, gravados, alterados ou renomeados.

1.2.1.17. As ações de gerenciamento de eventos/incidentes, via gestão centralizada (console), poderão ser realizadas tanto pelos usuários administradores, quanto, preventivamente, de forma automática pela própria solução.

1.2.1.18. A solução (console de gerenciamento) deverá fornecer forma de controle de acessos baseado em papeis ou funções (RBAC) ou outra forma que demonstre eficácia equivalente para o referido controle no âmbito da instituição.

1.2.1.19. Deverá permitir integração com soluções de terceiros para monitoramento e correlação de eventos de segurança, como XDR e SIEM.

LOTE 1

Solução de Proteção de Endpoint com funcionalidade EDR

(Endpoint Detection and Response)

1.2.2. REQUISITOS PARA O OBJETO DO LOTE 1:

1. A CONTRATADA deverá observar os seguintes requisitos técnicos específicos:
2. A gerência centralizada da solução deverá:
3. Fornecer uma interface gráfica (GUI) acessível de forma segura (HTTPS) via software ou navegador web.
4. Caso a console seja Web, deve ser compatível com pelo menos dois dos seguintes navegadores: Microsoft Edge, Google Chrome, ou Mozilla Firefox, todos em sua última versão ou, no mínimo, dentre as cinco últimas versões.
5. Funcionar plenamente sem necessidade de instalação de plug-ins, drivers, Java ou Flash Player.
6. Permitir o gerenciamento, controle, configuração e operação de todo o parque de dispositivos (produtos instalados nos clientes e quaisquer outros módulos da solução) de forma remota e centralizada.
7. Permitir acessos simultâneos de pelo menos 4 usuários à console de gerenciamento.
8. Possuir uma base de dados centralizada para armazenamento de informações e logs dos clientes e da gerência.
9 . Permitir a criação e distribuição de políticas e tarefas remotamente para todo o agrupamento de itens gerenciados, grupos específicos ou itens individuais via console de gerenciamento.
10. Permitir deploy em massa através de ferramentas de mercado, ou, instalação, desinstalação e/ou atualização dos módulos da solução para todo o agrupamento de itens gerenciados, grupos específicos ou itens individuais via console de gerenciamento.
11. Oferecer funcionalidades para execução, criação e customização de consultas às informações na base de dados, com possibilidade de exibição em gráficos ou tabelas e, preferencialmente, exportação em formatos como CSV ou JSON.
12. Permitir a criação de alertas e notificações de eventos para administradores e usuários específicos.
13. Possibilitar pesquisa no histórico de eventos
14. Permitir a execução de consultas por agendamento e envio do resultado por e-mail.
15. Disponibilizar consultas pré-definidas, tais como: eventos de ameaças, malwares detectados e bloqueados, máquinas ou usuários com maior número de ocorrências de ameaças e histórico de ameaças mais recorrentes, para, no mínimo, os últimos 30 dias.
16. Garantir que o tráfego de dados entre os agentes e a gerência centralizada ocorra via conexão segura.
17. O acesso à console da gerência centralizada deve ser feito via autenticação segura.

18. Todas as ações realizadas pelos usuários da gerência devem ser registradas em logs de auditoria, incluindo descrição da ação, nome do usuário, data e hora.
19. No caso de gerência na nuvem, deve prover retenção dos respectivos logs por, preferencialmente, no mínimo 1 mês, e permitir sua exportação. Para gerência on-premise, deve permitir a exportação dos logs e a criação de backups da base de dados.
20. Permitir cadastro de usuários com perfis, pelo menos, de administradores (com acesso total) e de visualização/monitoramento.
21. Permitir a instalação e desinstalação remota dos agentes através da console de gerenciamento.
2 2 . Possibilitar o download de pacotes executáveis de instalação para proceder com a instalação manual nos equipamentos suportados.
23. Permitir a limpeza automática de agentes inativos, liberando as respectivas licenças.
24. Para soluções na nuvem, a plataforma deve utilizar controles de segurança equivalentes ao nível do padrão SOC2.
25. Permitir a criação de políticas para distribuição de atualizações diárias e configuração para que o agente busque atualizações na nuvem do fabricante.
26. Permitir a visualização do inventário das máquinas que possuem o agente instalado, contendo, no mínimo, nome ou identificador da máquina e versão do agente.
27. A versão das atualizações aplicadas deve ser exibida em cada máquina (on premise), ou a data de última comunicação do agente (nuvem).
28. Manter log de auditoria com registro das configurações realizadas por qualquer administrador do sistema.
29. Consultas no histórico de eventos ou de achados (indicadores de atividades suspeitas, ameaças, falhas ou vulnerabilidades), via console, devem fornecer os resultados, em regra, imediatamente (em até 30 segundos, relativamente ao tempo de resposta da aplicação).
30. Ser compatível com as seguintes tecnologias de sistema operacional, no mínimo: Windows 10 e Windows 11.
31. Permitir criar bloqueios personalizados, baseado no nome do aplicativo, caminho do aplicativo ou hash do arquivo.
32. Possuir, preferencialmente, mecanismos de análise avançada para proteção contra vírus de código polimorfos, ofuscados, criptografados, e contra ameaças avançadas e persistentes (APTs).
33. Permitir, preferencialmente, a detecção de variações de malwares geradas em memória principal.
34. Em casos de aplicações com comportamento malicioso detectado, deverá efetuar bloqueios de processos e efetuar isolamento de comunicação, ou medida de contenção com efeito equivalente.
35. Oferecer proteção contra ransomware, com capacidade de avaliar, por exemplo, processos criptográficos em execução no sistema, exclusão de backups, número alto de operações de I/O no sistema de arquivos.
36. Informar o nome ou endereço IP da origem do ataque ou ameaça, quando aplicável.
37. Oferecer funcionalidade de controle de aplicações, identificando aplicações no mínimo pelo código hash do executável, caminho ou nome do aplicativo malicioso.
38. Oferecer proteção contra vírus de macro e por scripts variados, incluindo shell e powershell.
39. A console deve oferecer, preferencialmente, uma linha do tempo, contendo toda a sequência de eventos que ocorreram durante a execução do malware. Deverão estar incluídos na visualização da cadeia de ataque, preferencialmente, os processos e aplicativos executados, arquivos e registros utilizados, endereços acessados, dentre outros.
40. Devem ser coletadas as atividades dos artefatos analisados, por exemplo, informações como interação com outros processos, arquivos ou chaves de registro acessadas/modificadas, ou conexões de rede realizadas.

41. Oferecer proteção contra processos que tentem alterar ou manipular indevidamente os componentes instalados e em execução do antivírus (autoproteção).
42. As seguintes ocorrências, quando aplicáveis, deverão ser registradas em arquivo de log exportável ou enviadas para a gerência centralizada:

43. Atualização de engine e/ou repositório de vacinas.

44. Recebimento de políticas e tarefas da gerência.
45. Inicialização e finalização de varreduras, agendadas ou manuais, ou reportar imediatamente as detecções quando realizada por meio de análise dos processos em tempo real.
46. A detecção de alguma ameaça deverá ser registrada em arquivo de log local ou enviada para a gerência centralizada, contendo, quando aplicáveis, as seguintes informações:
47. Nome da ameaça
48. Tipo da ameaça
49. Severidade
50. Arquivo ou local infectado
51. Data e hora da detecção
52. Nome da máquina/endereço IP afetado
53. IP ou nome de origem, se disponível
54. Usuário logado no sistema
55. Ação realizada pela solução
56. Os logs deverão contemplar, além dos atributos do ataque ou da ameaça detectados, conforme descritos no item precedente, as ações realizadas pela ameaça no sistema. Esses logs devem poder ser exportados pela CONTRATADA para persistência e leitura em outro destino, ou deve ser possível sua obtenção, sem custo adicional, através de interface provida pela solução.
57. A solução deverá oferecer detecção e bloqueio em tempo real para as principais ameaças, contemplando, preferencialmente, os seguintes tipos ou vetores:
58. Na memória principal (RAM), incluindo técnicas de manipulação e randomização de memória, protegendo contra a exploração de vulnerabilidades em aplicações.
59. Em arquivos, incluindo compactados.
60. Em dados provenientes de browsers de navegação web.
61. Em processos de inicialização automática.
62. Em serviços criados/modificados.
63. Para ataques fileless.
64. Para ameaças persistentes avançadas (APTs).
65. Para ransomwares, exploits e outros comportamentos maliciosos, o que inclui a detecção e bloqueio de ferramental e técnicas de exploração amplamente disponíveis como metasploit, mimikatz, entre outros.
66. Ameaças que utilizem as seguintes técnicas ou respectivas tentativas:
67. ofuscação e sequestro de DLL.
68. evasão, incluindo injeção de processos (process injection) e uso de executáveis legítimos do Windows para executar scripts e ações maliciosas.
69. Execução a partir diretórios incomuns (ex: diretório de dados, temp e lixeira) ou criação e/ou escrita em locais suspeitos já conhecidos.
70. elevações de privilégio inesperadas.
71. conexões de rede suspeitas (call back ou command & control).
72. uso suspeito do PSEXEC.
73. invocação maliciosa através do Rundll.
74. exploração ou modificação do arquivo hosts.
75. invocação de Remote Shell.
76. A análise dos artefatos deve ocorrer, preferencialmente, em pré-execução, ou seja, antes de

serem executados no sistema operacional, evitando que a máquina seja infectada.
77. Deverá permitir bloqueio de alterações nas configurações do antivírus por parte do usuário, sendo permitido apenas por alterações de políticas ou mediante inserção de senha definida na gerência.
78. Deverá impedir instalação e execução de aplicativos cujo comportamento seja suspeito ou que estejam em lista de má reputação.
79. Deverá detectar e proteger em tempo real o computador contra ações maliciosas executadas em navegadores web por meio de páginas da web e scripts.
80. Deverá identificar e bloquear alterações suspeitas em chaves de registro ou tarefas agendadas na máquina.
81. Deverá fornecer informações do status do agente e de seus componentes, através da gerência, com informações atualizadas.
82. As informações disponibilizadas no console de gerência, pelos agentes e demais componentes devem sê-lo nos idiomas português, preferencialmente, ou inglês.
83. O agente da solução deve realizar suas análises e bloqueios nas estações mesmo quando estiver sem conectividade com os servidores da solução e sem acesso à Internet.
84. Deve ser possível realizar a configuração de proxy no agente ou obter as configurações de proxy definidas no próprio sistema operacional, caso necessário.
85. Deve ser possível definir as seguintes ações de resposta, ou ação com efeito de contenção equivalente da ameaça, quando uma ameaça ou comportamento malicioso for detectado:
86. Alertar
87. Bloquear
88. Remover ou quarentenar
89. Isolar a máquina, de maneira que ela perca a comunicação com a rede ou se comunique apenas com os servidores da solução ou com servidores e serviços definidos na política de isolamento.
90. O agente deve ter a capacidade de fazer o isolamento da máquina por si só, sem precisar de nenhuma intervenção manual.
91. Deve ser possível ao administrador efetuar a liberação da máquina do isolamento via console de gerência ou fornecer uma chave para realizar a liberação.
92. A criação de usuários para a console deve permitir senhas de no mínimo 8 caracteres de tipos como: letras maiúsculas, letras minúsculas, dígitos numéricos e caracteres especiais.
93. A console de gerência deve permitir, preferencialmente, a configuração de autenticação em múltiplos fatores.
94. Permitir a configuração de alertas em tempo real de ameaças com envio de e-mail a usuários pré-definidos.
95. Ser capaz de detectar e exibir em relatório as vulnerabilidades existentes em aplicativos ou softwares instalados nos dispositivos.

LOTE 2

Solução de Proteção de Endpoint com funcionalidade MDR

(Managed Detection and Response)

1.2.3. REQUISITOS PARA O OBJETO DO LOTE 2:

A gerência centralizada da solução deverá:

1. Fornecer uma interface gráfica (GUI) acessível de forma segura (HTTPS) via software ou navegador web.
2. Caso a console seja Web, deve ser compatível com pelo menos dois dos seguintes

navegadores: Microsoft Edge, Google Chrome, ou Mozilla Firefox, todos em sua última versão ou, no mínimo, dentre as cinco últimas versões.
3. Funcionar plenamente sem necessidade de instalação de plug-ins, drivers, Java ou Flash Player.
4. Permitir o gerenciamento, controle, configuração e operação de todo o parque de dispositivos (produtos instalados nos clientes e quaisquer outros módulos da solução) de forma remota e centralizada.
5. Permitir acessos simultâneos de pelo menos 4 usuários à console de gerenciamento.
6. Possuir uma base de dados centralizada para armazenamento de informações e logs dos clientes e da gerência.
7. Permitir a criação e distribuição de políticas e tarefas remotamente para todo o agrupamento de itens gerenciados, grupos específicos ou itens individuais via console de gerenciamento.
8 . Permitir deploy em massa através de ferramentas de mercado, ou, instalação, desinstalação e/ou atualização dos módulos da solução para todo o agrupamento de itens gerenciados, grupos específicos ou itens individuais via console de gerenciamento.
9. Oferecer funcionalidades para execução, criação e customização de consultas às informações na base de dados, com possibilidade de exibição em gráficos ou tabelas e, preferencialmente, exportação em formatos como CSV ou JSON.
10. Permitir a criação de alertas e notificações de eventos para administradores e usuários específicos.
11. Possibilitar pesquisa no histórico de eventos.
12. Permitir a execução de consultas por agendamento e envio do resultado por e-mail.
13. Disponibilizar consultas pré-definidas, tais como: eventos de ameaças, malwares detectados e bloqueados, máquinas ou usuários com maior número de ocorrências de ameaças e histórico de ameaças mais recorrentes, para, no mínimo, os últimos 30 dias.
14. Garantir que o tráfego de dados entre os agentes e a gerência centralizada ocorra via conexão segura.
15. O acesso à console da gerência centralizada deve ser feito via autenticação segura.
16. Todas as ações realizadas pelos usuários da gerência devem ser registradas em logs de auditoria, incluindo descrição da ação, nome do usuário, data e hora.
17. No caso de gerência na nuvem, deve prover retenção dos respectivos logs por, preferencialmente, no mínimo 1 mês, e permitir sua exportação. Para gerência on-premise, deve permitir a exportação dos logs e a criação de backups da base de dados.
18. Permitir cadastro de usuários com perfis, pelo menos, de administradores (com acesso total) e de visualização/monitoramento.
19. Permitir a instalação e desinstalação remota dos agentes através da console de gerenciamento.
2 0 . Possibilitar o download de pacotes executáveis de instalação para proceder com a instalação manual nos equipamentos suportados.
21. Permitir a limpeza automática de agentes inativos, liberando as respectivas licenças.
22. Para soluções na nuvem, a plataforma deve utilizar controles de segurança equivalentes ao nível do padrão SOC2.
23. Permitir a criação de políticas para distribuição de atualizações diárias e configuração para que o agente busque atualizações na nuvem do fabricante.
24. Permitir a visualização do inventário das máquinas que possuem o agente instalado, contendo, no mínimo, nome ou identificador da máquina e versão do agente.
25. A versão das atualizações aplicadas deve ser exibida em cada máquina (on premise), ou a data de última comunicação do agente (nuvem).
26. Manter log de auditoria com registro das configurações realizadas por qualquer administrador do sistema.

27. Consultas no histórico de eventos ou de achados (indicadores de atividades suspeitas, ameaças, falhas ou vulnerabilidades), via console, devem fornecer os resultados, em regra, imediatamente (em até 30 segundos, relativamente ao tempo de resposta da aplicação).
28. Ser compatível com as seguintes tecnologias de sistema operacional, no mínimo: Windows 10 e Windows 11; Red Hat Enterprise Linux (RHEL) e Windows Server, ambos no mínimo três versões anteriores à última estável disponibilizada pelo fabricante.
29. Permitir criar bloqueios personalizados, baseado no nome do aplicativo, caminho do aplicativo ou hash do arquivo.
3 0 . Possuir, preferencialmente, mecanismos de análise avançada para proteção e remediação de vírus de código polimorfos, ofuscados, criptografados, e contra ameaças avançadas e persistentes (APTs), que não são detectadas pelos métodos convencionais de antivírus.
31. Permitir, preferencialmente, detecção de variações de malwares geradas em memória principal.
32. Em casos de aplicações com comportamento malicioso detectado, deverá efetuar bloqueios de processos e efetuar isolamento de comunicação, ou medida de contenção com efeito equivalente.
33. Oferecer proteção contra ransomware, com capacidade de avaliar processos criptográficos em execução no sistema, exclusão de backups, número alto de operações de I/O no sistema de arquivos.
34. Informar o nome ou endereço IP da origem do ataque, quando aplicável.
35. Oferecer funcionalidade de controle de aplicações, identificando aplicações no mínimo pelo código hash do executável, caminho ou nome do aplicativo malicioso.
36. Oferecer proteção contra vírus de macro e por scripts variados, incluindo shell e powershell.
37. A console deve oferecer uma linha do tempo, contendo toda a sequência de eventos que ocorreram durante a execução do malware. Deverão estar incluídos na visualização da cadeia de ataque, quando aplicável, os processos e aplicativos executados, arquivos e registros utilizados, dentre outros.
38. Devem ser coletadas as atividades dos artefatos analisados, por exemplo, informações como interação com outros processos, arquivos ou chaves de registro acessadas/modificadas, ou conexões de rede realizadas.
39. Oferecer proteção contra processos que tentem alterar ou manipular indevidamente os componentes instalados e em execução do antivírus (autoproteção).
40. As seguintes ocorrências, quando aplicáveis, deverão ser registradas em arquivo de log exportável ou enviadas para a gerência centralizada:
41. Atualização de engine e/ou repositório de vacinas, quando aplicável.
42. Recebimento de políticas e tarefas da gerência.
43. Inicialização e finalização de varreduras, agendadas ou manuais, ou reportar imediatamente as detecções quando realizada por meio de análise dos processos em tempo real.
44. A detecção de alguma ameaça deverá ser registrada em arquivo de log local ou enviada para a gerência centralizada, contendo, quando aplicáveis, as seguintes informações:
45. Nome da ameaça
46. Tipo da ameaça
47. Tática e técnica utilizada
48. Severidade
49. Arquivo ou local infectado
50. Data e hora da detecção
51. Nome da máquina/endereço IP afetado
52. IP ou nome de origem, se disponível
53. Usuário logado no sistema
54. Ação realizada pela solução

55. Os logs deverão contemplar, além dos atributos do ataque ou da ameaça detectados, conforme descritos no item precedente, as ações realizadas pela ameaça no sistema. Esses logs devem poder ser exportados pela CONTRATADA para persistência e leitura em outro destino, ou deve ser possível sua obtenção, sem custo adicional, através de interface provida pela solução.
56. A solução deverá oferecer detecção e bloqueio em tempo real para as principais ameaças, contemplando, preferencialmente, os seguintes tipos ou vetores:
57. Na memória principal (RAM), incluindo técnicas de manipulação e randomização de memória, impossibilitando a exploração de vulnerabilidades em aplicações.
58. Em arquivos, incluindo compactados.
59. Via comunicação em rede.
60. Em dados provenientes de browsers de navegação web.
61. Em processos de inicialização automática.
62. Em serviços criados/modificados.
63. Para ataques fileless.
64. Para ameaças persistentes avançadas (APTs).
65. Para ransomwares, exploits e outros comportamentos maliciosos, o que inclui a detecção e bloqueio de ferramental e técnicas de exploração amplamente disponíveis como metasploit, mimikatz, entre outros.
66. Para ameaças que utilizem as seguintes técnicas ou respectivas tentativas:
67. ofuscação e sequestro de DLL.
68. evasão, incluindo injeção de processos (process injection) e uso de executáveis legítimos do Windows para executar scripts e ações maliciosas.
69. execução a partir diretórios incomuns (ex: diretório de dados, temp e lixeira) ou criação e/ou escrita em locais suspeitos já conhecidos.
70. elevações de privilégio inesperadas.
71. conexões de rede suspeitas (call back ou command & control).
72. uso suspeito do PSEXEC.
73. invocação maliciosa através do Rundll.
74. exploração ou modificação do arquivo hosts.
75. invocação de Remote Shell
76. A análise dos artefatos deve ocorrer em pré-execução, ou seja, antes de serem executados no sistema operacional, evitando que a máquina seja infectada.
77. Deverá permitir bloqueio de alterações nas configurações do antivírus por parte do usuário, sendo permitido apenas por alterações de políticas ou mediante inserção de senha definida na gerência.
78. Deverá impedir instalação e execução de aplicativos cujo comportamento seja suspeito ou que estejam em lista de má reputação.
79. Deverá detectar e proteger em tempo real o computador contra ações maliciosas executadas em navegadores web por meio de páginas da web e scripts.
80. Deverá identificar e bloquear alterações suspeitas em chaves de registro ou tarefas agendadas na máquina.
81. Deverá fornecer informações do status do agente e de seus componentes, através da gerência, com informações atualizadas.
82. As informações disponibilizadas no console de gerência, pelos agentes e demais componentes devem sê-lo nos idiomas português, preferencialmente ou inglês.
83. O agente da solução deve realizar suas análises e bloqueios nas estações mesmo quando estiver sem conectividade com os servidores da solução e sem acesso à Internet.
84. Deve ser possível realizar a configuração de proxy no agente ou obter as configurações de proxy definidas no próprio sistema operacional, caso necessário.
85. Deve ser possível definir as seguintes ações de resposta, ou ações de efeito equivalente para

contenção da ameaça, quando uma ameaça ou comportamento malicioso for detectado:
86. Alertar
87. Bloquear
88. Remover ou quarentenar
89. Isolar a máquina, de maneira que ela perca a comunicação com a rede ou se comunique apenas com os servidores da solução ou com servidores e serviços definidos na política de isolamento.
90. O agente deve ter a capacidade de fazer o isolamento da máquina por si só, sem precisar de nenhuma integração com outros softwares ou dispositivos de rede para isso.
91. Deve ser possível ao administrador efetuar a liberação da máquina do isolamento via console de gerência ou fornecer uma chave para realizar a liberação.
92. A criação de usuários para a console deve permitir senhas com complexidade em conformidade com os padrões de segurança aceitos no mercado (tamanho mínimo e caracteres especiais).
93. A console de gerência deve permitir a configuração de autenticação em múltiplos fatores.
94. Permitir a configuração de alertas em tempo real de ameaças com envio de e-mail a usuários pré-definidos.
95. Ser capaz de detectar e exibir em relatório as vulnerabilidades existentes em aplicativos ou softwares instalados nos dispositivos.
9 6 . A solução deve, preferencialmente, mitigar o risco associado aos seguintes comportamentos conhecidos de exploração de vulnerabilidades:
97. SEHOP - Structured Exception Handler Overwrite Protection;
98. Heap Spray (Exploits que iniciam através do HEAP)
99. Java Exploit Protection
100. A solução deverá ter a capacidade de bloquear exploits que trabalham em nível de “shell code”.
101. A solução deverá ser capaz de prevenir ataques de injeção de código malicioso em processos comumente atacados, como Local Security Authority Subsystem Service (LSASS) em sistemas Windows.
102. Oferecer serviço MDR que contemple:
103. Serviço remoto, hospedado e gerenciado pelo provedor da solução de proteção de endpoint (fabricante), que efetue atividades em tempo real de detecção de ameaça, investigação e ações de mitigação, tendo como ponto de partida os alertas, eventos e achados da solução.
104. Funcionamento 24x7, que monitore ativa e diariamente os eventos registrados pela ferramenta, relativos ao ambiente da instituição, com capacidade para atuar em análise customizada de acordo com o contexto dos eventos e cenários conhecidos de
risco cibernético.
105. Disponibilidade imediata para resposta investigativa e notificação da equipe designada da instituição em caso de detecção de eventos ou indicadores que necessitem de resposta, incluindo contenção.
106. Triagem, investigação, análise e comunicação à equipe designada da CONTRATANTE, independentemente de solicitação formal ou “ticket” aberto pela CONTRATANTE.
107. Atividades de resposta e análise que incluam a indicação dos objetivos prováveis do ataque, nível de sucesso do ataque, impactos estimados, ações de remediação e de prevenção que devem ser tomadas pela CONTRATANTE, descrição do incidente, incluindo linha do tempo, ações, táticas e técnicas utilizadas pela ameaça, estampa de tempo de ocorrência do incidente, tempo de detecção do incidente, prioridade, classificação conforme categoria do incidente, origem e ativos afetados.
108. Não haverá limitação de volume ou tempo para as atividades de detecção e resposta gerenciada.

109. Explicação, mediante demanda da CONTRATANTE, acerca dos eventos detectados pela solução ou do relatório de incidente enviado à CONTRATANTE.
110. O serviço poderá ser prestado em português ou inglês.

1.2.4. CAPACITAÇÃO:

1.2.4.1. A CONTRATADA deverá prover capacitação (passagem de conhecimento), sobre sua solução para até 10 (dez) pessoas indicadas pelo CONTRATANTE, atendendo às seguintes obrigações:

Operação da solução, incluindo:
- Instalação e configuração dos componentes de gerência;
- Gerência de políticas, tarefas e demais atividades disponibilizadas pela solução;
- Instalação e configuração dos agentes;
- Criação e execução de consultas e relatórios;
- Análise de relatórios;
- Análise de artefatos;
- Integrações para extração de dados, como via API ou WebService;

A capacitação será realizada em dias úteis (de segunda a sexta-feira), no horário das 9h (nove) às 18h (dezoito), por meio de videoconferência de forma REMOTA.

1.2.4.1.1. Todas as despesas relacionadas à capacitação, incluindo instrutores, elaboração de material didático e quaisquer outros custos associados, serão de responsabilidade exclusiva da CONTRATADA e deverão estar inclusas nas condições comerciais do licenciamento.

1.2.4.2. Se a solução contratada para ambos os lotes for do mesmo fabricante e fornecida por um único fornecedor, será necessária apenas uma capacitação para atender às exigências dos dois lotes. No caso de fornecedores distintos, mas do mesmo fabricante, a capacitação será de responsabilidade do vencedor do Lote 1 (EDR).

1.2.4.3. A CONTRATADA deverá disponibilizar material didático em formato digital, contendo guias detalhados, exemplos práticos e instruções para as atividades abordadas, permitindo aos participantes consultarem os conteúdos posteriormente.

1.2.4.4. A capacitação, incluída no fornecimento de cada lote, deverá ser iniciada após a entrega completa da solução e concluída em até 40 (quarenta) dias contados a partir da emissão da Ordem de Serviço (OS).

1.2.5. O Estudo Técnico Preliminar nº (8372878) foi devidamente aprovado pela chefia imediata Alexsander Batista Aguiar, da unidade
DIRETORIA DE SUPORTE E MANUTENÇÃO.

2 - DA FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO:

2.1. A Diretoria de Suporte e Manutenção (DSMT), unidade organizacional subordinada técnica e administrativamente à STI, tem como finalidade planejar, coordenar, promover, controlar e avaliar as atividades relacionadas à especificação, instalação e manutenção dos equipamentos de informática, bem como aquelas relativas ao atendimento ao usuário, na instituição.

Compete à Diretoria de Suporte e Manutenção promover a instalação e a configuração dos softwares homologados para o usuário pela STI, em conjunto com as demais unidades competentes. Para continuidade das atividades ministeriais de forma segura, observa-se a

necessidade de contratar serviço de proteção antivírus para os equipamentos institucionais em substituição à aplicação atualmente utilizada que está com o contrato em fase final de vigência.

O não atendimento da necessidade apresentada poderá ocasionar os seguintes prejuízos aos computadores institucionais:

Infecção por Malware: O computador pode ser facilmente infectado por malware, como vírus, worms, trojans e spyware, que podem causar desde pequenas perturbações até a destruição de dados ou roubo de informações. **Ransomware**: Sem um antivírus, o computador é mais vulnerável a ataques de ransomware, onde os invasores criptografam seus dados e exigem um pagamento para restaurar o acesso. **Roubo de Dados**: Informações pessoais e confidenciais, como senhas, dados bancários e documentos importantes, podem ser roubadas por hackers, que podem usá-las para fraudes ou outros crimes. **Phishing e Engenharia Social**: Sem proteção, o computador pode ser mais suscetível a ataques de phishing, onde os invasores tentam enganar o usuário para revelar informações sensíveis ou instalar malware. **Uso Indebido de Recursos**: Hackers podem usar o computador desprotegido para atividades ilícitas, como mineração de criptomoedas ou ataques de negação de serviço (DDoS), sem o conhecimento do usuário. **Redução de Desempenho**: Malwares podem consumir recursos do sistema, como CPU e memória, reduzindo o desempenho do computador e tornando-o lento e difícil de usar. **Perda de Dados**: Vírus e outros tipos de malware podem corromper ou apagar arquivos importantes, resultando em perda permanente de dados. **Comprometimento da Rede**: Se o computador faz parte de uma rede, a falta de um antivírus pode permitir que o malware se espalhe para outros dispositivos na mesma rede, ampliando o impacto do ataque. **Invasão de Privacidade**: Programas maliciosos podem permitir que hackers monitorem as atividades do usuário, gravem as teclas digitadas ou acessem a webcam e o microfone sem permissão.
Ataques Zero-Day: Sem um antivírus, o computador é mais vulnerável a ataques de dia zero, que exploram vulnerabilidades ainda desconhecidas pelos desenvolvedores de software.

Por esses motivos, é altamente recomendável que todos os computadores tenham um software antivírus atualizado instalado para proteger contra essas ameaças.

Uma EPP é um tipo de software de segurança que protege dispositivos controlados de usuários finais, como computadores desktop, laptops e dispositivos móveis, contra ataques prejudiciais novos e conhecidos. Além disso, os EPPs permitem que as equipes de segurança identifiquem e possam remediar eventos de ameaça que passem pelas primeiras camadas de controles preventivos, antes da chegada do conteúdo malicioso aos dispositivos. As soluções EPP são oferecidas como agentes de software instalados nos dispositivos e vinculados a análises de segurança centralizadas e interfaces de gerenciamento.

Um EPP normalmente fornece os seguintes componentes:

· Portal de gerenciamento: um console centralizado que permite que os analistas implantem e gerenciem agentes e configurações de segurança. Além disso, ajuda os analistas a realizarem a triagem, investigar, detectar e responder a incidentes de segurança.

· O software sensor/agente: instalado nas estações para fornecer recursos de prevenção, proteção, detecção e resposta. Ele reporta a telemetria ao portal de gerenciamento e aplica políticas de segurança.

Essas funcionalidades atendem a requisitos de segurança que são essenciais a organizações cujas operações dependem de dados e que gerenciam sistemas de Tecnologia da Informação.

Lote 1 - Solução de Proteção de Endpoint com funcionalidade EDR

Uma solução de Detecção e Resposta de *Endpoint* (*Endpoint Detection and Response* – EDR), componente principal de uma EPP, é um controle de defesa crítico para a maioria dos dispositivos de uma organização. Deve ser instalado um agente para auxiliar na detecção e reporte de comportamentos suspeitos e maliciosos, bem como na visualização da propagação de ataques e orientações de remediação. O EDR pode impedir famílias conhecidas de malware e *ransomware*, bem como detectar e remediar ameaças mais furtivas e desconhecidas.
É imperioso considerar que:

· Todas as estações de trabalho que se conectam a redes da organização ou tratam dados da instituição necessitam de proteção EDR.

· Novas ameaças e formas de explorações furtivas exigem detecção precoce e resposta rápida.

· Não é mais prático alcançar 100% de prevenção com controles de borda ou focados na entrega de ameaças ao ambiente organizacional, portanto, as ferramentas de EPP devem ser atualizadas para incluir a funcionalidade EDR, como forma de impedir ataques em curso nas fases subsequentes.

· Técnicas avançadas são usadas por campanhas furtivas de malware e ransomware, para evitar a detecção e contornar controles de segurança implementados em outras camadas.

· A resposta rápida em tempo real, à medida que os incidentes ocorrem, é fundamental para conter uma ameaça e evitar que ela se espalhe pelo ambiente de TI da organização.

· Para garantir que os sistemas não sejam mal configurados e não tenham vulnerabilidades não corrigidas, os programas de gestão de vulnerabilidades existentes devem ser complementados e dotados de meios para reduzir a superfície de ataque, para o que contribui a detecção de softwares vulneráveis nas estações de trabalho.

· A coleta de logs e eventos de agentes EDR serve como base para detecção e caça retrospectiva de ameaças.

· Ataques sofisticados exigem uma nova geração de ferramentas de EDR que colaborem holisticamente com outras ferramentas de segurança para criar um ecossistema de segurança que maximize a proteção e minimize a exposição.

Os ataques a endpoints corporativos estão se tornando mais complexos com o passar do tempo. No caso do *ransomware*, a ameaça estão sendo integrados aos Antivírus de Nova Geração (NGAVs) e EPPs para proteção contra essas ameaças mais avançadas. Essas soluções são alimentadas de dados para detectar e responder a ataques mais furtivos e ameaças sofisticadas, incluindo ataques incomuns, de longo prazo, direcionados e sem arquivo.

A análise estática de arquivos com aprendizado de máquina e pesquisas de hash baseadas em nuvem podem substituir ou complementar a detecção de malware baseada em assinaturas. Soluções nativas em nuvem que são simples de implantar e administrar, bem como detecção e análise baseadas em comportamento que identificam riscos desconhecidos, aumentam o retorno de uma EPP.

À medida que o sistema operacional central se torna mais seguro, os invasores provavelmente terão como alvo vulnerabilidades de aplicativos, bem como ataques de BIOS ou firmware, tornando os NGAVs ineficazes [1]. Além disso, NGAVs geralmente não detectam abordagens furtivas que utilizam softwares confiáveis.

Lote 2 - Solução de Proteção de Endpoint com serviço gerenciado de Detecção e Resposta (MDR)

Soluções contemporâneas de proteção de endpoint começam a trazer, de forma integrada, serviços gerenciados de detecção e resposta de incidentes, contemplando monitoramento continuado, por especialistas humanos, da telemetria gerada pelas soluções instaladas nos endpoints.

De acordo com o Gartner,

> *Os serviços gerenciados de detecção e resposta (MDR) fornecem aos clientes funções de centro de operações de segurança (SOC) entregues remotamente. Isso permite que as organizações detectem, analisem, investiguem e respondam ativamente através da interrupção e contenção de ameaças. Os provedores de MDR oferecem uma experiência pronta para uso, usando uma pilha de tecnologia que normalmente cobre endpoint, rede, logs e nuvem. Essa telemetria é analisada na plataforma do provedor por especialistas especializados em caça a ameaças e gerenciamento de incidentes*[2].

Nesse contexto, a utilização de serviços de MDR para obter recursos de operações de segurança acionados por humanos, 24 horas por dia, 7 dias por semana, entregues remotamente, afigura-se compatível com a otimização da eficiência na gestão dos recursos dedicados à segurança da informação na instituição, especialmente para os ativos de Tecnologia da Informação mapeados como mais críticos.

Para servidores e endpoints críticos, notadamente, aqueles que possuam vetores de acesso ou privilégios para modificação de infraestrutura crítica de TI da instituição, mostra-se desejável atrelar o provisionamento de uma solução de proteção de endpoints a serviços gerenciados de monitoramento 24hx7 providos pelo mesmo fabricante da ferramenta. Isso assegura maior rapidez, a qualquer tempo, na detecção e contenção de ameaças que tenham contato com esses ativos.

2.2. O objeto da contratação está previsto no Plano de Contratações Anual 2024 e 2025.

3 - DA DIVISÃO EM LOTES:

Número de Lotes: 2

Justificativa para o parcelamento ou não do objeto: Considerado o disposto no §1º do art. 47 da Lei Federal nº 14.133/2021, constatou-se a viabilidade do parcelamento da solução em 2 lotes (o primeiro contendo 1 item e o segundo contendo 2 itens), tendo em vista que o parcelamento promove a ampliação da competitividade entre fornecedores, permite a especialização das soluções contratadas e facilita o atendimento de características específicas de cada item. Essa divisão, além de possibilitar maior eficiência e economicidade, atende aos objetivos legais de assegurar contratações vantajosas e adequadas ao interesse público.

4 - DESCRIÇÃO DETALHADA DO OBJETO, QUANTITATIVOS, CÓDIGOS DO CATÁLOGO DE MATERIAIS E SERVIÇOS DO SIAD:

LOTE 1

ITEM	QTE	UNIDADE DE MEDIDA	DESCRIÇÃO RESUMIDA DO ITEM	CÓDIGO SIAD
1	9.700	unidades	Solução de Proteção de Endpoint com funcionalidade EDR (36 meses)	119750

LOTE 2

ITEM	QTE	UNIDADE DE MEDIDA	DESCRIÇÃO RESUMIDA DO ITEM	CÓDIGO SIAD
1	300	unidades	Solução de Proteção de Endpoint com serviço gerenciado de Detecção e Resposta (MDR) – para estações de trabalho (36 meses)	135267
2	100	unidades	Solução de Proteção de Endpoint com serviço gerenciado de Detecção e Resposta (MDR) – para servidores (36 meses)	119768

4.1 - DA JUSTIFICATIVA DO CÁLCULO ESTIMATIVO DOS QUANTITATIVOS APURADOS:

4.1.1. A quantidade de licenças da Solução de Proteção de Endpoint com funcionalidade EDR relativa ao Lote 1 foi estimada com base no atual parque tecnológico, atendido pela Solução de Proteção de Enpoint corrente (8.818). Tendo em vista que há constantes alterações no quadro funcional da instituição, é salutar a criação de uma reserva técnica, que corresponda a 10% do quantitativo de licenças para computadores e notebooks, ou seja 882 equipamentos, totalizando 9.700.

As quantidades para o Lote 2 (300 + 100) pautaram-se por uma análise de objetos com acessos privilegiados no ambiente de TI da instituição e em uma estimativa de quantitativo, com margem segura de ampliação, projetado para o período de duração da utilização da solução a ser contratada. O mesmo racional foi aplicado ao quantitativo atual de servidores críticos.

5 - DOS DOCUMENTOS TÉCNICOS E/OU APENSOS:

Não há necessidade de documentos técnicos.

6 - DA EXIGÊNCIA DE AMOSTRA:

Serão exigidas amostras para os lotes 1 e 2.

6.1. O pedido de amostra da licença de antivírus é necessário para assegurar a qualidade e a conformidade do produto com as especificações técnicas estabelecidas no edital, conforme o disposto no art. 41, inciso II, da Lei n.º 14.133/21. Esta exigência visa verificar previamente se a solução ofertada atende aos requisitos de proteção, desempenho e compatibilidade exigidos para

o ambiente tecnológico da Administração Pública, garantindo, assim, a adequação do software ao uso pretendido e a proteção dos dados sensíveis e sigilosos que são processados.

Além disso, a exigência da amostra possibilita avaliar, de maneira concreta e prática, se a solução proposta pelo fornecedor é efetiva no bloqueio de ameaças, detecção de vulnerabilidades e demais funcionalidades de segurança digital, minimizando o risco de falhas ou incompatibilidades que poderiam comprometer a operação dos sistemas de informação da Administração. Essa prática visa resguardar a Administração de possíveis prejuízos e zelar pela eficiência na gestão de recursos públicos, evitando a aquisição de produtos inadequados ou de baixa qualidade.

6.2. Será exigida amostra do primeiro classificado, e em caso de desclassificação, do seguinte na ordem de classificação, sucessivamente.
Após convocado pelo pregoeiro, o licitante deverá entregar licenças de teste na DIRETORIA DE SUPORTE E MANUTENÇÃO da PGJ (Av. Álvares Cabral, nº 1.740, 4º andar, BH/MG), em nome de Flávio Henrique Gomes ou por e-mail: flaviohenrique@mpmg.mp.br, durante o horário de 10:00 às 18:00 horas, no prazo máximo de 15 (quinze) dias, impreterivelmente.

6.3. Deverão ser entregues devidamente identificadas via sistema ou no e-mail.

6.4. Para a avaliação das amostras de licença de antivírus fornecidas, serão realizados os seguintes testes de aferição de compatibilidade e desempenho, com base em critérios objetivos previamente definidos:

Teste de Instalação e Desempenho no Ambiente Operacional: Verificação da compatibilidade do software com os sistemas operacionais utilizados pela instituição, garantindo que o antivírus seja instalado corretamente e funcione sem conflitos. Serão avaliados tempos de instalação, impacto no desempenho do sistema e consumo de recursos (CPU e memória).

Detecção e Remoção de Ameaças : Teste de eficácia do antivírus na identificação e remoção de ameaças comuns e avançadas, como malware, ransomware, trojans, e outras formas de software malicioso. Será utilizado um conjunto padronizado de arquivos de teste de malware para validar a capacidade do software de detectar, isolar e eliminar ameaças.

Compatibilidade com Aplicações Corporativas: Verificação da interação do antivírus com aplicações críticas e sistemas de gestão utilizados pela instituição. O objetivo é garantir que o software de segurança não interfira no funcionamento de programas essenciais ou cause falhas de compatibilidade com outros softwares corporativos.

Atualizações e Capacidade de Resposta: Avaliação da frequência e facilidade de atualização das definições de vírus e do motor de análise. Serão analisadas as opções de atualização automática e manual e a capacidade do sistema de se atualizar rapidamente para responder a novas ameaças.

Controle e Gerenciamento Centralizado: Teste de integração com plataformas de gestão centralizada, onde o software deve ser capaz de ser monitorado e controlado remotamente, permitindo a configuração de políticas de segurança, geração de relatórios e aplicação de atualizações em toda a rede, de acordo com os requisitos institucionais.

Relatórios de Segurança e Auditoria : Verificação da capacidade do software de gerar relatórios detalhados sobre eventos de segurança, tentativas de acesso não autorizado,

ataques bloqueados e outras atividades relevantes. O sistema deve permitir a extração de dados de auditoria de forma clara e acessível para o acompanhamento e a gestão de segurança.

Suporte a Políticas de Privacidade e Conformidade com Regulamentações: Avaliação de conformidade com normas de proteção de dados e segurança da informação, incluindo a LGPD (Lei Geral de Proteção de Dados). Esses testes serão aplicados com o objetivo de assegurar que o antivírus ofertado possui qualidade, desempenho e segurança necessários para proteger o ambiente de TI da Administração Pública, conforme especificado no edital.

6.5. As licenças de amostras (lotes 1 e 2) deverão ser exatamente iguais às versões que serão fornecidas em volume.

6.6. Após a realização dos testes do item 6.4 para os lotes específicos, as licenças de amostra poderão ser desativadas pelo licitante junto à Unidade Gestora da Contratação (Diretoria de Suporte e Manutenção).

6.7. As amostras serão analisadas pela equipe da Unidade Gestora da Contratação (Superintendência de Tecnologia da Informação - Squad segurança), sob supervisão de seu Coordenador.

6.8. As amostras da licença de antivírus poderão ser dispensadas, a pedido da CONTRATANTE, nas seguintes situações, conforme decisão do setor técnico ou demandante:

Apresentação de Parecer ou Laudo Técnico: Caso o licitante apresente parecer ou laudo técnico independente que ateste a qualidade do produto, indicando que ele atende integralmente às especificações e requisitos definidos no edital. O laudo deve ser emitido por instituição ou profissional reconhecido, garantindo que o software foi avaliado de acordo com normas e padrões de segurança e desempenho.

Participação de um Único Licitante no Certame : Quando houver apenas uma empresa participante na licitação e o produto ofertado for previamente conhecido pelo setor técnico, desde que o software já tenha sido utilizado anteriormente pela Administração e tenha demonstrado ser confiável, seguro e adequado às necessidades institucionais. Nesse caso, a experiência anterior pode ser considerada suficiente para dispensar o teste de amostra.

Outros Casos de Justificativa Técnica Documentada: O setor técnico ou demandante poderá dispensar a apresentação da amostra mediante justificativa formal, documentando que o software é amplamente conhecido, tem reputação comprovada no
mercado e atende a certificações de segurança de referência internacional, garantindo que ele cumpre com os requisitos essenciais para o uso institucional.

Observa-se que, caso o teste de amostra seja solicitado, qualquer licitante poderá acompanhar a análise, assegurando a transparência do processo. Essa prática visa garantir que todos os participantes tenham acesso às informações e procedimentos realizados na avaliação, reforçando a lisura e o caráter técnico da análise.

6.9. O teste da amostra terá duração máxima de 15 (quinze) dias a contar da ativação das licenças que serão utilizadas. Após este procedimento a CONTRATANTE emitirá um laudo técnico da aprovação ou desaprovação do produto.

6.10. O edital oferecerá maior detalhamento das regras que serão aplicadas em relação à exigência de amostra.

Membro 01 da Equipe responsável pela análise (servidor): FLAVIO HENRIQUE EVARISTO GOMES.
Membro 02 da Equipe responsável pela análise (servidor): THIAGO DIAS DE MATOS DINIZ.
Membro 03 da Equipe responsável pela análise (servidor): MATHEUS HORTA PIRES

7 - DA VISTORIA TÉCNICA:

Não se aplica.

8 - DOS CRITÉRIOS DE ACEITABILIDADE DA PROPOSTA:

8.1 - ATESTADOS E CERTIFICADOS ESPECÍFICOS AO OBJETO:

Não há necessidade de atestados ou certificados.

8.2 - EXIGÊNCIA DE CATÁLOGO, PROSPECTO OU FOLDER:

O licitante deverá apresentar, junto com a proposta, catálogo, prospecto ou folder, para permitir a verificação da compatibilidade do fabricante da solução, do modelo/versão da licença e do tipo de licenciamento com as especificações técnicas exigidas no edital.

9 - DA FORMA E DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR / DOS ATESTADOS DE CAPACIDADE:

9.1 - FORMA DE SELEÇÃO E CRITÉRIO DE JULGAMENTO DO FORNECEDOR:

Trata-se de serviço considerado de natureza comum, tendo em vista que envolve a aquisição e instalação de um software padronizado, amplamente comercializado e utilizado no mercado, com funcionalidades bem definidas e comparáveis entre diferentes fornecedores. Esse tipo de serviço não exige customizações significativas ou especificações técnicas altamente complexas para atender às necessidades da maioria dos usuários, seja em ambientes corporativos ou governamentais.

Desse modo, o fornecedor provavelmente será selecionado por meio do procedimento de licitação, na modalidade pregão, sob a forma eletrônica, com adoção do critério de julgamento pelo MENOR PREÇO.

9.2 - QUALIFICAÇÃO TÉCNICO-OPERACIONAL E TÉCNICO-PROFISSIONAL:

9.2.1. Não há necessidade de qualificação ou atestado de capacidade.

10 - DA SUBCONTRATAÇÃO:

Não é admitida a subcontratação do objeto.

11 - DAS GARANTIAS:

11.1 - GARANTIA DE EXECUÇÃO CONTRATUAL:

11.1.1. Não haverá exigência da garantia de execução contratual para este objeto, pelas razões a seguir justificadas:

Natureza da Contratação: A contratação de licença de antivírus por subscrição não envolve a entrega de bens tangíveis nem a execução de um serviço com complexidade técnica elevada. Trata-se de uma solução digital padronizada, onde os riscos associados ao fornecimento são mínimos, uma vez que o acesso ao software é concedido por meio de uma licença, e o próprio fornecedor mantém a responsabilidade pela manutenção e atualização contínua do serviço durante o período de subscrição.

Baixo Risco de Inexecução: Como o produto é entregue de forma digital (por download ou ativação de chave), não há atividades ou intervenções complexas para o fornecedor após a ativação da licença. Isso reduz significativamente a possibilidade de inexecução parcial ou total do contrato. Além disso, a renovação da subscrição ocorre automaticamente ou mediante pagamento, garantindo continuidade.

Economia Administrativa: A exigência de garantia de execução envolve custos adicionais tanto para a contratada quanto para a Administração, os quais não se justificam no caso de uma licença de software por subscrição. Esses custos podem ser evitados, reduzindo o impacto financeiro da contratação.

Previsibilidade do Objeto: O escopo da licença de antivírus é previsível e amplamente definido, o que facilita a avaliação de conformidade com os requisitos técnicos estabelecidos no edital, dispensando a necessidade de garantias financeiras para cobrir eventuais riscos contratuais.

Dessa forma, considerando o baixo risco de execução, a simplicidade do objeto e a economia para ambas as partes, a exigência de garantia de execução não se mostra necessária para a aquisição de licença de antivírus por subscrição.

11.2 - GARANTIA DO PRODUTO/SERVIÇO - FABRICANTE, LEGAL OU CONVENCIONAL:

11.2.1 A garantia do software para os LOTES 1 e 2, tratando-se de subscrição, será válida durante toda a vigência contratual, definida no item 15.1 deste Termo de Referência e será prestada pelo fabricante da solução. O fornecedor deve assegurar a continuidade do suporte técnico e das atualizações durante o prazo de vigência da licença, conforme estipulado na proposta e nos termos da contratação.

11.2.2 A garantia, em caso de renovação contratual, ou aditivos, deverá ser prestada de forma automática, ou seja, não deverá sofrer interrupção e o quantitativo será válido até o fim do prazo contratual.

11.2.3 O atendimento do serviço de suporte técnico da garantia deverá ser feito por intermédio da CONTRATADA ou diretamente com a fabricante através de portal específico para fins de suporte ou por e-mail.

11.2.4 A garantia técnica deverá ser acionada nas situações específicas nas quais a CONTRATADA não conseguir solução para um problema relacionado à solução contratada ou quando problema for detectado em relação aos elementos da solução contratada. A garantia técnica deverá incluir o fornecimento das atualizações do fabricante para a solução, as quais deverão ser fornecidas independente de solicitação da CONTRATANTE, e deverão compreender a remediação de vulnerabilidades eventualmente identificadas em qualquer componente da solução. Incluirá, adicionalmente, disponibilização de: atualizações, patches, correções, updates, fixes, service packs, upgrades, builds, novas funcionalidades e novos

módulos; esclarecimento de dúvidas; manuais dos produtos e serviços ofertados; base de conhecimento para soluções conhecidas e canal de comunicação.

11.2.5 As informações prestadas deverão ser disponibilizadas preferencialmente no idioma português, ou, na falta deste, obrigatoriamente no idioma inglês.

11.2.6 Em caso de lançamento de novas versões da solução lançadas pelo fabricante ou de novos softwares em substituição da solução contratada (descontinuação do software fornecido), o CONTRATANTE deverá receber a nova solução sem qualquer custo adicional.

11.2.7 Toda e qualquer ação realizada pela CONTRATADA no ambiente da CONTRATANTE só poderá ser realizada com anuência e autorização da CONTRATANTE e por meio de acompanhamento de representante indicado para tal fim.
11.2.8 Para cada serviço técnico prestado a CONTRATADA deverá fornecer um identificador para a chamada realizada, acompanhando o nome do responsável pelo tratamento do chamado.

11.2.9 Deve ser fornecida assistência técnica com resposta, no mínimo, 8x5 (horário comercial), para manutenção durante o período de garantia.

11.2.10 A CONTRATADA deve oferecer canais de suporte diversos, incluindo linha telefônica gratuita, e-mail e acesso remoto, com documentação completa de todos os chamados e manutenções.

11.2.11. Relativamente ao prazo de atendimento em caso de acionamento da garantia e suporte técnico, o prazo será de 24 (vinte e quatro) horas para Requisição e de 08 (oito) horas para incidente. Entende-se como Requisição a solicitação feita pelo cliente à equipe da CONTRATADA, que não cause impacto ao negócio. Entende-se como incidente qualquer evento não planejado, na solução contratada, que possa causar uma interrupção parcial ou total da ferramenta ou do ambiente da CONTRATANTE.

12 - DA MANUTENÇÃO E ASSISTÊNCIA TÉCNICA:

12.1. INSTALAÇÃO, ATIVAÇÃO E ACEITE DO SERVIÇO:

12.1.1. A CONTRATADA deverá participar do processo de implantação (rollout) de 30 (trinta) agentes de antivírus para o LOTE 1 e 10 (dez) agentes para o LOTE 2.

12.1.1.1. O suporte técnico do fabricante ou parceiro será fornecido na fase inicial, abrangendo a customização do agente, o encapsulamento e a instalação remota utilizando o software do CONTRATANTE, com base em linhas de comando definidas pelo fabricante da solução contratada.

12.1.1.1.1. Todas as despesas relacionadas ao serviço base de implantação serão de responsabilidade exclusiva da CONTRATADA e deverão estar inclusas nas condições comerciais do licenciamento.

12.1.1.2. Compete à CONTRATADA estabelecer os parâmetros necessários para a correta instalação remota e silenciosa do agente no cliente. A operacionalização do software de controle de ativos será de responsabilidade do CONTRATANTE.

12.1.1.3. Considera-se instalado o agente cuja conexão ou estado ativo apareça no painel de gestão centralizada da solução.

12.1.2. Após o recebimento das licenças contratadas para cada LOTE, a CONTRATADA terá o prazo de 15 (quinze) dias para concluir o suporte inicial relacionado ao serviço de implantação

descrito no item 12.1.1.

12.1.2.1. O aceite do serviço de subscrição das licenças dos lotes será dado ao final da etapa de implantação (rollout), item 12.1.1.

12.1.3. A desinstalação do agente antivírus do contrato anterior será realizada exclusivamente pela CONTRATANTE.

13 - DO MODELO DE EXECUÇÃO DO OBJETO:

13.1 - PRAZO DE ENTREGA / EXECUÇÃO E PRAZO DE SUBSTITUIÇÃO / REFAZIMENTO:

13.1.1 - PRAZO DE ENTREGA / EXECUÇÃO:

LOTES 1 e 2:

13.1.1.1. O prazo de entrega das licenças de subscrição deverá ocorrer em no máximo 15 (quinze) dias corridos, contados do recebimento pela contratada da Ordem de Serviço, em entrega única.

13.1.1.2. As licenças demandadas serão entregues em uma única vez no ambiente tecnológico do Contratante, na forma de uma mídia virtual (ISO ou similar) e/ou chave de ativação do licenciamento, contendo os softwares certificados. As informações para acesso à mídia virtual e/ou chave de ativação deverão ser passadas por e-mail a endereço acordado com a CONTRATADA em reunião de Kick-Off.

13.1.1.3. A ativação das licenças será realizada somente após a conclusão da montagem da infraestrutura de administração de licenças da CONTRATANTE (Tenant), cuja finalização deverá ser previamente comunicada pela CONTRATADA.

13.1.1.4. A capacitação, incluída no fornecimento de cada lote, deverá ser iniciada após a entrega completa da solução e deverá ser concluída no prazo máximo de 40 (quarenta) dias a partir do recebimento pela contratada da Ordem de Serviço (OS).

13.1.2 - PRAZO DE SUBSTITUIÇÃO / REFAZIMENTO:

O prazo de substituição/refazimento do objeto é de 07 (sete) dias corridos, a partir da solicitação da Contratante.

13.2 - LOCAL DE ENTREGA / DE PRESTAÇÃO DE SERVIÇOS:

13.2.1. As licenças serão fornecidas à Superintendência de TI (STI) da Procuradoria-Geral de Justiça, no seguinte endereço: Av. Álvares Cabral, 1740, 4º andar - Santo Agostinho, Belo Horizonte/MG. CEP: 30170916.

13.2.1.1. O fornecimento das licenças deve incluir o acesso a um portal de gerenciamento online, por meio do qual a Administração poderá monitorar as licenças, realizar ativações, desativações e ajustes nas configurações do antivírus, conforme necessário.

13.3 - CRITÉRIOS DE RECEBIMENTO:

13.3.1. O recebimento e o aceite do objeto dar-se-ão da forma seguinte:

a) Provisoriamente: em até 15 (quinze) dias, do recebimento da nota fiscal respectiva, após a execução do serviço de implantação (item 12.1.2 do Termo de Referência), pela DIRETORIA DE SUPORTE E MANUTENÇÃO (DSMT) ou por servidor designado, mediante termo detalhado, sem prejuízo da posterior verificação da perfeição e da conformidade do resultado do serviço prestado com as exigências deste Termo de Referência, nos termos explicitados na alínea seguinte;

b) Definitivamente: em até 05 (cinco) dias, contados do recebimento provisório da nota fiscal, pela DSMT ou por servidor designado, com a conferência da perfeição e qualidade do resultado do serviço prestado, atestando sua conformidade e total adequação ao objeto contratado, mediante termo detalhado, com o consequente encaminhamento da nota fiscal à Diretoria de Administração Financeira - DAFI, para análise e pagamento, após os registros pertinentes em sistema próprio.

14 - DOS CRITÉRIOS DE MEDIÇÃO E PAGAMENTO:

14.1 - CRITÉRIOS DE MEDIÇÃO:

14.1.1. A CONTRATADA deverá prestar os serviços contratados de acordo com todas as regras e procedimentos estabelecidos neste Termo de Referência, de forma eficiente e qualificada, entregando à CONTRATANTE:

I) O quantitativo total de licenças informados no Lote 1 e no Lote 2;

II) Ativação completa do licenciamento para o prazo contratado;

III) Fornecimento de capacitação para uso satisfatório das soluções a serem disponibilizadas no Lote 1 e no Lote 2 (um para cada lote), conforme item 1.2.4 do TR;

IV) Suporte e assistência inicial com a implantação;

V) Manter o suporte e a garantia durante todo o período de vigência contratual.

14.2 - CRITÉRIOS DE PAGAMENTO:

14.2.1. O pagamento será realizado em até 30 (trinta) dias após o recebimento da nota fiscal (ou documento equivalente), correspondente ao valor da parcela única, referente ao total de licenças de cada lote, com validade de 36 meses, conforme os critérios a seguir:

a) A Contratada apresentará à Contratante, após a ativação das licenças de software no tenant de administração e a execução da implantação inicial, a respectiva nota fiscal (ou documento equivalente) emitida em nome da Procuradoria-Geral de Justiça, CNPJ nº 20.971.057/0001-45, Av. Álvares Cabral, 1.690, bairro Santo Agostinho, Belo Horizonte, MG, constando, em seu corpo, o nome do setor solicitante (DIRETORIA DE SUPORTE E MANUTENÇÃO), local de entrega, número do contrato, número do empenho, elementos caracterizadores do objeto, bem como seus dados bancários para pagamento;

b) Recebida a nota fiscal (ou documento equivalente), o fiscal do contrato terá o prazo de 10 (dez) dias úteis para encaminhá-la à Diretoria de Administração Financeira (DAFI/Gestão) para pagamento, via SEI, em processo próprio (Tipo: Gestão Orçamentária e Financeira – Processo de Pagamento) acompanhada do atestado de nota fiscal (ou documento equivalente) e do formulário de encaminhamento de documento fiscal. O processo de pagamento iniciado deverá estar relacionado ao processo da contratação respectivo;

c) Recebido o processo de pagamento, constatada a sua regularidade, a DAFI terá o prazo de até 09 (nove) dias úteis para efetuar o pagamento, efetuando a retenção tributária, quando a legislação assim a exigir;

d) No caso da não aprovação da nota fiscal (ou documento equivalente) por motivo de incorreção, rasura, imprecisão ou circunstância que impeça a liquidação da despesa, ela será devolvida à Contratada para a devida regularização, reiniciando-se os prazos para aceite e consequente pagamento a partir da reapresentação da nota fiscal (ou documento equivalente) devidamente regularizada;

e) Ocorrendo atraso na entrega/substituição do objeto, a Contratada deverá anexar à respectiva nota fiscal (ou documento equivalente) justificativa e documentação comprobatória dos motivos alegados;

f) Na hipótese precedente, a Contratante efetuará o pagamento pertinente, retendo o valor de eventual multa por atraso, até a conclusão do Processo Administrativo instaurado para avaliação do descumprimento e da justificativa apresentada;

g) O valor eventualmente retido será restituído à Contratada caso a justificativa apresentada seja julgada procedente, sendo convertido em penalidade caso se conclua pela improcedência da justificativa;

h) Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao CAGEF para: 1) verificar a manutenção das condições de habilitação exigidas no edital; 2) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

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

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

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

14.2.2. Para viabilizar a passagem de conhecimento mencionada no item 1.2.4 deste Termo de Referência e atender ao prazo estabelecido no item 1.2.4.4, torna-se necessário antecipar o pagamento, sendo esta uma condição indispensável para a execução do serviço, conforme disposto no §1º do art. 145 da Lei 14.133/21. Ressaltamos que as licenças deverão estar devidamente ativadas e em pleno funcionamento, de modo a permitir que a transferência de conhecimento seja realizada com os dados e configurações do CONTRATANTE, evitando, assim, que o prazo estipulado para o minitreinamento gere ônus indevido ao CONTRATADO. Informamos, ainda, que o treinamento é parte integrante do fornecimento de cada lote, não se tratando de um serviço independente com condições de pagamento diferenciadas.

15 - DA VIGÊNCIA CONTRATUAL E DA POSSIBILIDADE DE PRORROGAÇÃO:

15.1. O prazo de vigência da contratação é de 36 (trinta e seis) meses contados a partir da data da publicação do instrumento no Diário Oficial do Ministério Público de Minas Gerais, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021. Trata-se de serviço de natureza continuada, sendo a vigência plurianual mais vantajosa, enquadrando-se no inciso XXVII (serviços de disponibilização de acesso a softwares comercializados mediante subscrição) da Instrução Normativa PGJAA n.º 2, de 8 de setembro de 2021.

15.2. Maior detalhamento das regras que serão aplicadas em relação à vigência da contratação será estabelecido no contrato.

16 - DAS OBRIGAÇÕES DA CONTRATADA E DO CONTRATANTE:

16.1. As obrigações contratuais gerais serão estabelecidas em contrato.

17- DO MODELO DE GESTÃO DO CONTRATO:

17.1. A forma de comunicação entre os gestores ou fiscais da Contratante e o preposto da Contratada será realizada preferencialmente por meio de correspondência eletrônica, com endereço de e-mail informado previamente e/ou cadastrado em seu banco de dados.

17.1.1. Nos casos de solicitações de fornecimento/serviço, de refazimento, comunicação sobre decisão de pedido de dilação de prazo, pedido de alteração contratual pelo contratado, considerar-se-á realizada a comunicação no dia que em que o destinatário confirmar o recebimento;

17.1.2. Presumir-se-á recebida a comunicação cuja confirmação não for realizada no prazo de 5 (cinco) dias úteis.

17.2. Nos casos de notificações e intimações relacionadas a ocorrências na execução contratual, decisões administrativas proferidas em sede de processo administrativo e decisão acerca de pedido de reequilíbrio, a forma de comunicação será realizada, preferencialmente, de forma eletrônica pelo Sistema Eletrônico de Informações (SEI-MPMG), por meio de prévio cadastro do contratado como usuário externo.

17.2.1. Considerar-se-á realizada a comunicação no dia em que o usuário externo proceder à consulta eletrônica de seu teor;

17.2.2. Na hipótese do inciso anterior, a comunicação será considerada realizada no primeiro dia-útil seguinte, quando a consulta ocorra em dia não-útil;

17.2.3. A consulta referida nos itens anteriores deverá ser feita em até 10 (dez) dias corridos, contados da data do encaminhamento de correspondência eletrônica ao usuário externo, sob pena de considerar-se automaticamente realizada na data do término desse prazo.

17.3. As Partes desde já acordam que terão pleno vigor e produzirão seus efeitos, inclusive como prova documental, todos os documentos e correspondências trocados entre as Partes, na vigência do presente Contrato e eventuais aditivos, desde que a comunicação seja feita de acordo com os itens acima.

17.4. A Contratante não se responsabilizará por qualquer inconsistência nos dados do endereço de e-mail fornecido pela Contratada.

18 - DAS INFRAÇÕES E DAS SANÇÕES ADMINISTRATIVAS:

18.1. Comete infração administrativa, nos termos do art. 155 da Lei nº 14.133, de 2021, o contratado que:

a. der causa à inexecução parcial 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;

c. der causa à inexecução total do contrato;

d. ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

e. apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

f. praticar ato fraudulento na execução do contrato;

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

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

18.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

a) Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

b) Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem 18.1, sempre que não se justificar a imposição de penalidade mais grave;

c) Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem 18.1, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave;

d) Multa:

d.1) ATÉ TRINTA DIAS DE ATRASO INJUSTIFICADO NA EXECUÇÃO/REFAZIMENTO DO SERVIÇO/DA ENTREGA DO OBJETO: multa moratória de 0,5% (cinco décimos por cento) por dia, calculada sobre o valor do contrato, a partir do primeiro dia útil subsequente ao do vencimento do prazo estipulado para cumprimento da obrigação;

d.2) MAIS DE TRINTA DIAS DE ATRASO INJUSTIFICADO NA EXECUÇÃO/REFAZIMENTO DO SERVIÇO/ DA ENTREGA DO OBJETO: multa moratória de 10% (dez por cento), calculada sobre o valor do contrato;

d.3) NÃO-EXECUÇÃO/REFAZIMENTO DO SERVIÇO/ DA ENTREGA DO OBJETO: multa compensatória de 30% (trinta por cento), calculada sobre o valor do contrato, aplicável a partir do primeiro dia útil subsequente ao do vencimento do prazo para cumprimento das obrigações, sem embargo de indenização dos prejuízos porventura causados à Contratante;

d.4) DESCUMPRIMENTO DE OBRIGAÇÃO ACESSÓRIA PREVISTA EM QUALQUER ITEM DESTE INSTRUMENTO: multa compensatória de 0,5% (cinco décimos por cento) por dia, calculada sobre o valor do contrato e limitada a 30% (trinta por cento) desse valor, contada da comunicação da Contratante (via internet, correio etc.), até cessar a inadimplência;

18.3. A inexecução parcial ou total do contrato, bem como o não cumprimento ou cumprimento irregular de suas condições por parte da Contratada poderá implicar a sua extinção unilateral, nos termos dos arts. 137, inciso I, e 138, inciso I, da Lei Federal nº 14.133/2021, com aplicação das penalidades cabíveis, mediante a instauração do devido processo administrativo, resguardando-se aos interessados o direito ao contraditório e a ampla defesa, consoante o disposto na Lei nº 14.133/2021, regulamentada pela Resolução PGJ nº 02, de 16 de fevereiro de 2023;

18.4. Ocorrida a extinção pelo motivo retrocitado, a Contratante poderá contratar o remanescente, com fulcro no art. 90, § 7º da Lei nº 14.133/2021;

18.5. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante;

18.6. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa;

18.7. Ocorrendo atraso de pagamento por culpa exclusiva da Administração, o pagamento será acrescido de atualização financeira, entre as datas do vencimento e do efetivo pagamento, de acordo com a variação pro rata tempore do IPCA, ou outro índice que venha substituílo, conforme a legislação vigente;

18.8. Na hipótese de a Contratada incorrer em algum dos atos previstos como infrações administrativas na Lei Federal nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos do art. 5º, inciso IV, da Lei Federal nº 12.846, de 2013, ficará sujeita às penalidades descritas no art. 6º daquele diploma legal;

18.9. As penalidades previstas na alínea acima serão aplicadas segundo os critérios estabelecidos nos arts. 6º e 7º da Lei Federal nº 12.846/13 e nos arts 20 a 27 do Decreto Federal nº 11.129/2022, resguardado à Contratada o direito ao devido processo legal e à ampla defesa;

18.10. 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 e a ampla defesa;

18.11. 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 de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual (CAFIMP);

18.12. 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 Federal nº 14.133/21.

19 - DAS INFORMAÇÕES COMPLEMENTARES:

19.1. DO MAPEAMENTO DE RISCO

Para o presente objeto, não se vislumbram riscos específicos relevantes a serem mapeados. Não se trata de hipótese em que a lei trate como obrigatório o mapeamento específico ou a elaboração de cláusula de matriz de riscos. Nos termos do art. 18, inciso X, da Lei 14.133/21, a Superintendência de Gestão Administrativa, com apoio da Diretoria-Geral, do Escritório de Integridade e da Auditoria Interna, está realizando o mapeamento genérico dos riscos que possam comprometer o sucesso das licitações e a boa execução contratual (que será oportunamente juntado aos processos de contratação, após sua conclusão e validação).

Tendo por referência também o art. 22, §3°, da nova lei de licitações, cabe destacar, ainda, que não se trata de contratação de obra, serviço de grande vulto ou em que seja adotado regimes de contratação integrada ou semi-integrada, e nem das hipóteses contempladas no art. 1º da Deliberação Conjunta CEGEC/CEINT n° 01/24.

20 - UNIDADE ADMINISTRATIVA RESPONSÁVEL:

Unidade Administrativa Responsável: DIRETORIA DE SUPORTE E MANUTENÇÃO - 1091038.

Servidor Gerenciador/Fiscal do Contrato: Thiago Dias de Matos Diniz

Servidor Gerenciador/Fiscal Suplente do Contrato: Matheus Horta Pires

21 - DA PROTEÇÃO E DO TRATAMENTO DE DADOS:

21.1. É dever das PARTES observar e cumprir as regras impostas pela Lei Geral de Proteção de Dados (Lei n.º 13.709/18), suas alterações e regulamentações posteriores, bem como as diretrizes estabelecidas pela Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no Ministério Público (Resolução n.º 281/2023, do Conselho Nacional do Ministério Público – CNMP), devendo ser observadas, no tratamento de dados, a respectiva finalidade específica e a consonância ao interesse público.

21.2. O CONTRATANTE assume o papel de controlador, nos termos do artigo 5º, VI, da Lei n.º 13.709/2018, e a CONTRATADA assume o papel de operador, nos termos do artigo 5º, VII, da Lei n.º 13.709/2018.

21.3. A CONTRATADA deverá guardar sigilo sobre os dados pessoais compartilhados pelo CONTRATANTE e só poderá fazer uso dos dados exclusivamente para fins de cumprimento do objeto, sendo-lhe vedado, a qualquer tempo, o compartilhamento desses dados sem a expressa autorização do CONTRATANTE, ou o tratamento dos dados de forma incompatível com as finalidades e prazos acordados, sob pena de responsabilização administrativa, civil e criminal.

21.4. É dever da CONTRATADA orientar e treinar seus empregados e colaboradores sobre os deveres, requisitos e responsabilidades decorrentes das leis e regulamentos de proteção de dados pessoais.

21.5. A CONTRATADA se compromete a adequar todos os procedimentos internos e adotar as medidas de segurança técnicas, administrativas e operacionais necessárias a resguardar os dados pessoais que lhe serão confiados, levando em conta as diretrizes de órgãos reguladores, padrões técnicos e boas práticas existentes, incluindo as diretrizes da Resolução CNMP n.º 281/2023.

21.6. Quando solicitada, a CONTRATADA fornecerá ao CONTRATANTE todas as informações

necessárias para comprovar a sua conformidade com as obrigações referentes à proteção de dados pessoais, incluindo registros cronológicos ou outros métodos eficazes que demonstrem a licitude do tratamento e garantam a integridade e a segurança dos dados pessoais, devendo atender prontamente eventuais pedidos de comprovação formulados, respeitando-se o sigilo empresarial e as demais proteções legais.

21.7. A CONTRATADA cooperará com o CONTRATANTE no cumprimento das obrigações referentes ao exercício dos direitos dos titulares previstos na LGPD e nas leis e regulamentos de proteção de dados em vigor e, também, no atendimento de requisições de autoridades competentes ou quaisquer outros legítimos interessados.

21.8. Os dados pessoais obtidos a partir da contratação serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, sendo permitida a conservação para as finalidades estabelecidas no artigo 16 da Lei n.º 13.709/2018.

21.9. A CONTRATADA deverá comunicar ao CONTRATANTE, no prazo máximo de 72 (setenta e duas) horas, contados do seu conhecimento, qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Parágrafo único: A comunicação deverá ser enviada para o e-mail: encarregado@mpmg.mp.br, devendo trazer em seu bojo, no mínimo, as seguintes informações:

I - a descrição e a natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, observados os casos de sigilo legal e institucional;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

22 – DAS ESTIMATIVAS DO VALOR DA CONTRATAÇÃO:

A estimativa da despesa será oportunamente informada nos autos do processo pela DGCL, conforme Mapa de Preços a ser elaborado.

23 – DA ADEQUAÇÃO ORÇAMENTÁRIA:

A adequação orçamentária será oportunamente informada nos autos do processo pela DIOR.

AUTOR DO TERMO DE REFERÊNCIA (AGENTE DE PLANEJAMENTO DA CONTRATAÇÃO):

Nome: FLÁVIO HENRIQUE EVARISTO GOMES

Cargo: ANALISTA DE SUPORTE

Unidade Administrativa: DIRETORIA DE SUPORTE E MANUTENÇÃO - 1091038

APROVAÇÃO DO TERMO DE REFERÊNCIA:

Nome: ALEXSANDER BATISTA AGUIAR

Cargo: COORDENADOR II

Unidade Administrativa: DIRETORIA DE SUPORTE E MANUTENÇÃO - 1091038

[1] GARTNER, Inc; HINNER; PATNAIK; GRENIER; PATEL. Hype Cycle for Endpoint Security, 2023, p. 74.

[2] GARTNER, Inc; AGGIO, Jess; YOUNG, Danellie. Hype Cycle for Managed IT Services.

Assim ajustadas, as partes assinam o presente Contrato, para um só efeito de direito, por meio de senha/assinatura eletrônica, na presença de duas testemunhas.

Iraídes de Oliveira Marques

Procuradora-Geral de Justiça Adjunta Administrativa

CONTRATANTE

Walter F. da S. Júnior

Brasoftware Informática Ltda.

CONTRATADA

Testemunhas:

1)

2)

Documento assinado eletronicamente por **Walter Ferreira da Silva Junior**, **Usuário Externo**, em 25/06/2025, às 17:03, conforme art. 22, da Resolução PGJ n. 27, de 17 de dezembro de 2018.

Documento assinado eletronicamente por **IRAIDES DE OLIVEIRA MARQUES**, **PROCURADORA-GERAL DE JUSTICA ADJUNTA ADMINISTRATIVA**, em 25/06/2025, às 17:52, conforme art. 22, da Resolução PGJ n. 27, de 17 de dezembro de 2018.

Documento assinado eletronicamente por **MARIA JOSILENE DO AMARAL THOMAZ**, **OFICIAL DO MINIST. PUBLICO - QP**, em 25/06/2025, às 18:31, conforme art. 22, da Resolução PGJ n. 27, de 17 de dezembro de 2018.

Documento assinado eletronicamente por **MAIRA COSTA VAL FAJARDO**, **ANALISTA DO MINIST. PUBLICO - QP**, em 26/06/2025, às 09:58, conforme art. 22, da Resolução PGJ n. 27, de 17 de dezembro de 2018.

A autenticidade do documento pode ser conferida no site http://www.mpmg.mp.br/sei/processos/verifica, informando o código verificador **9063441** e o código CRC **2EEB0A54**.

AVENIDA ÁLVARES CABRAL, 1740 6º ANDAR - Bairro SANTO AGOSTINHO - Belo Horizonte/ MG
CEP 30170008 - - www.mpmg.mp.br