TERMO DE REFERÊNCIA

Data	Versão	Descrição	Autor
20/08/2026	1.0	Finalização da prévia do TR	Tatiane
11/09/2026	2.0	Ajustando - Finalização da prévia do TR	Tatiane / Lidiane
16/09/2026	3.0	Versão Pós Cotação	Lidiane
23/09/2026	4.0	Adequações conforme Parecer nº 733/2026/PGM/PELC	

TERMO DE REFERÊNCIA

1. DO OBJETO E CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Do Objeto

1.1.1. O presente Termo de Referência tem por objeto a contratação de Licenciamento de Software Antivírus corporativo de proteção integrada de endpoints, com recursos de Endpoint Protection Platform – EPP e Endpoint Detection and Response – EDR, contemplando licenciamento, gerenciamento centralizado, atualizações, suporte técnico e garantia pelo período de 36 (trinta e seis) meses, conforme as condições e exigências estabelecidas neste Termo de Referência e em seus anexos.

Tabela 1 - Itens da Contratação

Código	Especificação	Unidade	Quant.	Valor Unitário	Valor Total
1	Contratação de licenciamento de software antivírus corporativo para proteção integrada de endpoints, com recursos de Endpoint Protection Platform (EPP) e Endpoint Detection and Response (EDR), incluindo gerenciamento centralizado, atualizações, suporte técnico e garantia durante o período de 36 (trinta e seis) meses.	Licença de uso	2920	R$ 162,17	R$ 473.536,40

1.1.2. Cada licença deverá permanecer ativa durante todo o período de vigência contratual, contemplando, sem custos adicionais além do valor contratado, o acesso às atualizações das bases de detecção de ameaças, dos modelos de análise, dos agentes, dos mecanismos de proteção, dos componentes de EPP e EDR, das correções de segurança, dos aprimoramentos e das versões abrangidas pelo licenciamento contratado, bem como ao suporte técnico e à garantia da solução nas condições estabelecidas neste Termo de Referência.

1.1.3. A solução ofertada deverá atender integralmente a todos os requisitos técnicos mínimos estabelecidos neste Termo de Referência e no Anexo II – Especificações Técnicas Mínimas, mediante comprovação na forma definida no Apêndice A – Matriz de Comprovação dos Requisitos Técnicos.

1.2. Da natureza do objeto

1.2.1. O objeto da contratação caracteriza-se como serviço comum de tecnologia da informação e comunicação – TIC, cujos padrões de desempenho e qualidade podem ser objetivamente definidos por meio de especificações usuais de mercado, conforme demonstrado no Estudo Técnico Preliminar e detalhado neste Termo de Referência e no Anexo II – Especificações Técnicas Mínimas,

observadas as disposições da Lei Federal nº 14.133, de 1º de abril de 2021.

1.3. Dos parâmetros da licitação

1.3.1. Será adotado o Sistema de Registro de Preços (SRP)?

( ) SIM (x) NÃO

1.3.2. Haverá necessidade de vistoria prévia (visita técnica)?

( ) SIM (X) NÃO

1.3.2.1. Justifica-se a não exigência de vistoria técnica, tendo em vista que as informações necessárias à elaboração da proposta encontram-se descritas neste Termo de Referência e no Anexo II – Especificações Técnicas Mínimas, não sendo necessário o conhecimento presencial do ambiente para a formulação da proposta.

1.3.3. Será admitida a subcontratação?

( ) SIM (X) NÃO

1.3.3.1. Não será admitida a subcontratação parcial dos serviços, nos termos do art. 122 da Lei 14.133/21, tendo em vista que não se verifica a possibilidade de terceirizar parte dos serviços a outra empresa.

1.3.3.2. Não será considerado subcontratação o acesso da Administração aos serviços de atualização, garantia e suporte técnico prestados diretamente pelo fabricante ou por integrante de sua cadeia oficial, permanecendo a CONTRATADA integralmente responsável pelo cumprimento das obrigações assumidas.

1.3.4. Será admitida a participação de consórcios?

( ) SIM (X) NÃO

1.3.4.1. Não será admitida a participação de pessoas jurídicas em consórcio, considerando que o objeto possui escopo definido, é usualmente fornecido por empresas individualmente habilitadas no mercado e não demanda a conjugação de capacidades técnicas, econômicas ou operacionais de diferentes empresas para sua execução.

1.3.5. Será admitida a participação de cooperativas?

( ) SIM (X) NÃO

1.3.5.1. Não será admitida a participação de profissionais sob a forma de cooperativa, tendo em vista que para o objeto a ser licitado o próprio fabricante ou empresas autorizadas por ele, poderão participar. Nesse sentido, considera-se raro que cooperativas possuam tal autorização considerando ainda a especificidade do objeto.

1.3.6. Será exigida garantia contratual?

( ) SIM (X) NÃO

1.3.6.1. Não será exigida garantia da proposta, nos termos do artigo 58 da Lei Federal nº 14.133/2021, considerando a natureza do objeto e a ausência de circunstâncias concretas que justifiquem sua exigência.

1.3.7. Será exigida garantia da proposta?

( ) SIM (X) NÃO

Não será exigida garantia contratual, considerando a natureza do objeto, o fornecimento oficial das licenças e a ausência de circunstâncias concretas que justifiquem essa exigência.

1.4. Prazo da contratação

1.4.1. O prazo inicial de vigência da contratação será de 36 (trinta e seis) meses, contado a partir do primeiro dia útil subsequente à divulgação do contrato no Portal Nacional de Contratações Públicas – PNCP.

1.4.2. Considerada a natureza contínua do objeto, o contrato poderá ser prorrogado sucessivamente, observado o limite máximo de vigência previsto no art. 107 da Lei Federal nº 14.133/2021, desde que haja previsão no edital e no contrato e que a autoridade competente ateste que as condições e os preços permanecem vantajosos para a Administração. Na hipótese de prorrogação, é permitida a negociação com a CONTRATADA ou a extinção contratual sem ônus para qualquer das partes, nos termos do art. 107 da Lei Federal nº 14.133/2021.

1.4.3. As licenças deverão permanecer ativas durante toda a vigência contratual, inclusive em eventual período de prorrogação, contemplando as atualizações, o suporte técnico e os demais recursos previstos neste Termo de Referência e em seu Anexo de Especificações Técnicas Mínimas.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A presente contratação justifica-se pela necessidade de assegurar a continuidade da proteção dos ativos computacionais da Prefeitura Municipal de Dourados/MS, considerando o encerramento, em outubro de 2026, da vigência da solução de antivírus corporativa para proteção de endpoints atualmente utilizada pela Administração Municipal.

2.2. A centralização de dados em ambiente digital, a expansão da rede corporativa municipal, o aumento da dependência dos sistemas informatizados e a evolução das ameaças cibernéticas ampliam a exposição da infraestrutura tecnológica a incidentes capazes de comprometer a continuidade dos serviços públicos. Nesse contexto, torna-se necessária a nova contratação de software antivírus, com recursos de prevenção, detecção, investigação, contenção, resposta e remediação de ameaças.

2.3. A solução deverá proteger as estações de trabalho, notebooks e servidores da Administração Municipal contra códigos maliciosos, ransomware, ataques sem arquivo, exploração de vulnerabilidades e demais ameaças cibernéticas, bem como disponibilizar recursos de análise comportamental, correlação dos eventos associados às ameaças detectadas nos endpoints, análise de causa raiz, representação da cadeia de execução, investigação das ameaças detectadas, execução centralizada de ações de contenção, tratamento e remediação e integração com serviços de reputação e inteligência de ameaças do fabricante, conforme detalhado no Anexo II.

2.4. A adoção de recursos integrados de EPP e EDR, incluindo análise de causa raiz e representação da cadeia de execução das ameaças, justifica-se pela dimensão e diversidade do ambiente tecnológico municipal, composto por estações de trabalho, notebooks e servidores distribuídos entre os órgãos e unidades administrativas, bem como pela necessidade de reduzir o

tempo de identificação, investigação, contenção e remediação de incidentes.

2.5. O quantitativo de 2.920 (duas mil novecentas e vinte) licenças corresponde à manutenção da capacidade de proteção estabelecida no Contrato nº 296/2022, sem qualquer acréscimo para a nova contratação.

2.5.1. O quantitativo será utilizado de forma global na proteção de estações de trabalho, notebooks e servidores físicos ou virtuais compatíveis com a solução, distribuídos entre os órgãos e unidades da Administração Municipal, sem divisão prévia por categoria de equipamento.

2.5.2. Cada licença corresponderá à proteção simultânea de um endpoint, podendo ser realocada entre equipamentos durante a execução contratual, respeitado o limite máximo de 2.920 endpoints protegidos simultaneamente.

2.5.3. A solução deverá disponibilizar recursos de instalação remota, centralizada e silenciosa dos agentes, integração com o ambiente Microsoft Active Directory e Group Policy Objects – GPO, gerenciamento centralizado e apoio técnico à implantação, visando assegurar a efetiva distribuição, ativação e administração das licenças contratadas.

2.6. A fundamentação detalhada da necessidade, a análise das alternativas disponíveis no mercado, a justificativa do quantitativo e a demonstração da viabilidade técnica e econômica da contratação encontram-se consignadas no Estudo Técnico Preliminar que integra o respectivo processo administrativo.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

3.1. A Prefeitura Municipal de Dourados/MS possui infraestrutura tecnológica composta por estações de trabalho, notebooks e servidores que suportam a execução dos sistemas corporativos e a prestação dos serviços públicos digitais. Para garantir a segurança desses ativos, faz-se necessária a contratação de software antivírus corporativo para a proteção de endpoints, composta por recursos de EPP e EDR administrados por plataforma centralizada.

3.2. A solução deverá prover mecanismos de prevenção, detecção, investigação, contenção, resposta e remediação de ameaças cibernéticas, incluindo proteção contra vírus, malware, ransomware, ataques sem arquivo, exploração de vulnerabilidades e demais códigos ou comportamentos maliciosos, contribuindo para preservar a disponibilidade, a integridade e a confidencialidade das informações institucionais.

3.3. A solução como um todo compreenderá o fornecimento de 2.920 (duas mil novecentas e vinte) licenças de uso, agentes de proteção, componentes de EPP e EDR, console centralizada, análise comportamental, aprendizado de máquina, integração com serviços de reputação e inteligência de ameaças do fabricante e demais módulos necessários ao atendimento integral dos requisitos obrigatórios, bem como ativação, configuração inicial, apoio remoto à implantação, gerenciamento dos equipamentos, aplicação de políticas de segurança, atualizações e suporte técnico durante toda a vigência contratual.

3.4. O ciclo de vida da solução abrangerá sua implantação e ativação, utilização, administração, atualização e suporte durante os 36 (trinta e seis) meses de vigência contratual. Nesse período, deverão ser disponibilizadas, sem custos adicionais além do valor contratado, as atualizações das bases de detecção de ameaças, dos modelos de análise, dos agentes, dos mecanismos de proteção, dos componentes de EPP e EDR, das correções de segurança, dos aprimoramentos e das versões abrangidas pelo licenciamento contratado.

3.5. A contratação permitirá à Administração Municipal manter seus ativos computacionais protegidos por solução corporativa integrada e atualizada, com aplicação centralizada de políticas, monitoramento automatizado de atividades relevantes, correlação dos eventos associados às ameaças detectadas, investigação das detecções e execução de ações de contenção, tratamento e remediação.

3.6. Entre os principais benefícios esperados com a contratação, destacam-se:

3.6.1. Manutenção da proteção multicamada dos ativos de tecnologia da informação da Administração Municipal;

3.6.2. Ampliação da capacidade de detecção de ameaças avançadas, desconhecidas, comportamentais e sem arquivo;

3.6.3. Melhoria da visibilidade sobre eventos e detecções por meio da coleta de informações de segurança, da correlação dos eventos associados às ameaças e da representação da respectiva cadeia de execução;

3.6.4. Redução do tempo necessário para investigação, contenção e remediação de incidentes de segurança;

3.6.5. Execução centralizada de ações de contenção, tratamento e remediação das ameaças nos equipamentos protegidos;

3.6.6. Fortalecimento da proteção contra ransomware, inclusive mediante mecanismos de recuperação dos arquivos afetados;

3.6.7. Gerenciamento centralizado dos equipamentos protegidos, dos eventos, das detecções e das políticas de segurança;

3.6.8. Redução da necessidade de intervenções presenciais mediante recursos de implantação, gerenciamento e resposta remotos;

3.6.9. Contribuição para a continuidade dos serviços públicos digitais e para a proteção da integridade, disponibilidade e confidencialidade das informações institucionais.

3.7. As características funcionais e os requisitos de compatibilidade, gerenciamento, implantação, proteção multicamada, remediação de ransomware, EDR com análise de causa raiz e representação da cadeia de execução das ameaças, integração com serviços de reputação e inteligência de ameaças do fabricante, aprendizado de máquina, análise comportamental, atualização e comprovação técnica encontram-se detalhados no Anexo II – Especificações Técnicas Mínimas e no Apêndice A – Matriz de Comprovação dos Requisitos Técnicos deste Termo de Referência.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos do negócio

4.1.1. Fornecer 2.920 (duas mil novecentas e vinte) licenças de uso de solução corporativa integrada de proteção de endpoints, com recursos de EPP e EDR, incluindo atualizações, suporte técnico e garantia da solução durante o período de 36 (trinta e seis) meses.

4.1.2. As licenças deverão ser originais, regulares e válidas, disponibilizadas mediante licenciamento oficial do fabricante da solução ofertada, garantindo à Administração Municipal o direito de utilização durante todo o período contratado.

4.1.3. Todos os produtos, agentes, módulos, componentes e níveis de licenciamento necessários ao atendimento dos requisitos obrigatórios estabelecidos no Anexo II – Especificações Técnicas Mínimas deverão estar incluídos na proposta, sem necessidade de aquisição adicional pela Administração durante a vigência contratual.

4.1.4. Durante toda a vigência contratual, deverão estar incluídas as atualizações das bases de detecção de ameaças, dos modelos de análise, dos agentes, dos mecanismos de proteção, dos componentes de EPP e EDR, das correções de segurança, dos aprimoramentos e das versões abrangidas pelo licenciamento contratado, sem custos adicionais para a Administração.

4.1.5. A solução deverá ser compatível com a infraestrutura tecnológica da Prefeitura Municipal de Dourados/MS e permitir sua implantação, administração e operação centralizadas, observados os requisitos estabelecidos no Anexo II – Especificações Técnicas Mínimas.

4.1.6. A solução deverá disponibilizar mecanismos de prevenção, detecção, investigação, contenção, resposta e remediação de ameaças cibernéticas, incluindo proteção multicamada, análise comportamental, aprendizado de máquina, EDR com análise de causa raiz e representação da cadeia de execução das ameaças, remediação de ransomware e integração com serviços de reputação e inteligência de ameaças do fabricante, conforme estabelecido no Anexo II – Especificações Técnicas Mínimas.

4.1.7. A contratação deverá contemplar suporte técnico e garantia da solução durante toda a vigência contratual, sem custos adicionais para a Administração, observadas as condições mínimas estabelecidas no item 5.2 deste Termo de Referência e no Anexo II – Especificações Técnicas Mínimas.

4.1.8. A solução ofertada deverá atender integralmente às condições e às especificações técnicas mínimas estabelecidas neste Termo de Referência e no Anexo II – Especificações Técnicas Mínimas.

4.2. Da comprovação dos requisitos técnicos

4.2.1. A licitante provisoriamente classificada em primeiro lugar deverá apresentar a Matriz de Comprovação dos Requisitos Técnicos, conforme modelo constante do Apêndice A deste Termo de Referência, devidamente preenchida com a identificação da solução, da edição, do nível de licenciamento, dos módulos e dos componentes ofertados.

4.2.2. A matriz contemplará os blocos de requisitos considerados prioritários para a classificação técnica da solução, devendo a licitante indicar, para cada bloco, a documentação técnica oficial do fabricante que demonstre o atendimento às funcionalidades relacionadas.

4.2.3. Serão aceitos como documentação comprobatória:

4.2.3.1. Fichas Técnicas ou Datasheets;

4.2.3.2. Manuais Técnicos;

4.2.3.3. Guias de Instalação, Configuração ou Administração;

4.2.3.4. Matrizes oficiais de funcionalidades ou compatibilidade;

4.2.3.5. Catálogos Técnicos;

4.2.3.6. Bases oficiais de conhecimento; e

4.2.3.7. Páginas e Documentação disponibilizadas no portal oficial do fabricante.

4.2.4. A referência apresentada deverá identificar o título do documento e a página, seção, capítulo

ou tópico em que a informação possa ser localizada. Quando a comprovação estiver disponível na internet, deverá ser indicado o endereço eletrônico oficial do fabricante e a respectiva seção ou página.

4.2.5. Quando um bloco compreender mais de uma funcionalidade, poderão ser indicados diferentes documentos, páginas, seções ou endereços eletrônicos oficiais na mesma linha da matriz.

4.2.6. Não será considerada suficiente, para comprovação dos blocos prioritários, a simples declaração de atendimento emitida pela própria licitante, desacompanhada da documentação técnica oficial do fabricante.

4.2.7. A documentação apresentada deverá corresponder à solução, à edição e ao nível de licenciamento efetivamente ofertados, não sendo admitida a comprovação mediante funcionalidade pertencente exclusivamente a produto, módulo, componente ou licença não incluída na proposta.

4.2.8. A Administração poderá realizar diligências para esclarecer ou confirmar as informações apresentadas, inclusive mediante consulta à documentação oficial do fabricante, vedada a utilização da diligência para substituir a solução, a edição, os módulos ou o nível de licenciamento originalmente ofertados.

4.2.9. Não comprovado o atendimento de qualquer bloco prioritário da Matriz de Comprovação, após a análise da documentação apresentada e a realização das diligências eventualmente cabíveis, a solução ofertada não será aceita, observados os procedimentos estabelecidos no edital e na legislação aplicável.

4.2.10. A limitação da Matriz de Comprovação aos requisitos prioritários não afasta a obrigatoriedade de atendimento integral a todos os requisitos estabelecidos no Anexo II – Especificações Técnicas Mínimas, inclusive aqueles não individualizados no Apêndice A.

4.2.11. A licitante deverá declarar que todos os produtos, módulos, componentes e níveis de licenciamento necessários ao atendimento integral do Anexo II encontram-se incluídos na proposta apresentada, sem necessidade de aquisição adicional pela Administração.

5. EXECUÇÃO DO OBJETO

5.1. Condições gerais:

5.1.1. A CONTRATADA deverá disponibilizar as 2.920 (duas mil novecentas e vinte) licenças no prazo máximo de 15 (quinze) dias corridos após o recebimento da Ordem de Fornecimento emitida pela CONTRATANTE.

5.1.2. As licenças deverão ser fornecidas em formato digital, mediante disponibilização no portal oficial do fabricante ou encaminhamento das informações necessárias ao endereço eletrônico institucional indicado pela CONTRATANTE.

5.1.3. A disponibilização das licenças deverá ser comprovada por documento emitido pela CONTRATADA, pelo distribuidor autorizado ou pelo fabricante, ou mediante consulta ao portal oficial da solução, devendo ser possível verificar, no mínimo:

5.1.3.1. A identificação da Prefeitura Municipal de Dourados/MS como titular ou beneficiária do licenciamento;

5.1.3.2. O fabricante, o nome comercial, a edição, o nível de licenciamento e, quando identificáveis no documento ou no portal oficial da solução, os módulos e componentes fornecidos;

5.1.3.3. A quantidade de 2.920 (duas mil novecentas e vinte) licenças;

5.1.3.4. O período de validade do licenciamento; e

5.1.3.5. O direito de acesso às atualizações e ao suporte técnico incluído na contratação durante toda a vigência contratual.

5.1.4. A solução disponibilizada deverá corresponder integralmente àquela indicada na proposta aceita e na Matriz de Comprovação dos Requisitos Técnicos, inclusive quanto ao produto, à edição, ao nível de licenciamento, aos módulos e aos componentes ofertados.

5.1.5. As licenças deverão ser disponibilizadas regularizadas, ativas ou aptas à ativação e suficientes para utilização de todos os recursos obrigatórios, sem necessidade de aquisição adicional de produto, módulo, componente ou licença pela Administração.

5.1.6. O período de validade das licenças deverá assegurar à CONTRATANTE 36 (trinta e seis) meses integrais de utilização, contados da data de sua efetiva disponibilização pela CONTRATADA, não sendo admitida a entrega de licenças cujo prazo de validade tenha se iniciado anteriormente.

5.1.7. A CONTRATADA deverá prestar apoio técnico remoto à equipe da CONTRATANTE durante a fase inicial de ativação, configuração e implantação da solução, abrangendo, quando solicitado pela CONTRATANTE:

a) orientação para ativação e disponibilização das licenças;
b) orientação para configuração inicial da console de gerenciamento;
c) orientação para criação ou ajuste inicial das políticas de segurança;
d) orientação para definição dos pacotes e dos parâmetros de instalação dos agentes;
e) orientação para integração da solução com o ambiente tecnológico da CONTRATANTE;
f) apoio à configuração dos mecanismos de implantação remota, silenciosa e centralizada;
g) apoio à validação da comunicação entre os agentes e a console de gerenciamento;
h) orientação para remoção ou substituição da solução anteriormente instalada, observadas as ferramentas e os procedimentos oficialmente disponibilizados pelos respectivos fabricantes; e
i) apoio ao diagnóstico de falhas diretamente relacionadas à ativação, à configuração inicial e à comunicação dos agentes durante a fase de implantação.

5.1.8. A implantação dos agentes nos equipamentos será executada pela equipe técnica da CONTRATANTE, utilizando os mecanismos de instalação remota, silenciosa e centralizada disponibilizados pela solução, com apoio técnico remoto da CONTRATADA durante a fase inicial de implantação, quando solicitado pela CONTRATANTE.

5.1.9. A CONTRATADA deverá realizar repasse de conhecimento por meio remoto, durante a etapa de configuração inicial, para que a equipe da CONTRATANTE possa iniciar a administração da solução.

5.1.10. A CONTRATADA deverá realizar repasse de conhecimento complementar da solução, quando solicitado, durante a vigência contratual, por meio remoto e sem custos adicionais.

5.1.11. O repasse de conhecimento deverá abranger orientações sobre:

5.1.11.1. Acesso e utilização básica da console;
5.1.11.2. Aplicação e alteração de políticas de segurança;
5.1.11.3. Acompanhamento da situação dos endpoints;
5.1.11.4. Consulta de detecções, eventos, alertas e relatórios;
5.1.11.5. Execução das principais tarefas administrativas, de tratamento e de remediação disponíveis na solução; e

5.1.11.6. Abertura e acompanhamento de chamados de suporte.

5.1.12. O repasse de conhecimento não será caracterizado como treinamento formal, não sendo exigidos carga horária mínima, realização presencial, avaliação, certificação ou emissão de certificado.

5.2. *Requisitos de Suporte Técnico e Garantia*

5.2.1. A solução deverá contar, durante toda a vigência contratual, com suporte técnico necessário ao atendimento das condições mínimas estabelecidas neste item, abrangendo as licenças, os agentes, a console e os demais componentes integrantes da edição ofertada.

5.2.2. O suporte técnico poderá ser prestado pela CONTRATADA, pelo fabricante ou por parceiro autorizado, por meio dos canais oficiais incluídos na proposta, desde que assegurado o atendimento integral às condições mínimas estabelecidas neste Termo de Referência.

5.2.3. O suporte deverá permitir, no mínimo:

5.2.3.1. Comunicação de falhas relacionadas ao funcionamento da solução;

5.2.3.2. Obtenção de orientações para diagnóstico e tratamento das falhas identificadas;

5.2.3.3. Tratamento de inconsistências relacionadas à ativação ou ao licenciamento;

5.2.3.4. Acesso à documentação, aos manuais, aos guias técnicos e à base de conhecimento disponibilizados para a solução; e

5.2.3.5. O direito de acesso às atualizações e aos serviços de suporte técnico incluídos na solução ou na proposta contratada durante toda a vigência contratual.

5.2.4. Os chamados poderão ser registrados por portal de suporte, sistema de tickets, correio eletrônico ou outro canal oficial disponibilizado pela CONTRATADA ou pelo fabricante, não sendo obrigatória a disponibilização de atendimento telefônico, WhatsApp ou canal exclusivo.

5.2.5. Quando o canal utilizado disponibilizar número ou código de identificação, o chamado deverá permanecer acessível para acompanhamento de sua situação até o encerramento.

5.2.6. Quando o suporte for acionado diretamente por meio do fabricante, a CONTRATADA deverá, quando solicitada pela CONTRATANTE, prestar orientações para abertura do chamado e auxiliar no seu escalonamento, permanecendo responsável pelas providências comerciais, cadastrais ou relacionadas ao licenciamento que estiverem sob sua responsabilidade.

5.2.7. Não será exigido prazo específico de resposta ou solução para os chamados técnicos, devendo os atendimentos observar as condições e os procedimentos aplicáveis ao suporte ou ao pacote de serviços incluído na proposta contratada.

5.2.8. A CONTRATADA deverá assegurar à CONTRATANTE, durante toda a vigência contratual, o direito de acesso às atualizações das bases de detecção de ameaças, dos mecanismos de proteção, dos agentes, dos motores de detecção, às correções de segurança e às versões abrangidas pelo licenciamento contratado.

5.2.9. Quando a aplicação de atualização ou correção exigir procedimento específico, a CONTRATADA deverá disponibilizar ou indicar a documentação e as orientações técnicas oficiais necessárias à sua execução.

5.2.10. Quando eventual intervenção puder causar indisponibilidade, interrupção ou impacto aos serviços municipais, sua execução deverá ser previamente acordada com a CONTRATANTE.

5.2.11. A CONTRATADA deverá manter a regularidade, a validade e o pleno funcionamento do

licenciamento durante todo o período contratual, adotando as providências necessárias para solucionar inconsistências relacionadas às licenças fornecidas.

5.2.12. As obrigações previstas neste item poderão ser atendidas pelo suporte padrão associado ao licenciamento, por atendimento prestado diretamente pela CONTRATADA, pelo fabricante, por parceiro autorizado ou pela combinação dessas modalidades, não sendo exigida modalidade comercial específica de suporte, plano premium ou atendimento dedicado.

5.2.13. Caso a licitante necessite incluir plano, pacote ou serviço adicional para cumprir as condições mínimas deste Termo de Referência, esse componente deverá ser identificado na proposta e estar integralmente incluído no valor ofertado, não sendo admitida cobrança posterior ou separada da Administração.

5.2.14. O suporte técnico continuado previsto neste item não compreende implantação integral da solução, administração ou monitoramento contínuo do ambiente, serviço de SOC, consultoria permanente, atendimento em regime 24 horas por dia e 7 dias por semana ou disponibilização de profissional dedicado.

5.2.15. O apoio técnico remoto destinado à ativação, à configuração inicial e à implantação da solução observará as condições estabelecidas no item 5.1 deste Termo de Referência.

5.2.16. Caso a proposta inclua serviços de suporte superiores aos requisitos mínimos, tais serviços integrarão a contratação e deverão ser mantidos durante a vigência contratual, sem alteração do valor contratado.

5.2.17. A proposta deverá identificar a modalidade de suporte incluída, o responsável por sua prestação, os canais oficiais disponíveis, o horário de atendimento e, quando existentes, os prazos de resposta e solução estabelecidos pelo fabricante ou pelo pacote de suporte ofertado.

6. NÍVEIS MÍNIMOS DE SERVIÇOS – NMS

6.1. Para fins de acompanhamento e fiscalização da execução do objeto, ficam estabelecidos os seguintes Níveis Mínimos de Serviço, aplicáveis às obrigações diretamente executadas ou controladas pela CONTRATADA.

6.2. A execução do objeto deverá observar os seguintes indicadores e prazos:

Tabela 2 – Níveis Mínimos de Serviço

INDICADOR	OBRIGAÇÃO AVALIADA	PRAZO OU CONDIÇÃO MINIMA	EVIDÊNCIA DE CUMPRIMENTO
NMS-01	Disponibilização das licenças.	Até 15 dias corridos, contados do recebimento da Ordem de Fornecimento.	Documento de licenciamento, registro de disponibilização ou consulta ao portal oficial da solução, contendo as informações mínimas estabelecidas no item 5.1.3.
NMS-02	Regularização de divergência relacionada à quantidade, edição, módulos, validade, titularidade ou ativação das licenças.	Até 5 dias úteis, contados da comunicação da CONTRATANTE, para a efetiva regularização quando esta estiver sob controle direto da CONTRATADA ou, nos demais casos, para adoção e comprovação das providências estabelecidas no item 6.3.	Documento, comunicação, registro no portal ou outra evidência da efetiva regularização ou, quando esta depender do fabricante ou distribuidor, protocolo, comprovante de encaminhamento e registro das providências adotadas pela CONTRATADA.

NMS-03	Início do apoio técnico remoto, pela CONTRATADA, à ativação e à configuração inicial da solução, bem como à instalação e à distribuição dos agentes, estas últimas executadas pela equipe técnica da CONTRATANTE.	Até 5 dias úteis, contados da solicitação da CONTRATANTE, salvo data distinta acordada entre as partes.	Registro de atendimento, mensagem eletrônica, ata ou relatório da atividade.
NMS-04	Realização do repasse de conhecimento.	Em data acordada entre as partes durante a fase de configuração inicial, observado o prazo máximo de 10 (dez) dias úteis contado da solicitação da CONTRATANTE, salvo data distinta formalmente acordada entre as partes.	Lista de participantes, ata, mensagem eletrônica ou registro da apresentação realizada.
NMS-05	Registro e tratamento inicial das solicitações técnicas recebidas diretamente pela CONTRATADA, incluindo seu encaminhamento ao fabricante ou parceiro autorizado quando necessário.	Até 2 (dois) dias úteis, contados do recebimento da solicitação, para registrar o chamado, comunicar à CONTRATANTE o início do atendimento ou encaminhá-lo ao canal competente de suporte, conforme aplicável.	Número do chamado, protocolo, mensagem eletrônica, registro de atendimento ou comprovante de encaminhamento.

6.3. Para fins do indicador NMS-02, quando a regularização depender de providência do fabricante ou do distribuidor, a CONTRATADA deverá, dentro do prazo estabelecido:

6.3.1. Registrar ou encaminhar a solicitação ao responsável competente;

6.3.2. Disponibilizar à CONTRATANTE o respectivo protocolo ou comprovante de encaminhamento; e

6.3.3. Acompanhar a solicitação até sua conclusão, prestando informações sobre sua situação quando solicitado.

6.4. O prazo previsto no NMS-02 será considerado atendido quando a CONTRATADA comprovar que adotou tempestivamente as providências sob sua responsabilidade e que a conclusão permanece dependente exclusivamente de atuação do fabricante ou distribuidor.

6.5. O apoio técnico remoto previsto no NMS-03 será executado em data e horário previamente acordados entre as partes, considerando a disponibilidade da equipe técnica da CONTRATANTE, os acessos necessários e as condições do ambiente tecnológico.

6.6. O prazo estabelecido no NMS-03 refere-se ao início do apoio técnico remoto prestado pela CONTRATADA. A instalação e a distribuição dos agentes nos equipamentos serão executadas pela equipe técnica da CONTRATANTE, cabendo à CONTRATADA prestar as orientações e o apoio técnico remoto necessários durante a fase inicial de implantação, nos termos do item 5.1.7.

6.7. O repasse de conhecimento previsto no NMS-04 será considerado realizado mediante apresentação de visão geral e orientação operacional sobre os assuntos estabelecidos no item 5.1.9, observadas as condições do item 5.1.10, não sendo exigidos carga horária mínima, treinamento formal, avaliação, certificação ou emissão de certificado.

6.8. Sem prejuízo do prazo estabelecido no NMS-05 para registro, tratamento inicial ou encaminhamento da solicitação, os chamados técnicos relacionados a falhas de funcionamento da solução observarão os canais, os procedimentos e as condições do suporte incluído na proposta contratada, não sendo estabelecido por este Termo de Referência prazo máximo para resposta

técnica ou solução definitiva.

6.9. Quando o chamado for aberto diretamente pela CONTRATANTE em canal oficial do fabricante ou de parceiro autorizado, não será aplicável o indicador NMS-05, permanecendo a CONTRATADA obrigada a prestar auxílio para o escalonamento quando solicitado e nos limites das responsabilidades previstas no item 5.2.

6.10. A indisponibilidade, a falha ou o atraso cuja solução dependa exclusivamente de atuação do fabricante ou distribuidor não caracterizará, por si só, descumprimento dos prazos dos NMS aplicáveis à atuação da CONTRATADA, desde que esta comprove ter adotado tempestivamente todas as providências sob sua responsabilidade. Essa circunstância não dispensa a apuração de eventual falta de disponibilização das licenças, atualizações, suporte ou demais recursos contratados, conforme os itens 6.16 a 6.19.

6.11. A contagem dos prazos em dias úteis observará os dias de expediente da Administração Municipal de Dourados/MS.

6.12. A contagem poderá ser suspensa quando o cumprimento da obrigação depender de informação, acesso, autorização, disponibilidade da equipe técnica ou providência da CONTRATANTE, desde que a pendência seja devidamente comunicada e registrada.

6.13. A contagem será retomada após o fornecimento da informação, do acesso, da autorização ou da providência necessária, considerando-se o período anteriormente transcorrido.

6.14. Eventuais condições de suporte superiores às exigências mínimas somente constituirão obrigações contratuais quando estiverem expressamente identificadas na proposta aceita, incluindo os respectivos canais, serviços, horários e prazos.

6.15. O cumprimento dos Níveis Mínimos de Serviço será aferido pela fiscalização com base nos prazos, condições e evidências estabelecidos na Tabela 2. O descumprimento injustificado de obrigação sob responsabilidade da CONTRATADA será registrado nos autos, com identificação do indicador afetado, da ocorrência e das evidências disponíveis.

6.16. Identificada divergência na quantidade, edição, validade, titularidade ou ativação das licenças, ou indisponibilidade de recurso contratado, a CONTRATANTE notificará formalmente a CONTRATADA, descrevendo a ocorrência, solicitando as providências cabíveis e informando sobre a possibilidade de apuração de valor relativo à parcela não executada, de desconto no pagamento devido e de aplicação das medidas contratuais pertinentes.

6.17. A fiscalização apurará a causa da ocorrência, as licenças ou os recursos afetados, o início e o término comprovados da indisponibilidade, as providências adotadas pela CONTRATADA e o impacto na execução do objeto. Serão consideradas as evidências disponíveis, inclusive registros da console, do portal de licenciamento, dos chamados técnicos e das comunicações com a CONTRATADA e com o fabricante ou distribuidor.

6.18. Comprovado que parcela do objeto contratado não foi disponibilizada ou permaneceu inoperante por causa atribuível à CONTRATADA, será apurado o valor proporcional à quantidade de licenças afetadas e ao período comprovado de indisponibilidade, limitado ao valor contratado da parcela correspondente. Após a manifestação da CONTRATADA e decisão motivada da Administração, esse valor poderá ser descontado de pagamento ainda devido ou, caso já tenha sido pago, exigido em restituição pelos meios administrativos cabíveis.

6.19. A apuração do valor da parcela não executada não constitui, por si só, sanção administrativa. Eventual aplicação de penalidade observará as hipóteses, os critérios e o procedimento previstos neste Termo de Referência, no contrato e na legislação aplicável, assegurados o contraditório e a ampla defesa. Não será aplicado desconto por indisponibilidade sem comprovação de sua duração,

extensão e relação com obrigação contratual não cumprida.

7. DO RECEBIMENTO E ACEITAÇÃO DO OBJETO

7.1. O objeto será recebido provisória e definitivamente, observadas as condições estabelecidas neste Termo de Referência, no Decreto Municipal nº 2.915, de 7 de fevereiro de 2024, no artigo 24 do Decreto Municipal nº 2.097/2023 e no artigo 140 da Lei Federal nº 14.133, de 1º de abril de 2021.

7.2. **Do recebimento provisório**

7.2.1. O objeto será recebido provisoriamente pelo fiscal técnico do contrato, mediante termo detalhado, após a disponibilização das licenças e o recebimento da documentação comprobatória apresentada pela CONTRATADA.
7.2.2. O recebimento provisório será realizado no prazo de até 3 (três) dias úteis, contado da comunicação formal da disponibilização das licenças pela CONTRATADA, desde que acompanhada dos documentos necessários à verificação do objeto.
7.2.3. Para fins de recebimento provisório, o fiscal técnico verificará, no mínimo:
7.2.3.1. A disponibilização das 2.920 (duas mil novecentas e vinte) licenças contratadas;
7.2.3.2. A identificação da Prefeitura Municipal de Dourados/MS como titular ou beneficiária do licenciamento;
7.2.3.3. A correspondência entre a solução fornecida e aquela constante da proposta aceita;
7.2.3.4. A validade do licenciamento pelo período de 36 (trinta e seis) meses;
7.2.3.5. A disponibilidade de acesso à console de gerenciamento e aos componentes necessários ao funcionamento da solução;
7.2.3.6. A disponibilidade das atualizações e dos canais de suporte técnico;
7.2.3.7. O atendimento às demais condições estabelecidas neste Termo de Referência e no Anexo II – Especificações Técnicas Mínimas; e
7.2.3.8. A correspondência entre a solução disponibilizada, incluindo produto, edição, módulos e nível de licenciamento, e aquela indicada na proposta e na Matriz de Comprovação dos Requisitos Técnicos aprovada durante o procedimento licitatório.
7.2.4. A Matriz de Comprovação dos Requisitos Técnicos e a documentação apresentada durante o procedimento licitatório poderão ser utilizadas pela fiscalização como instrumentos auxiliares para verificação da conformidade da solução entregue, sem prejuízo da realização de testes, consultas ao portal oficial do fabricante ou outras verificações tecnicamente necessárias.
7.2.5. A fiscalização deverá registrar o resultado da verificação no Relatório de Aceitação dos Serviços – RAS ou em documento equivalente adotado pela Administração, encaminhando-o ao gestor do contrato para realização do recebimento definitivo.
7.2.6. O relatório deverá conter o registro, a análise e a conclusão da fiscalização quanto ao atendimento das exigências técnicas e contratuais, acompanhado dos documentos considerados necessários à comprovação da entrega.
7.2.7. Caso sejam identificadas irregularidades que impeçam o recebimento do objeto, a CONTRATADA será formalmente notificada para promover as correções necessárias no prazo máximo de 5 (cinco) dias corridos, contado do recebimento da notificação, sem ônus adicional para a CONTRATANTE.
7.2.8. O objeto poderá ser recusado, no todo ou em parte, quando estiver em desacordo com as especificações estabelecidas neste Termo de Referência, no Anexo II – Especificações Técnicas Mínimas, na Matriz de Comprovação dos Requisitos Técnicos aprovada ou na proposta aceita.
7.2.9. A correção das irregularidades não implicará prorrogação automática do prazo de entrega, ficando a CONTRATADA sujeita às medidas cabíveis em caso de atraso injustificado.

7.3. Do Recebimento Definitivo

7.3.1. O objeto será recebido definitivamente pelo gestor do contrato ou por servidor ou comissão designada pela autoridade competente, mediante termo detalhado que comprove o atendimento das exigências contratuais.
7.3.2. O recebimento definitivo ocorrerá no prazo de até 5 (cinco) dias úteis, contado do recebimento provisório, após a análise do respectivo relatório e dos demais documentos apresentados pela fiscalização.
7.3.3. Para fins do recebimento definitivo, caberá ao responsável:
7.3.3.1. Analisar o relatório elaborado pela fiscalização e a documentação comprobatória da execução do objeto;
7.3.3.2. Verificar a inexistência de irregularidades que impeçam a aceitação, a liquidação e o pagamento da despesa;
7.3.3.3. Solicitar à CONTRATADA, por escrito, as correções eventualmente necessárias;
7.3.3.4. Emitir o Termo de Recebimento Definitivo; e
7.3.3.5. Comunicar a CONTRATADA para emissão da Nota Fiscal correspondente ao objeto definitivamente recebido.
7.3.4. Se a verificação não for concluída no prazo estabelecido por motivo imputável à CONTRATADA, o prazo para o recebimento definitivo ficará suspenso até a correção das irregularidades identificadas.
7.4. O recebimento provisório ou definitivo não excluirá a responsabilidade da CONTRATADA pela regularidade do licenciamento, pelo funcionamento da solução nem pelo cumprimento das obrigações de atualização, suporte técnico e garantia durante toda a vigência contratual.
7.5. Após o recebimento definitivo, permanecerão exigíveis todas as obrigações de execução continuada previstas neste Termo de Referência, especialmente as relacionadas à validade das licenças, às atualizações da solução, ao suporte técnico e ao cumprimento dos Níveis Mínimos de Serviço – NMS.

8. FATURAMENTO, LIQUIDAÇÃO E PAGAMENTO

8.1. A emissão da nota fiscal será realizada após a autorização do Gestor de Contrato através das SF - Solicitação de Fornecimento, conforme quantidades e valores contratados, sendo entregues em parcela única.

8.2. Liquidação

8.2.1. Recebida a Nota Fiscal ou instrumento de cobrança equivalente, correrá o prazo de até 30 dias corridos (conforme art. 6º, inciso I, do Decreto Municipal n° 2.894 de 19/01/2024) para fins de liquidação.

8.2.2. A alteração da ordem cronológica de pagamento somente ocorrerá mediante prévia justificativa da autoridade competente e posterior comunicação ao Controle Interno e ao Tribunal de Contas do Estado de Mato Grosso do Sul, exclusivamente nas seguintes situações (Art°9 do Decreto Municipal N° 2.894):

I. grave perturbação da ordem, situação de emergência ou calamidade pública;

II. pagamento a microempresa, empresa de pequeno porte, agricultor familiar, produtor rural pessoa física, microempreendedor individual e sociedade cooperativa, desde que demonstrado o risco de descontinuidade do cumprimento do objeto do contrato;

III. pagamento de serviços necessários ao funcionamento dos sistemas estruturantes, desde que demonstrado o risco de descontinuidade do cumprimento do objeto do contrato;

IV. pagamento de direitos oriundos de contratos em caso de falência, recuperação judicial ou dissolução da empresa contratada; ou

V. pagamento de contrato cujo objeto seja imprescindível para assegurar a integridade do patrimônio público ou para manter o funcionamento das atividades finalísticas do órgão ou entidade,

quando demonstrado o risco de descontinuidade da prestação de um serviço público de relevância ou o cumprimento da missão institucional;

8.2.3. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

I. o prazo de validade;

II. a data da emissão;

III. os dados do contrato e do órgão contratante;

IV. o período respectivo de execução do contrato;

V. o valor a pagar; e

VI. eventual destaque do valor de retenções tributárias cabíveis.

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

8.2.5. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line mediante consulta aos sítios eletrônicos oficiais ou documentação mencionada no art. 68 da Lei n.° 14.133, de 2021.

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

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

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

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

8.3. Prazo de pagamento

8.3.1. O pagamento será efetuado no prazo de até 30 (trinta) dias corridos contados da finalização da liquidação da despesa (conforme art. 6º, inciso II, do Decreto Municipal N° 2.894 de 19/01/2024).

8.3.2. Nos casos de eventuais atrasos de pagamento, por culpa exclusiva do Contratante, o pagamento será efetuado com atualização financeira, calculada de acordo com a taxa SELIC, após 60 (sessenta) dias do vencimento do documento fiscal.

8.4. Forma de pagamento

8.4.1. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

8.4.2. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

8.4.3. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

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

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

8.4.6. Durante a vigência contratual, a CONTRATADA deverá estar em dia com todas as condições de habilitação exigidas quando da contratação.

8.4.7. A CONTRATADA devera, obrigatoriamente, encaminhar os seguintes documentos no fechamento do fornecimento do objeto, conforme período estabelecido entre as partes:

a) 02 (duas) vias da Solicitação de Fornecimento (SF), geradas com base nas requisições executadas, serem encaminhadas pela CONTRATANTE;

b) Nota fiscal gerada pela execução conforme valor(es) constante(s) nas SF's.

c) Prova de Regularidade Fiscal:

i. No caso de contratação de serviços, deverão ser apresentados documentos que comprovem a regularidade fiscal perante a União (Secretaria de Receita Federal, INSS e FGTS) e o Município (ISS), e Certidão de Débitos Trabalhistas (Justiça do Trabalho). Todas as certidões deverão estar dentro do prazo de validade.

ii. No caso de aquisição de bens materiais, deverão ser apresentados documentos que comprovem a regularidade fiscal perante a União (Secretaria de Receita Federal, INSS e FGTS) e o Estado (ICMS), e Certidão de Débitos Trabalhistas (Justiça do Trabalho). Todas as certidões deverão estar dentro do prazo de validade.

iii. A eventual perda das condições de que trata o caput do art. 7º do Decreto Municipal 2.894/2024, não enseja, por si, retenção de pagamento pela Administração.

d) Empresa optante do SIMPLES, deve apresentar junto ã nota fiscal documento(s) que comprove(m) seu enquadramento como a Declaração, conforme modelo (ANEXO I), conforme inciso IV do art.42 da IN da Receita Federal do Brasil n.º 21.244 de 30/01/2012, devidamente datada e assinada pelo responsável e no original;

e) A falta de um dos documentos solicitados no item anterior poderá implicar no não recebimento do objeto e, consequentemente, da nota fiscal.

9. RECOMPOSIÇÃO DO EQUILÍBRIO ECONÔMICO-FINANCEIRO

9.1. Do Reajuste

9.1.1. O preço permanecerá fixo e irreajustável durante a vigência do Contrato, salvo se após 12 (doze) meses a contar do orçamento estimativo em **16/09/2026**, houver saldo ou para compensação inflacionária, hipótese em que a CONTRATADA poderá através de requerimento, solicitar o reajuste.

9.1.2. Havendo a ocorrência do item anterior, o saldo contratual será reajustado aplicando-se o **Índice de Custo da Tecnologia da Informação (ICTI)**, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

9.1.3. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

9.1.4. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

9.1.5. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

9.1.6. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

9.1.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

9.1.8. O descumprimento de cronograma físico-financeiro, se houver, por responsabilidade da CONTRATADA, bem como de outras obrigações, ensejará a não concessão de reajuste anual.

9.1.9. O reajuste poderá ser realizado por apostilamento.

9.2. Da Revisão/Reequilíbrio

9.2.1. Caso ocorra o desequilíbrio econômico durante a vigência contratual, a CONTRATADA poderá requerer formalmente à CONTRATANTE a revisão dos valores pactuados.

9.2.2. Para tanto, deverá relatar em detalhes os fatos (imprevisíveis ou previsíveis porém de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, ou, ainda, em caso de força maior, caso fortuito ou fato do príncipe, superveniente ao originalmente contratado), anexando documentos que comprovem o alegado desequilíbrio, informando ainda, o valor pleiteado.

9.2.3. A revisão/reequilíbrio econômico-financeiro será realizado por meio de termo aditivo.

9.3. Da Repactuação

9.3.1. Não há previsão de repactuação para o objeto do presente termo de referência.

10. ESTIMATIVA DA CONTRATAÇÃO

10.1. O custo estimado total da contratação é de **R$ 473.536,40** (Quatrocentos e setenta e três mil, quinhentos e trinta e seis reais e quarenta centavos), conforme pesquisa de preços realizado para o orçamento estimativo. A memória de cálculo e os documentos de suporte da estimativa constam do Mapa de Apuração de Preços, do Relatório Unificado das Pesquisas de Preços e das pesquisas de preço que instruem o processo, elaborados nos termos do Decreto Municipal nº 787/2021.

11. ADEQUAÇÃO ORÇAMENTÁRIA

11.1. As despesas provenientes da contratação ocorrerão pela seguinte dotação orçamentária:

07.000 – SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO
07.001 – Secretaria Municipal de Administração
04.126.0110 - Programa de Desenvolvimento da Tecnologia da Informação
04.126 - Administração/Tecnologia da Informação
2.017 – Manutenção das Atividades de Gestão e de investimento em TIC

33.90.40.00 – Serviços de Tecnologia da Informação e Comunicação – Pessoa Jurídica
Fonte: 1.500.0000

12. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

12.1. Forma de seleção e critério de julgamento da proposta

12.1.1. Os serviços a serem contratados caracterizam-se como ***serviços contínuos***, conforme art. 3º, inciso XIII, do Decreto Municipal de nº 556 de 15 de setembro de 2017 que "Dispõe sobre a definição de Serviços Contínuos no âmbito do Município de Dourados e dá outras providencias". A Secretaria solicitante manifesta interesse na aplicação do art. 107 da Lei Federal nº 14.133/2021, tendo em vista que a proteção dos endpoints deve ser mantida de forma ininterrupta, não sendo admissível a descontinuidade do licenciamento, das atualizações e do suporte, sob pena de exposição dos ativos computacionais da Administração Municipal, conforme item 2 deste Termo de Referência, razão pela qual se prevê, no item 1.4.2, a possibilidade de prorrogação sucessiva, respeitada a vigência máxima decenal e condicionada à comprovação da vantajosidade das condições e dos preços.

12.1.2. Por se tratar de uma contratação de serviços comuns, o fornecedor será selecionado por meio da modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO por item, nos termos do Decreto Municipal nº 2.129/2023.

12.1.3. Plataforma: "Bolsa de Licitações e Leilões do Brasil - BLL" (www.bll.org.br).

12.1.4. O modo de disputa para o envio de lances no pregão eletrônico será ***aberto e fechado***, em que os licitantes apresentarão lances públicos e sucessivos, com lance final fechado.

12.1.5. Os intervalos mínimos de diferença de valores ou de percentuais entre os lances será de R$ 10,00 (dez reais).

12.2. Critérios de aceitação da proposta

12.2.1. Serão exigidos documentos adicionais para análise da proposta da licitante provisoriamente classificada em primeiro lugar?

(X) SIM ( ) NÃO

12.2.1.1. A Matriz de Comprovação dos Requisitos Técnicos e a documentação comprobatória nela indicada serão exigidas apenas da licitante provisoriamente classificada em primeiro lugar, após convocação, para análise da conformidade da solução ofertada, constituindo requisito de aceitabilidade da proposta, observado o procedimento estabelecido no item 4.2 deste Termo de Referência. Não será exigida sua apresentação por todos os licitantes no envio inicial das propostas.

12.2.1.2. A exigência da Matriz de Comprovação dos Requisitos Técnicos, como requisito de aceitabilidade da proposta, possui caráter excepcional e justifica-se por ser indispensável à garantia da execução contratual, uma vez que o objeto consiste em solução corporativa integrada de proteção de endpoints, com recursos de EPP e EDR, cuja aderência aos requisitos técnicos mínimos do Anexo II não pode ser aferida apenas pela proposta de preços, e a contratação de solução que não os atenda comprometeria a proteção dos ativos computacionais da Administração Municipal durante toda a vigência contratual, conforme item 2 deste Termo de Referência. Em observância à proporcionalidade, a exigência restringe-se à licitante provisoriamente classificada em primeiro lugar, à documentação técnica oficial do fabricante e aos blocos de requisitos prioritários indicados no Apêndice A, sem prejuízo do atendimento integral ao Anexo II.

12.2.2. A proposta de preços deverá contemplar o valor por item, incluindo todos os custos diretos e indiretos necessários ao cumprimento do objeto deste Termo de Referência, em especial o valor de tributos, tarifas, encargos sociais, custos com entregas e demais despesas decorrentes da execução da presente contratação.

12.2.3. A proposta de preços deve respeitar o máximo estimado para a contratação.

12.2.4. A proposta terá a validade de 90 (noventa) dias.

12.3. Exigências de habilitação:

12.3.1. ***Econômico-financeira***

12.3.1.1. Certidão negativa de falência ou concordata expedida pelo distribuidor da sede da pessoa jurídica, que esteja dentro do prazo de validade expresso na própria Certidão.

12.3.1.1.1. Em caso de empresa em recuperação judicial, deverá a licitante apresentar certidão emitida pela instância judicial competente, que certifique que a interessada está apta econômica e financeiramente a participai de procedimento licitatório, nos termos da Lei Federal n.º 14.133/21.

12.3.1.2. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2(dois) últimos exercícios sociais.

12.3.1.3. Demais informações quanto à qualificação econômico-financeira serão definidas em Edital.

12.3.2. ***Fiscal, Social e Trabalhista***

12.3.2.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas;

12.3.2.2. Prova de inscrição no cadastro de contribuintes estadual, relativa à sede ou domicílio da licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

12.3.2.3. Prova de Regularidade com a Fazenda Pública Federal (Certidão Conjunta de Débitos Relativos a Tributos Federais e à Dívida Ativa da União, abrangendo contribuições sociais, nos termos da Portaria MF n.° 358, de 05 de setembro de 2014);

12.3.2.4. Prova de regularidade com a Fazenda Municipal, através de certidão apta a demonstrar a regularidade ou a inexistência de débitos relativamente ao Imposto Sobre Serviços(ISS), expedida pelo órgão municipal competente em que domiciliada a licitante;

12.3.2.5. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

12.3.2.6. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei n.° 5.452, de 1º de maio de 1943;

12.3.2.7. Caso o licitante seja considerado isento dos tributos Estadual/Distrital ou Municipal/Distrital relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

12.3.3. ***Qualificação Técnica***

12.3.3.1. A licitante deverá comprovar aptidão para o desempenho de atividade pertinente e compatível com o objeto da contratação, mediante apresentação de um ou mais atestados ou declarações de capacidade técnica, emitidos por pessoa jurídica de direito público ou privado, em

nome da licitante, nos termos do artigo 67 da Lei Federal nº 14.133, de 1º de abril de 2021.

12.3.3.2. O atestado ou o conjunto de atestados deverá comprovar experiência anterior no fornecimento ou licenciamento de solução corporativa de proteção de endpoints, antivírus corporativo ou solução equivalente de segurança de endpoints, acompanhada de atualizações e/ou suporte técnico.

12.3.3.3. Será admitida a apresentação de um ou mais atestados para comprovação da experiência exigida no item 12.3.3.2, inclusive referentes a contratos executados em períodos distintos, desde que seus objetos sejam compatíveis com a contratação pretendida. Não será exigido quantitativo mínimo de licenças ou endpoints nos atestados. O objeto é composto por item único e a parcela de maior relevância e valor significativo, para os fins do art. 67 da Lei Federal nº 14.133/2021, corresponde ao fornecimento ou licenciamento de solução corporativa de proteção de endpoints acompanhada de atualizações e/ou suporte técnico, conforme item 12.3.3.2. Não serão admitidas limitações de tempo ou de locais específicos relativas aos atestados (art. 67, § 2º). A ausência de quantitativo mínimo decorre da avaliação da Administração de que a comprovação de experiência anterior em objeto compatível é necessária e suficiente para demonstrar a capacidade da licitante, nos termos dos arts. 62 e 67 da Lei Federal nº 14.133/2021, evitando-se exigência superior ao necessário.

12.3.3.4. Os atestados deverão conter informações suficientes para permitir a identificação:

12.3.3.4.1. Da pessoa jurídica emitente;

12.3.3.4.2. Da licitante responsável pelo fornecimento ou serviço;

12.3.3.4.3. Do objeto executado;

12.3.3.4.4. Do período de execução, quando aplicável; e

12.3.3.4.5. Do cumprimento satisfatório das obrigações assumidas.

12.3.3.5. Os atestados deverão ser apresentados em documento emitido em papel timbrado ou em formato que permita a identificação da entidade emitente, contendo nome, cargo e forma de contato do responsável pelas informações prestadas.

12.3.3.6. No caso de atestados emitidos por pessoa jurídica de direito privado, não serão aceitos documentos emitidos por empresa pertencente ao mesmo grupo econômico da licitante, sua controladora, controlada ou coligada, nem por empresa que possua sócio em comum com a licitante.

12.3.3.7. Quando as informações constantes do atestado não forem suficientes para comprovar o atendimento às exigências estabelecidas neste item, a licitante poderá apresentar documentos complementares, como contratos, notas fiscais, termos de referência, ordens de fornecimento, termos de recebimento ou outros documentos relacionados à execução do objeto atestado.

12.3.3.8. A Administração poderá realizar diligências para esclarecer ou confirmar as informações constantes dos documentos apresentados, inclusive mediante contato com a pessoa jurídica emitente, consulta a contratos, notas fiscais, portais públicos ou outros meios idôneos de verificação.

12.3.3.9. As diligências destinam-se à complementação e ao esclarecimento das informações relativas à documentação apresentada, não sendo admitida a substituição de documento inexistente nem a comprovação posterior de condição que não estivesse atendida na data prevista para a habilitação.

12.3.4. ***Demais exigências de habilitação***

12.3.4.1. O edital definirá as exigências de habilitação jurídica bem como oferecerá maior

detalhamento com relação à habilitação fiscal, social, trabalhista e econômico-financeira, caso necessário.

13. DA GESTÃO E FISCALIZAÇÃO DOS SERVIÇOS

13.1. A Comissão de Fiscalização repassará à CONTRATADA, conhecimentos necessários à execução dos serviços;

13.2. Serão esclarecidos todos os pontos relativos a questões operacionais, administrativas e de gestão do contrato.

13.3. O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

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

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

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

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

13.8. A execução do contrato deverá ser acompanhada e fiscalizada por 1 (um) ou mais fiscais do contrato, representantes da Administração especialmente designados conforme estabelecidos no art. 117 da Lei 14.133/21 bem como no art. 7º do Decreto Municipal nº 2.097/23.

13.9. A gestão do contrato será realizada pelo Gestor e a fiscalização, por seu fiscal técnico e/ou administrativo, cujas funções mínimas estão descritas a seguir:

13.9.1. Gestor de contratos:

13.9.1.1. Conforme art. 20 do Decreto Municipal n.º 2.097/23, caberá ao gestor do contrato e, nos seus afastamentos e seus impedimentos legais, ao seu substituto, em especial:

I - coordenar as atividades relacionadas à fiscalização técnica, administrativa e setorial, de que tratam os incisos II, III e IV do caput do art. 18 do referido decreto;

II - acompanhar os registros realizados pelos fiscais do contrato das ocorrências relacionadas à execução do contrato e as medidas adotadas, e informar à autoridade superior aquelas que ultrapassarem a sua competência;

III - acompanhar a manutenção das condições de habilitação do contratado, para fins de empenho de despesa e de pagamento, e anotar os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais;

IV - coordenar a rotina de acompanhamento e de fiscalização do contrato, cujo histórico de gerenciamento deverá conter todos os registros formais da execução, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, e elaborar

relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração;

V - coordenar os atos preparatórios à instrução processual e ao envio da documentação pertinente ao setor de contratos para a formalização dos procedimentos de que trata o inciso I do caput do art. 18 do referido decreto;

VI - elaborar o relatório final de que trata a alínea "d" do inciso VI do § 3º do art. 174 da Lei nº 14.133, de 2021, com as informações obtidas durante a execução do contrato;

VII - coordenar a atualização contínua do relatório de riscos durante a gestão do contrato, com apoio dos fiscais técnico, administrativo e setorial;

VIII - emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, a constarem do cadastro de atesto de cumprimento de obrigações conforme disposto em regulamento;

IX - realizar o recebimento definitivo do objeto do contrato referido no art. 24 do referido decreto, mediante termo detalhado que comprove o atendimento das exigências contratuais; e

X - tomar providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor competente para tal, conforme o caso.

13.9.2. Fiscal técnico

13.9.2.1. O fiscal técnico acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

13.9.2.2. Conforme art. 21 do Decreto Municipal n.º 2.097/23, caberá ao fiscal técnico do contrato e, nos seus afastamentos e seus impedimentos legais, ao seu substituto, em especial:

I - prestar apoio técnico e operacional ao gestor do contrato com informações pertinentes às suas competências;

II - anotar no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados;

III - emitir notificações para a correção de rotinas ou de qualquer inexatidão ou irregularidade constatada, com a definição de prazo para a correção;

IV - informar ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem a sua competência, para que adote as medidas necessárias e saneadoras, se for o caso;

V - comunicar imediatamente ao gestor do contrato quaisquer ocorrências que possam inviabilizar a execução do contrato nas datas estabelecidas;

VI - fiscalizar a execução do contrato para que sejam cumpridas as condições estabelecidas, de modo a assegurar os melhores resultados para a administração, com a conferência das notas fiscais e das documentações exigidas para o pagamento e, após o ateste, que certifica o recebimento provisório, encaminhar ao gestor de contrato para ratificação;

VII - comunicar ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual;

VIII - participar da atualização do relatório de riscos durante a fase de gestão do contrato, em conjunto com o fiscal administrativo e com o setorial, conforme o disposto no inciso VII do caput do art. 20 do referido decreto;

IX - auxiliar o gestor do contrato com as informações necessárias, na elaboração do documento comprobatório da avaliação realizada na fiscalização do cumprimento de obrigações assumidas pelo contratado, conforme o disposto no inciso VIII do caput do art. 20 do referido decreto; e

X - realizar o recebimento provisório do objeto do contrato referido no art. 24 do referido decreto, mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico.

13.9.3. Fiscal administrativo

13.9.3.1. Conforme art. 22 do Decreto Municipal n.º 2.097/23, caberá ao fiscal administrativo do contrato e, nos seus afastamentos e seus impedimentos legais, ao seu substituto, em especial:

I - prestar apoio técnico e operacional ao gestor do contrato, com a realização das tarefas relacionadas ao **controle dos prazos relacionados ao contrato e à formalização de apostilamentos e de termos aditivos, ao acompanhamento do empenho e do pagamento e ao acompanhamento de garantias e glosas;**

II - verificar a manutenção das condições de habilitação da CONTRATADA, com a solicitação dos documentos comprobatórios pertinentes, caso necessário;

III - examinar a regularidade no recolhimento das contribuições fiscais, trabalhistas e previdenciárias e, na hipótese de descumprimento, observar o disposto no termo de referencia e documento contratual;

IV - atuar tempestivamente na solução de eventuais problemas relacionados ao descumprimento das obrigações contratuais e reportar ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência;

V - participar da atualização do relatório de riscos durante a fase de gestão do contrato, em conjunto com o fiscal técnico e com o setorial, conforme o disposto no inciso VII do caput do art. 20 deste decreto;

VI - auxiliar o gestor do contrato com as informações necessárias, na elaboração do documento comprobatório da avaliação realizada na fiscalização do cumprimento de obrigações assumidas pelo contratado, conforme o disposto no inciso VIII do caput do art. 20; e

VII - realizar o recebimento provisório do objeto do contrato referido no art. 24, mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo.

13.10. Disposições gerais:

13.10.1. O fiscal do contrato anotará em registro próprio todas as ocorrências relacionadas à execução do contrato, determinando o que for necessário para a regularização das faltas ou dos defeitos observados, conforme disposto no artigo 117, § 1º da Lei nº14.133/21.

13.10.2. O fiscal do contrato informará a seus superiores, em tempo hábil para a adoção das medidas convenientes, a situação que demandar decisão ou providência que ultrapasse sua competência conforme disposto no artigo 117, § 2º, da Lei nº14.133/21 .

13.10.3. O fiscal do contrato será auxiliado pelos órgãos de assessoramento jurídico e de controle interno da Administração, que deverão dirimir dúvidas e subsidiá-lo com informações relevantes para prevenir riscos na execução contratual, conforme disposto no artigo 117, § 3º, da Lei nº14.133/21.

13.10.4. A fiscalização executará rigoroso controle em relação à quantidade e particularidade da qualidade dos serviços executados, a fim de possibilitarem a aplicação das penalidades previstas, quando desatendidas as disposições a ele relativas;

13.10.5. O fiscal de contrato deverá apontar quaisquer serviços incompatíveis com os padrões técnicos e de qualidade definidos neste Termo de Referência e demais projetos anexos/ complementares;

13.10.6. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela **CONTRATADA** ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e demais projetos anexos/ complementares.

14. RESPONSABILIDADES E OBRIGAÇÕES DA CONTRATADA

14.1. Indicar formalmente preposto apto a representá-la junto à CONTRATANTE, que deverá responder pela fiel execução do contrato;

14.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

14.3. Reparar quaisquer danos diretamente causados à CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução do contrato pela CONTRATANTE;

14.4. Propiciar todos os meios necessários à fiscalização do contrato pela CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

14.5. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

14.6. Tomar todas as providências necessárias para o fiel cumprimento das disposições contidas neste Termo de referência.

14.7. Entregar o objeto de acordo com o especificado neste documento;

14.8. Responder integralmente por perdas e danos que vier a causar a administração municipal;

14.9. Manter durante toda a execução do fornecimento do objeto, a compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas pela administração;

14.10. Relatar à administração toda e qualquer irregularidade verificada no fornecimento do objeto;

15. RESPONSABILIDADES E OBRIGAÇÕES DA CONTRATANTE

15.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

15.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

15.3. Receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta

aceita, conforme inspeções realizadas;

15.4. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

15.5. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

15.6. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

15.7. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do Contratado, com base em pesquisas de mercado, quando aplicável;

15.8. Verificar minuciosamente a conformidade do objeto recebido com as especificações constantes neste Termo de referência para fins de aceitação e recebimento definitivo;

15.9. Comunicar ao fornecedor, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido.

16. DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

16.1. Das Infrações:

16.1.1. De acordo com o disposto no art. 155 da Lei 14.133/21, a CONTRATADA será responsabilizada administrativamente pelas seguintes infrações:

I - dar causa à inexecução parcial do contrato;

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

III - dar causa à inexecução total do contrato;

IV - deixar de entregar a documentação exigida para o certame;

V - não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

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

VII - ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

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

IX - fraudar a licitação ou praticar ato fraudulento na execução do contrato;

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

XI - praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

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

16.2. Das Sanções

16.2.1. De acordo com o que dispõe o art. 156 da Lei 14.133/21, serão aplicadas ao responsável pelas infrações administrativas previstas no **item 16.1.1** deste Termo de Referência, as seguintes sanções:

I - advertência. Infração: no caso previsto do inciso I do **item 16.1.1**, quando não se justificar a imposição de penalidade mais grave;

II - multa (compensatória): Infração: qualquer das infrações dispostas nos incisos I ao XII do **item 16.1.1**, sendo nos seguintes percentuais e infrações:

a) 0,5% (cinco décimos por cento) a 1% (um por cento) do valor estimado da contratação: nos casos dos incisos IV e V;

b) 1% (um por cento) a 10% (dez por cento) do valor estimado da contratação para aquele que não celebrar o contrato, ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta: nos casos dos incisos VI;

c) 20% (vinte por cento) sobre o valor da parcela do objeto não executada: nos casos dos incisos I e VII;

d) de 20% (vinte por cento) a 30% (trinta por cento) sobre o valor contratado: nos casos dos incisos II, III, VIII, IX, X, XI e XII;

III - impedimento de licitar e contratar: Infração: nos casos de ocorrência dos incisos II, III, IV, V e VI do **item 16.1.1**, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo **prazo máximo de 3 (três) anos**.

IV - declaração de inidoneidade para licitar ou contratar: Infração: nos casos de ocorrência dos incisos VIII, IX, X, XI e XII bem como pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do **item 16.1.1** que justifiquem a imposição de penalidade mais grave que a sanção referida no § 4º do art. 156 da Lei 14.133/21, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo **prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos**.

16.2.2. A sanção estabelecida no inciso IV - declaração de inidoneidade para licitar ou contratar será precedida de análise jurídica, sendo a sua aplicação de competência do secretário municipal.

16.2.3. As sanções previstas nos incisos I, III e IV do **item 16.2.1**, poderão ser aplicadas cumulativamente com a prevista no inciso II do referido item.

16.2.4. A aplicação das sanções previstas no **item 16.1.1** não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

16.2.5. Para aplicação das sanções previstas no **item 16.2** deverão ser observadas o disposto no subitem **13.9.1.1 inciso X** deste Termo de Referência.

16.3. Da multa de mora

16.3.1. O atraso injustificado na execução do contrato sujeitará o contratado a multa de mora, na forma prevista em edital ou em contrato.

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

16.3.2.1. As penalidades de multa moratória e de multa compensatória não serão cumuladas.

16.4. Da defesa do interessado

16.4.1. Na aplicação da sanção prevista no inciso II do caput do art. 156 da Lei 14.133/21, será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

16.4.2. A aplicação das sanções previstas nos incisos III e IV do caput do art. 156 da Lei requererá a instauração de processo de responsabilização, a ser conduzido por comissão composta de 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o contratado para, no prazo de 15 (quinze) dias úteis, contado da data de intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

16.4.3. Em órgão ou entidade da Administração Pública cujo quadro funcional não seja formado de servidores estatutários, a comissão a que se refere o **item 16.4.2** deste Termo, será composta de 2 (dois) ou mais empregados públicos pertencentes aos seus quadros permanentes, preferencialmente com, no mínimo, 3 (três) anos de tempo de serviço no órgão ou entidade.

16.4.4. Na hipótese de deferimento de pedido de produção de novas provas ou de juntada de provas julgadas indispensáveis pela comissão, o licitante ou o contratado poderá apresentar alegações finais no prazo de 15 (quinze) dias úteis, contado da data da intimação.

16.4.5. Serão indeferidas pela comissão, mediante decisão fundamentada, provas ilícitas, impertinentes, desnecessárias, protelatórias ou intempestivas.

17. DA RESPONSABILIDADE PELA ELABORAÇÃO DO TERMO DE REFERÊNCIA

17.1. Por fim, registra-se que o presente Termo de Referência foi elaborado pelos servidores que abaixo assinam, na qual ratificam as informações nele contidas atestando sua veracidade, estando em consonância com as disposições legais e normativas aplicáveis, sendo submetido à consideração e aprovação pelo Ordenador de Despesa.

gov.br Documento assinado digitalmente
TATIANE CIMARA ARAUJO IKEDA SABINO
Data: 23/09/2026 13:58:30-0300
Verifique em https://validar.iti.gov.br

Tatiane Cimara Araújo Ikeda Sabino
Matricula: 1147629491
Integrante Técnico
Depto de Tecnol. da Informação/SEMAD

gov.br Documento assinado digitalmente
FABIO JOSE ESPINDOLA SANDIM
Data: 23/09/2026 14:11:37-0300
Verifique em https://validar.iti.gov.br

Fabio José Espindola Sandim
Mat. 1147751552
Integrante Técnico
Depto de Tecnol. da Informação/SEMAD

gov.br Documento assinado digitalmente
LIDIANE MODENEZ DUARTE
Data: 23/09/2026 14:17:30-0300
Verifique em https://validar.iti.gov.br

Lidiane Modenez Duarte
Matrícula - 2759 (LRV-MT)
Integrante Administrativo
Planejamento de Contratações/SEMAD

18. DA AUTORIZAÇÃO

18.1. Aprovo o presente Termo de Referência e autorizo o encaminhamento para abertura do

processo de licitatório.

Dourados/MS, 2026.

TAYS PEREIRA LITRAN DINIZ:85560529168
Secretária Municipal de Administração
2026.09.24 10:15:51-04'00'

Tays Pereira Litran Diniz
Secretária Municipal de Administração

ANEXO I

DECLARAÇÃO A SER APRESENTADA PELA PESSOA JURÍDICA CONSTANTE DO INCISO XI DO ART 4º

(Redação dada pela Instrução Normativa RFB n.º 1.244, de 30 de janeiro de 2012) (Vide art. 3º da IN RFB n.º 1244/2012)

Prefeitura Municipal de Dourados

(Nome da empresa), com sede (endereço completo), inscrita no CNPJ sob o nº..... DECLARA à **Prefeitura Municipal de Dourados**, para fins de não incidência na fonte do Imposto sobre a Renda da Pessoa Jurídica (IRPJ), da Contribuição Social sobre o Lucro Líquido (CSLL), da Contribuição para o Financiamento da Seguridade Social (Cofins), e da Contribuição para o PIS/Pasep, a que se refere o art. 64 da Lei nº 9.430, de 27 de dezembro de 1996, que é regularmente inscrita no Regime Especial Unificado de Arrecadação de Tributos e Contribuições devidos pelas Microempresas e Empresas de Pequeno Porte - **Simples Nacional**, de que trata o art. 12 da Lei Complementar nº 123, de 14 de dezembro de 2006.

Para esse efeito, a declarante informa que:

I - preenche os seguintes requisitos:

a) conserva em boa ordem, pelo prazo de 05 (cinco anos), contado da data da emissão, os documentos que comprovam a origem de suas receitas e a efetivação de suas despesas, bem como a realização de quaisquer outros atos ou operações que venham a modificar sua situação patrimonial; e

b) cumpre as obrigações acessórias a que está sujeita, em conformidade com a legislação pertinente;

II - o signatário é representante legal desta empresa, assumindo o compromisso de informar à Secretaria da Receita Federal do Brasil e à entidade pagadora, imediatamente, eventual desenquadramento da presente situação e está ciente de que a falsidade na prestação destas informações, sem prejuízo do disposto no art. 32 da Lei nº 9.430, de 1996, o sujeitará, juntamente com as demais pessoas que para ela concorrem, às penalidades previstas na legislação criminal e tributária, relativas à falsidade ideológica (art. 299 do Decreto-Lei n.º 2.848 de 7 de dezembro de 1940 - Código Penal) e ao crime contra a ordem tributária (art. 1º da Lei nº 8.137, de 27 de dezembro de 1990).

Local e data.....

Assinatura do Responsável

ANEXO II - ESPECIFICAÇÕES TÉCNICAS MÍNIMAS

ITEM	Especificação Técnica Mínima
1	**Disposições Gerais**
1.1	A solução ofertada deverá consistir em solução corporativa de proteção de endpoints, destinada à prevenção, detecção, investigação, contenção, resposta e remediação de ameaças cibernéticas em estações de trabalho, notebooks e servidores da Administração Municipal.
1.2	A solução deverá contemplar, de forma integrada, recursos de proteção de endpoints, análise comportamental, proteção contra ameaças avançadas, gerenciamento centralizado, correlação de eventos de segurança e execução de ações de contenção, resposta e remediação nos equipamentos protegidos.
1.3	A solução deverá ser composta pelos agentes de proteção, pela console de gerenciamento e pelos demais módulos e componentes necessários ao atendimento integral dos requisitos estabelecidos neste Anexo.
1.4	Todos os componentes ofertados deverão ser compatíveis entre si e operar de forma integrada, permitindo a administração centralizada da solução.
1.5	A solução deverá contemplar recurso integrado de Endpoint Detection and Response – EDR, incluindo análise de causa raiz, destinado ao monitoramento das atividades relevantes nos endpoints, à investigação das ameaças detectadas, à identificação da origem e do encadeamento das atividades relacionadas ao incidente e ao apoio à execução de ações de contenção, resposta e remediação nos equipamentos protegidos.
1.6	Os agentes, módulos e componentes utilizados no atendimento dos requisitos obrigatórios deverão integrar oficialmente a plataforma da solução ofertada, estar incluídos no licenciamento contratado e ser administrados por uma única console de gerenciamento.
1.7	A solução deverá permitir a aplicação centralizada de políticas de prevenção e detecção, bem como a visualização consolidada dos endpoints, eventos, alertas, detecções, ameaças identificadas e ações administrativas, de contenção ou de remediação executadas.
2	**Compatibilidade**
2.1	A solução deverá possuir agentes de proteção compatíveis, no mínimo, com o sistema operacional Microsoft Windows 11, em suas edições de 64 bits e versões oficialmente suportadas pela Microsoft e pelo fabricante da solução, e com Microsoft Windows Server 2016, 2019 e 2022, em suas edições de 64 bits.
2.2	A solução deverá possuir agente de proteção compatível com sistemas operacionais Linux, incluindo Ubuntu Server 22.04 LTS e Ubuntu Server 24.04 LTS, em arquitetura x86-64, oficialmente suportados pelo fabricante da solução.
2.3	O agente destinado aos sistemas Linux deverá disponibilizar, no mínimo: a) proteção antimalware em tempo real; b) verificações de segurança sob demanda e programadas; c) atualização automática dos mecanismos de detecção; d) registro de eventos de segurança; e e) gerenciamento por meio da mesma console centralizada da solução.
2.4	Para os sistemas Linux serão obrigatórias as funcionalidades estabelecidas no item 2.3, não sendo exigida equivalência integral com as funcionalidades avançadas previstas neste Anexo para os sistemas Windows e Windows Server.
2.5	A solução deverá integrar-se ao ambiente Microsoft Active Directory – AD, permitindo a sincronização ou importação de unidades organizacionais, computadores e grupos, para utilização na organização dos endpoints e na aplicação de políticas de segurança.
2.6	A comunicação entre os agentes, a infraestrutura de gerenciamento e a console deverá ser protegida por criptografia durante a transmissão, utilizando TLS 1.2 ou superior nas comunicações baseadas nesse protocolo.
2.7	Os mecanismos locais de proteção deverão permanecer ativos quando o endpoint estiver temporariamente desconectado da rede corporativa ou sem comunicação com a infraestrutura de gerenciamento da solução.
2.8	Após o restabelecimento da comunicação, os agentes deverão receber automaticamente as políticas e atualizações aplicáveis e transmitir à console os eventos e demais informações de segurança armazenados localmente durante o período de desconexão.

2.9	O licenciamento da solução deverá permitir a utilização das licenças nos endpoints abrangidos, incluindo estações de trabalho, notebooks e servidores, observadas as compatibilidades dos agentes com os respectivos sistemas operacionais.
3	**Console de Gerenciamento**
3.1	A solução deverá possuir console gráfica de gerenciamento centralizado para administração de todos os endpoints protegidos. Serão aceitas consoles em arquitetura local, em nuvem ou híbrida.
3.2	A console deverá permitir o gerenciamento simultâneo de todos os equipamentos licenciados, por meio de uma visão consolidada do ambiente protegido.
3.3	A console deverá permitir organizar os endpoints em grupos ou unidades organizacionais, possibilitando sua administração segmentada.
3.4	A console deverá permitir criar, editar, aplicar e alterar políticas de segurança de forma centralizada.
3.5	A console deverá permitir aplicar políticas distintas, no mínimo, a grupos de servidores e de estações de trabalho.
3.6	A console deverá permitir visualizar, no mínimo: a) o estado de proteção dos equipamentos; b) a versão dos agentes instalados; c) a situação das atualizações; d) a data e a hora da última comunicação; e) as ameaças e os eventos de segurança identificados; f) as detecções ou os incidentes que demandem investigação ou tratamento; e g) os equipamentos desprotegidos, inativos, desatualizados ou sem comunicação.
3.7	A console deverá permitir pesquisar, filtrar ou localizar equipamentos utilizando, no mínimo, os seguintes atributos: nome do equipamento, endereço IP, sistema operacional, usuário associado e grupo ao qual pertençam.
3.8	A console deverá permitir executar remotamente tarefas administrativas e de segurança nos equipamentos gerenciados, observadas as permissões atribuídas ao usuário responsável.
3.9	A console deverá permitir, no mínimo, iniciar ou determinar remotamente: a) verificações de segurança; b) atualização dos agentes e dos mecanismos de proteção; c) aplicação ou sincronização de políticas; d) alteração da configuração dos agentes e dos módulos de proteção por meio de políticas centralizadas, nos endpoints Windows e Windows Server; e e) ações centralizadas de tratamento e remediação previstas neste Anexo e incluídas na edição ofertada.
3.10	A console deverá permitir visualizar eventos, alertas e incidentes de segurança registrados pelos agentes e demais componentes da solução.
3.11	A solução deverá correlacionar ou relacionar os eventos associados a uma mesma ameaça detectada no endpoint, permitindo identificar a origem e o encadeamento das atividades relacionadas ao incidente, incluindo, quando presentes, vínculos entre processos, arquivos, usuários, conexões de rede e demais informações tecnicamente coletadas, com apresentação das informações necessárias à investigação e ao tratamento.
3.12	A console deverá permitir a geração de alertas ou notificações sobre eventos e incidentes de segurança, falhas de proteção e agentes desatualizados, bem como identificar os equipamentos que estejam sem comunicação.
3.13	A solução deverá permitir configurar as categorias ou condições que gerarão alertas ou notificações e definir os respectivos destinatários.
3.14	A console deverá permitir a geração de relatórios administrativos, técnicos e executivos relacionados, no mínimo, ao estado de proteção dos equipamentos, ameaças ou detecções registradas, atualizações, riscos identificados e ações executadas.
3.15	Os relatórios deverão ser visualizados pela console e exportados em pelo menos um dos formatos PDF ou CSV.
3.16	A console deverá permitir a criação de usuários administrativos com diferentes perfis, funções ou níveis de permissão, de acordo com as atribuições definidas pela Administração.
3.17	A solução deverá permitir restringir o acesso dos usuários administrativos a grupos de equipamentos, funcionalidades e operações, de acordo com o perfil atribuído a cada usuário.
3.18	O acesso à console deverá possuir suporte à autenticação multifator — MFA para os usuários administrativos.
3.19	A console deverá registrar as ações administrativas executadas, contendo identificação do usuário, ação realizada, data, horário e objeto afetado.
3.20	Os registros de auditoria deverão ser protegidos contra alteração ou exclusão por usuários sem permissão específica e permanecer disponíveis para consulta, geração de relatório ou exportação.

3.21	A solução deverá proteger suas configurações administrativas, políticas de segurança e mecanismos de gerenciamento contra alterações realizadas por usuários não autorizados.
3.22	A console deverá identificar o sistema operacional e o tipo de dispositivo gerenciado, permitindo distinguir, no mínimo, estações de trabalho e servidores.
4	**Implantação e Gerenciamento dos Agentes**
4.1	A solução deverá permitir a implantação remota e silenciosa dos agentes de proteção nos equipamentos pertencentes ao domínio da Administração Municipal.
4.2	A solução deverá possibilitar a instalação dos agentes por meio de Group Policy Objects – GPO ou por mecanismo de distribuição centralizada compatível com o ambiente Microsoft Active Directory da Administração.
4.3	A instalação deverá poder ser realizada sem intervenção individual do usuário e sem necessidade de acesso presencial a cada equipamento.
4.4	A solução deverá permitir criar pacotes de instalação contendo os agentes, módulos e configurações necessárias à proteção dos diferentes tipos de endpoint.
4.5	A solução deverá permitir que os endpoints instalados sejam registrados automaticamente na console e associados ao grupo e à política de segurança correspondentes, por meio do pacote de instalação, da tarefa de implantação, de regra de agrupamento, da integração com o Active Directory ou de outro mecanismo de configuração centralizado disponibilizado pela solução.
4.6	A solução deverá permitir identificar, por meio da console ou de mecanismo integrado, equipamentos gerenciados, desprotegidos, com agente ausente, inativo, desatualizado ou com falha de comunicação.
4.7	A solução deverá permitir atualização automática e remota dos agentes, dos mecanismos de proteção e das bases de detecção, conforme políticas definidas centralmente.
4.8	A solução deverá permitir distribuir atualizações de forma segmentada por grupos de equipamentos ou mediante políticas distintas de atualização, possibilitando sua validação em grupo reduzido antes da distribuição geral no ambiente.
4.9	A solução deverá permitir configurar horários, periodicidade e demais parâmetros de atualização, de forma a reduzir impactos sobre a rede e sobre as atividades dos usuários.
4.10	A solução deverá disponibilizar mecanismo de distribuição local intermediada, capaz de armazenar ou retransmitir internamente pacotes de instalação, atualizações e componentes da solução para outros endpoints, reduzindo o consumo de banda de internet.
4.11	O mecanismo previsto no item anterior deverá ser administrado pela solução e não poderá exigir a aquisição de plataforma independente para sua utilização.
4.12	A solução deverá permitir executar centralmente tarefas de reinstalação ou reconfiguração dos agentes, destinadas à correção de falhas ou à alteração de seus componentes, sem exigir intervenção presencial em cada equipamento.
4.13	A solução deverá permitir adicionar, remover, ativar ou desativar remotamente módulos de proteção integrantes da solução ofertada, de acordo com as políticas definidas centralmente.
4.14	A solução deverá permitir a remoção remota e silenciosa dos agentes por meio da console ou de mecanismo oficial de administração centralizada, observadas as autorizações e os mecanismos de autoproteção definidos pela Administração.
4.15	A solução deverá possuir mecanismo de autoproteção capaz de impedir a remoção, a desativação ou a alteração não autorizada dos agentes e de seus componentes, inclusive por usuários com privilégios administrativos locais, mediante senha, código, token, autorização central ou outro mecanismo equivalente disponibilizado pela solução e configurado pela Administração.
4.16	A solução deverá permitir identificar, durante o processo de instalação, a presença de softwares de segurança que possam causar incompatibilidade ou conflito com o agente ofertado.
4.17	Caso a solução disponibilize ferramenta oficial para remoção automática de softwares de segurança incompatíveis, sua utilização deverá estar incluída no licenciamento ou ser disponibilizada à Administração sem cobrança adicional.
4.18	Quando a remoção automática da solução anteriormente instalada não for possível, a empresa fornecedora deverá prestar orientação técnica remota para definição do procedimento de migração, considerando as ferramentas oficiais, as credenciais e os mecanismos de distribuição disponíveis no ambiente da Administração.
4.19	A Administração será responsável por disponibilizar, quando existentes e sob sua posse, as credenciais administrativas, senhas ou códigos de desinstalação, pacotes e ferramentas oficiais da solução anteriormente instalada necessários à execução da migração.
4.20	A implantação deverá permitir a adoção de estratégia gradual, iniciando por grupo reduzido de equipamentos para validação da remoção da solução anterior, instalação do novo agente, aplicação das políticas e comunicação com a console, antes da distribuição geral.

4.21	O processo de migração deverá buscar reduzir o período em que os equipamentos permaneçam sem proteção, evitando, sempre que tecnicamente possível, a operação simultânea de agentes de segurança incompatíveis.
4.22	As tarefas de instalação, atualização, reconfiguração ou remoção executadas pelos mecanismos centralizados da solução deverão gerar registros ou evidências técnicas que permitam identificar o equipamento, a operação executada, seu resultado e, em caso de falha, as informações de erro disponibilizadas pela solução.
5	**Funcionalidades de Proteção**
5.1	**Proteção Antimalware**
5.1.1	A solução deverá possuir proteção antimalware em tempo real para as estações de trabalho e servidores abrangidos pela contratação.
5.1.2	A proteção em tempo real deverá analisar automaticamente arquivos quando acessados, criados, copiados, modificados, gravados ou executados no endpoint.
5.1.3	A solução deverá detectar e bloquear, no mínimo, vírus, worms, trojans, spyware, adware, rootkits, ransomware e aplicações potencialmente indesejadas ou potencialmente inseguras, incluindo categorias classificadas pelo fabricante como PUA, PUP ou riskware.
5.1.4	A solução deverá permitir habilitar ou desabilitar, por política centralizada, a detecção de aplicações potencialmente indesejadas ou potencialmente inseguras.
5.1.5	A proteção antimalware deverá utilizar, de forma combinada, mecanismos de detecção por assinaturas, análise heurística e análise comportamental.
5.1.6	A proteção deverá permanecer operacional quando o endpoint estiver temporariamente desconectado da rede corporativa, da internet ou da console de gerenciamento.
5.1.7	A solução deverá analisar arquivos provenientes de unidades locais, compartilhamentos de rede e dispositivos de armazenamento removíveis quando acessados pelo endpoint.
5.1.8	A solução deverá impedir ou interromper a execução de arquivos e processos identificados como maliciosos, adotando automaticamente as ações de tratamento definidas pela política de segurança.
5.1.9	As detecções deverão ser registradas e disponibilizadas na console, contendo, no mínimo: a) identificação do endpoint; b) data e horário da detecção; c) nome ou classificação da ameaça; d) arquivo, objeto, processo ou caminho relacionado, quando aplicável; e) ação adotada pela solução; e f) resultado ou estado do tratamento.
5.1.10	Quando a detecção ocorrer com o equipamento desconectado da console, o evento deverá ser armazenado localmente e enviado após o restabelecimento da comunicação.
5.2	**Métodos de Detecção e Proteção Comportamental**
5.2.1	A solução deverá utilizar mecanismos de detecção que não dependam exclusivamente de assinaturas previamente conhecidas.
5.2.2	A solução deverá possuir mecanismo de análise comportamental capaz de monitorar continuamente processos e suas atividades durante a execução.
5.2.3	O mecanismo de análise comportamental deverá ser capaz de identificar e bloquear ou interromper atividades maliciosas com base no comportamento apresentado pelos processos e por suas atividades relacionadas.
5.2.4	A solução deverá utilizar modelos de aprendizado de máquina para auxiliar na identificação e classificação de arquivos, processos e comportamentos maliciosos, conhecidos ou desconhecidos.
5.2.5	A solução deverá possuir proteção contra ameaças desconhecidas e de dia zero, mediante utilização combinada de análise heurística, análise comportamental e modelos de aprendizado de máquina.
5.2.6	A solução deverá detectar e bloquear atividades maliciosas executadas sem a gravação prévia de arquivo malicioso convencional no disco do equipamento, incluindo ameaças executadas diretamente por processos, scripts ou memória.
5.2.7	A solução deverá monitorar e detectar a utilização maliciosa de interpretadores de comandos, mecanismos de script e ferramentas legítimas do sistema operacional, incluindo, no ambiente Windows, PowerShell e Windows Script Host.
5.2.8	A solução deverá possuir mecanismos de proteção capazes de identificar e bloquear a execução de código malicioso diretamente na memória do endpoint.
5.2.9	A solução deverá possuir mecanismos capazes de identificar e bloquear técnicas de injeção de código ou de manipulação não autorizada de processos em execução.
5.2.10	A solução deverá permitir configurar centralmente os mecanismos de proteção comportamental, seus parâmetros de operação e as ações aplicáveis às detecções.
5.2.11	A solução deverá permitir bloquear ou interromper automaticamente processos e atividades identificados como maliciosos pelos mecanismos de proteção comportamental.

5.2.12	Os eventos gerados pela proteção comportamental deverão ser enviados à console, contendo, no mínimo: a) endpoint afetado; b) processo, aplicação ou atividade envolvida; c) data e horário; d) comportamento ou atividade detectada; e) classificação ou severidade, quando atribuída pela solução; e f) ação executada e respectivo resultado.
5.2.13	A proteção comportamental deverá permanecer operacional quando o endpoint estiver temporariamente desconectado da console, ainda que determinados recursos de reputação, correlação ou análise em nuvem dependam de conectividade.
5.2.14	A solução deverá permitir configurar, mediante política centralizada, exclusões específicas para os mecanismos de proteção comportamental, utilizando, no mínimo, processo, arquivo ou caminho como critérios de identificação, com acesso restrito aos usuários administrativos autorizados.
5.3	**Proteção Contra Ransomware**
5.3.1	A solução deverá possuir mecanismo específico de prevenção, detecção, bloqueio e remediação de ataques de ransomware nos endpoints protegidos.
5.3.2	O mecanismo deverá utilizar análise comportamental para identificar atividades anormais ou não autorizadas de criptografia, alteração, exclusão ou substituição em massa de arquivos.
5.3.3	A solução deverá detectar ataques de ransomware conhecidos e desconhecidos, sem depender exclusivamente de assinaturas previamente existentes.
5.3.4	A solução deverá monitorar os processos em execução e bloquear ou interromper automaticamente aqueles identificados como responsáveis por atividade de ransomware, impedindo a continuidade das alterações maliciosas.
5.3.5	O monitoramento comportamental deverá abranger as atividades realizadas pelos processos sobre os arquivos armazenados localmente no endpoint protegido.
5.3.6	A solução deverá possuir mecanismo de remediação capaz de restaurar arquivos armazenados localmente no endpoint que tenham sido modificados, danificados ou criptografados em decorrência da atividade de ransomware detectada, mediante utilização de cópias protegidas, reversão ou rollback das alterações.
5.3.7	O mecanismo de remediação deverá integrar a solução de proteção de endpoints e não poderá depender exclusivamente de solução externa de backup para recuperação dos arquivos afetados durante a atividade detectada.
5.3.8	A remediação deverá ser realizada automaticamente após o bloqueio da atividade maliciosa ou iniciada centralmente pelo administrador, de acordo com o modo de operação disponibilizado pela solução.
5.3.9	As cópias temporárias, os registros e as demais informações mantidas pelo mecanismo de remediação deverão ser protegidos contra alteração ou exclusão por processos não autorizados.
5.3.10	A proteção contra ransomware e os mecanismos locais de remediação deverão permanecer operacionais quando o endpoint estiver temporariamente desconectado da rede corporativa, da internet ou da console de gerenciamento.
5.3.11	A solução deverá permitir habilitar, configurar e aplicar centralmente as políticas de proteção e remediação de ransomware, bem como estabelecer exclusões autorizadas para processos, arquivos ou diretórios.
5.3.12	Os eventos de ransomware deverão ser registrados e disponibilizados na console, contendo, no mínimo: a) identificação do endpoint afetado; b) data e horário da detecção; c) processo ou aplicação responsável pela atividade; d) usuário relacionado à execução, quando identificado; e) arquivo, diretório ou objeto relacionado ao evento, quando essa informação estiver disponível; f) ação de bloqueio executada; e g) resultado ou estado da remediação.
5.3.13	Quando o endpoint estiver desconectado da console, os eventos de ransomware deverão ser armazenados localmente e transmitidos após o restabelecimento da comunicação.
5.3.14	A solução deverá gerar alerta ou notificação aos administradores quando detectar atividade de ransomware, informando, no mínimo, o endpoint afetado e a ação adotada.
5.4	**Proteção contra Exploração de Vulnerabilidades**
5.4.1	A solução deverá possuir mecanismo de proteção contra tentativas de exploração de vulnerabilidades existentes no sistema operacional e nas aplicações instaladas nos endpoints.
5.4.2	O mecanismo deverá ser capaz de detectar e bloquear técnicas associadas à exploração de vulnerabilidades conhecidas e desconhecidas, incluindo ameaças de dia zero, sem depender

	exclusivamente da existência de assinatura específica para a vulnerabilidade ou para o código malicioso utilizado no ataque.
5.4.3	A solução deverá monitorar processos e aplicações durante sua execução, identificando comportamentos e técnicas associados à exploração de vulnerabilidades.
5.4.4	A solução deverá possuir mecanismos capazes de identificar e bloquear tentativas de exploração que envolvam: a) corrupção ou manipulação indevida de memória; b) injeção ou execução não autorizada de código em processos legítimos; e c) execução de código malicioso sem a gravação prévia de arquivo malicioso convencional no disco.
5.4.5	A proteção deverá abranger componentes do sistema operacional e aplicações comumente utilizadas como vetores de exploração, incluindo, no mínimo: a) navegadores de internet; b) suítes de produtividade e editores de documentos; c) leitores de arquivos PDF; e d) interpretadores de comandos e mecanismos de script.
5.4.6	Ao identificar tentativa de exploração, a solução deverá bloquear ou interromper a atividade maliciosa, impedindo a continuidade da execução relacionada ao ataque.
5.4.7	A solução deverá permitir configurar centralmente os mecanismos de proteção contra exploração de vulnerabilidades e aplicar políticas distintas a grupos de equipamentos.
5.4.8	A solução deverá permitir configurar centralmente exclusões ou exceções para aplicações que apresentem incompatibilidade com determinado mecanismo de proteção, restringindo essa operação aos usuários administrativos autorizados.
5.4.9	A ação administrativa de criação ou alteração da política que contenha exclusões ou exceções deverá permanecer registrada na trilha de auditoria da solução.
5.4.10	Os eventos relacionados à exploração de vulnerabilidades deverão ser registrados e disponibilizados na console, contendo, no mínimo: a) identificação do endpoint afetado; b) data e horário da detecção; c) processo ou aplicação envolvida; d) técnica, comportamento ou categoria identificada; e) ação executada pela solução; e f) resultado ou estado do bloqueio ou tratamento.
5.4.11	A proteção contra exploração de vulnerabilidades deverá permanecer operacional quando o endpoint estiver temporariamente desconectado da rede corporativa, da internet ou da console de gerenciamento.
5.4.12	Os eventos gerados durante o período de desconexão deverão ser armazenados localmente e transmitidos à console após o restabelecimento da comunicação.
5.5	**Verificações, Quarentena e Tratamento de Ameaças**
5.5.1	A solução deverá permitir a realização de verificações de segurança sob demanda, programadas e iniciadas remotamente pela console de gerenciamento.
5.5.2	A solução deverá permitir configurar centralmente a periodicidade, os horários, os objetos analisados e as ações aplicáveis às ameaças identificadas nas verificações.
5.5.3	A solução deverá permitir que arquivos identificados como maliciosos ou potencialmente maliciosos sejam automaticamente bloqueados ou colocados em quarentena, conforme a política de segurança aplicada, impedindo sua execução.
5.5.4	A console deverá permitir consultar e administrar centralmente os objetos colocados em quarentena, incluindo sua restauração e exclusão por usuário administrativo autorizado.
5.5.5	A solução deverá permitir definir e aplicar centralmente ações de bloqueio, desinfecção, quarentena e, quando aplicável ao tipo de ameaça ou objeto, exclusão automática.
5.5.6	A solução deverá permitir configurar centralmente exclusões de verificação baseadas, no mínimo, em arquivo, diretório, extensão e processo ou aplicação.
5.5.7	Os resultados das verificações e as ações de tratamento executadas deverão ser registrados e disponibilizados na console, contendo, no mínimo, o endpoint, o tipo e a data da verificação, o resultado, as ameaças identificadas e as ações executadas.
5.5.8	A console deverá apresentar visão centralizada dos endpoints com ameaças não tratadas ou falhas de remediação, permitindo ao administrador iniciar nova verificação e executar as ações de tratamento disponibilizadas pela solução.
5.6	**Proteção para Navegação Web e Ameaças Originadas da Internet**
5.6.1	A solução deverá possuir mecanismo de proteção da navegação web executado nos endpoints protegidos, sem dependência de equipamento adicional de segurança de rede.

5.6.2	A solução deverá utilizar serviços de reputação ou classificação de endereços eletrônicos para identificar e bloquear o acesso a páginas, domínios ou endereços classificados como maliciosos, fraudulentos ou relacionados a phishing.
5.6.3	A solução deverá monitorar as conexões web realizadas por protocolos HTTP e HTTPS, aplicando mecanismos de reputação e controle aos endereços acessados e analisando arquivos, scripts e demais conteúdos disponibilizados ao endpoint para identificação de ameaças.
5.6.4	A solução deverá identificar e bloquear o download ou a execução de arquivos maliciosos provenientes da navegação web.
5.6.5	A solução deverá permitir autorizar ou bloquear o acesso a páginas de internet com base em categorias de conteúdo mantidas pelo fabricante.
5.6.6	A solução deverá permitir criar e administrar centralmente listas de endereços, domínios ou páginas permitidos e bloqueados.
5.6.7	As configurações de proteção e controle da navegação deverão ser definidas por políticas centralizadas e aplicadas a grupos de equipamentos.
5.6.8	A proteção contra endereços maliciosos, phishing e downloads maliciosos deverá permanecer ativa quando o endpoint estiver conectado à internet fora da rede corporativa, independentemente de comunicação contínua com a rede interna da Administração.
5.6.9	Os bloqueios relacionados a endereços, páginas e arquivos maliciosos deverão ser registrados e disponibilizados na console, contendo, no mínimo, a identificação do endpoint, o endereço ou domínio relacionado, a data e o horário e a ação executada.
5.7	**Controle de Dispositivos Removíveis**
5.7.1	A solução deverá permitir controlar centralmente o acesso a dispositivos de armazenamento removíveis conectados aos endpoints.
5.7.2	A solução deverá permitir aplicar políticas distintas de controle de dispositivos a diferentes grupos de equipamentos.
5.7.3	As políticas deverão permitir definir, no mínimo, os seguintes níveis de acesso aos dispositivos de armazenamento removíveis: a) acesso permitido; e b) acesso bloqueado.
5.7.4	A solução deverá permitir criar exceções para dispositivos autorizados com base em identificador técnico que permita individualizar o dispositivo, como Device ID, Hardware ID — HWID ou número de série.
5.7.5	As exceções deverão ser configuradas centralmente e aplicadas a equipamentos ou grupos definidos pela Administração.
5.7.6	A solução deverá registrar e disponibilizar na console os eventos de restrição, bloqueio ou violação das políticas de controle de dispositivos, contendo, no mínimo, a identificação do endpoint, do usuário e do dispositivo, a data e o horário e a ação executada.
5.7.7	As políticas de controle de dispositivos deverão permanecer aplicadas quando o endpoint estiver temporariamente desconectado da rede corporativa ou da console de gerenciamento.
5.7.8	As alterações realizadas nas políticas e nas exceções de controle de dispositivos deverão ser distribuídas centralmente aos endpoints, sem necessidade de configuração individual em cada equipamento.
5.8	**Autoproteção da Solução**
5.8.1	Nos endpoints Windows e Windows Server, a solução deverá possuir mecanismo de autoproteção contra adulteração ou manipulação não autorizada dos agentes e de seus componentes de segurança.
5.8.2	A autoproteção deverá impedir a desativação ou interrupção não autorizada dos processos, serviços e mecanismos de proteção executados no endpoint.
5.8.3	A solução deverá impedir a desinstalação do agente por usuário não autorizado, inclusive quando este possuir privilégios administrativos locais, mediante exigência de senha, token ou autorização específica administrada pela solução.
5.8.4	A solução deverá proteger os arquivos, processos, serviços, configurações e políticas locais do agente contra alteração ou exclusão não autorizada.
5.8.5	A console deverá permitir habilitar e configurar centralmente os mecanismos de autoproteção e a proteção contra desinstalação não autorizada dos agentes.
5.8.6	Quando os mecanismos de autoproteção gerarem eventos ou alertas relacionados a tentativas de desativação, interrupção, alteração ou desinstalação não autorizada, essas informações deverão permanecer disponíveis para consulta local ou na console de gerenciamento, conforme a arquitetura da solução.
5.8.7	Os mecanismos locais de autoproteção deverão permanecer ativos quando o endpoint estiver temporariamente desconectado da rede corporativa ou da console de gerenciamento.

6	**Detecção, Investigação e Resposta em Endpoints - EDR**
6.1	**Endpoint Detection and Response - EDR**
6.1.1	A solução deverá possuir recurso integrado de Endpoint Detection and Response – EDR, incluindo análise de causa raiz, administrado pela mesma plataforma utilizada para proteção e gerenciamento dos endpoints.
6.1.2	O recurso será obrigatório para os endpoints Windows e Windows Server abrangidos pela contratação. Para os sistemas Linux permanecerão obrigatórias somente as funcionalidades estabelecidas nos itens 2.3 e 2.4.
6.1.3	A solução deverá monitorar e registrar atividades relevantes relacionadas às ameaças detectadas nos endpoints, incluindo processos, arquivos, usuários e conexões de rede, de acordo com a natureza do evento e com as informações coletadas pela plataforma.
6.1.4	A solução deverá relacionar os eventos associados a uma mesma ameaça, possibilitando identificar o processo originador, os processos derivados e as demais atividades vinculadas à detecção.
6.1.5	A solução deverá apresentar representação gráfica da cadeia de execução ou do desenvolvimento da ameaça detectada, permitindo visualizar o relacionamento entre os eventos e objetos envolvidos.
6.1.6	A representação da cadeia da ameaça deverá apresentar, quando aplicáveis ao evento: a) identificação do endpoint afetado; b) data e horário dos eventos; c) usuário relacionado à atividade; d) processo originador e processos derivados; e) arquivos ou objetos relacionados; f) hashes ou outros identificadores técnicos; g) conexões ou endereços de rede relacionados; h) classificação ou severidade da detecção; e i) ações executadas pela solução ou pelo administrador.
6.1.7	A console deverá permitir consultar, pesquisar ou filtrar as detecções e as respectivas informações de investigação, no mínimo, por período, endpoint, ameaça ou detecção e classificação ou severidade.
6.1.8	A solução deverá permitir iniciar centralmente ações de tratamento ou remediação nos endpoints Windows e Windows Server, contemplando, no mínimo: a) execução de verificação de segurança; b) tratamento de objetos detectados ou não tratados, mediante quarentena, exclusão ou desinfecção, conforme aplicável ao tipo de objeto e à ameaça; c) atualização ou reaplicação da política de segurança no equipamento afetado; e d) contenção do equipamento afetado, mediante isolamento remoto de suas comunicações de rede, preservando as conexões necessárias à comunicação com a infraestrutura de gerenciamento da solução.
6.1.9	As ações previstas no item 6.1.8 deverão ser iniciadas pela console de gerenciamento e observar as permissões atribuídas ao usuário administrativo.
6.1.10	A solução deverá permitir o bloqueio ou a interrupção automática de processos, arquivos ou atividades identificados como maliciosos pelos mecanismos de proteção.
6.1.11	As ações de tratamento e remediação executadas deverão ser registradas pela solução, contendo a identificação do endpoint, a ação realizada, a data e o horário e o respectivo resultado.
6.1.12	A console deverá apresentar informações contextuais sobre a ameaça detectada que auxiliem o administrador na compreensão da cadeia de execução e na definição das medidas de tratamento.
6.1.13	Os agentes e componentes utilizados para proteção, coleta de eventos, análise de causa raiz e remediação deverão integrar oficialmente a plataforma da solução ofertada e ser administrados pela mesma console, sem necessidade de aquisição ou administração de console independente.
6.2	**Serviços de Reputação e Inteligência de Ameaças**
6.2.1	A solução deverá utilizar serviços de reputação e inteligência de ameaças mantidos pelo fabricante, integrados aos mecanismos de aprendizado de máquina, análise heurística ou análise comportamental da solução, para auxiliar na identificação de arquivos, objetos ou atividades suspeitas.
6.2.2	Os serviços deverão complementar os mecanismos locais de proteção, contribuindo para a identificação e classificação de ameaças conhecidas e desconhecidas.
6.2.3	A solução deverá permitir a comunicação automática com a infraestrutura de análise do fabricante, incluindo o envio ou a consulta de hashes, metadados ou outros identificadores técnicos necessários à obtenção de informações de reputação ou veredito.
6.2.4	Quando a arquitetura da solução contemplar o envio de arquivos, objetos ou amostras suspeitas para análise, essa funcionalidade deverá ser controlada pelas políticas definidas pela Administração.

6.2.5	Os vereditos e as informações obtidos dos serviços do fabricante deverão ser utilizados pelos mecanismos de proteção para classificar o objeto ou a atividade e, quando identificado risco, bloquear, colocar em quarentena ou impedir sua execução.
6.2.6	Os serviços utilizados deverão integrar oficialmente a plataforma ou a infraestrutura de proteção da solução ofertada, sem exigir da Administração a aquisição ou administração de console independente.
7	**Atualizações da Solução**
7.1	A solução deverá fornecer, durante toda a vigência contratual e sem custos adicionais para a Administração, atualizações das bases e conteúdos de detecção de ameaças, dos modelos de análise, dos mecanismos de proteção, dos agentes e dos demais componentes necessários ao funcionamento da solução.
7.2	As atualizações das bases e dos conteúdos de detecção e dos mecanismos locais de proteção deverão ser obtidas e aplicadas automaticamente pelos agentes, de acordo com as políticas definidas centralmente, sem necessidade de intervenção individual nos equipamentos protegidos.
7.3	A solução deverá permitir gerenciar centralmente a obtenção e a distribuição das atualizações destinadas aos agentes instalados.
7.4	A plataforma de gerenciamento deverá permitir configurar políticas de atualização distintas por grupo de equipamentos, incluindo: a) periodicidade ou horário de atualização; b) origem ou local utilizado para obtenção das atualizações, incluindo servidores do fabricante e mecanismos internos de distribuição disponibilizados pela solução; e c) distribuição de versões dos agentes por etapas, grupos de equipamentos, políticas distintas de atualização ou mecanismo equivalente, possibilitando sua validação em grupo reduzido antes da distribuição geral.
7.5	A plataforma de gerenciamento deverá permitir consultar, para cada equipamento protegido, no mínimo: a) versão do agente instalado; b) situação das bases ou dos conteúdos de detecção; c) data e horário da última atualização bem-sucedida; e d) existência de falha ou pendência de atualização.
7.6	Os equipamentos que estiverem desligados, desconectados ou temporariamente sem comunicação com a plataforma deverão retomar ou realizar automaticamente o processo de atualização após o restabelecimento da comunicação, conforme a política de atualização aplicável.
7.7	A plataforma deverá disponibilizar informações sobre o resultado das tarefas ou processos de atualização, permitindo identificar os equipamentos atualizados, desatualizados ou com falha e, para as falhas registradas, a data e as informações de erro disponibilizadas pela solução.
7.8	Durante todo o período de licenciamento, a solução deverá permanecer regular, ativa e apta à utilização de todas as funcionalidades exigidas neste Anexo, as quais deverão estar abrangidas pela edição e pelos módulos fornecidos.
7.9	A Administração deverá ter direito, durante todo o período de licenciamento, às atualizações, correções de segurança, correções de falhas e versões abrangidas pelo licenciamento fornecido, sem custos adicionais.
7.10	Eventuais inconsistências relacionadas à ativação, à validade ou ao funcionamento das licenças fornecidas deverão ser regularizadas pela empresa fornecedora, de modo a assegurar a continuidade de utilização da solução durante todo o período contratado.
8	**Apoio Técnico à Implantação**
8.1	A solução deverá contemplar apoio técnico remoto à equipe da Administração durante a fase inicial de ativação, configuração e implantação.
8.2	O apoio técnico remoto deverá abranger, quando solicitado pela Administração: a) orientação para ativação e disponibilização das licenças; b) orientação para configuração inicial da console de gerenciamento; c) orientação para criação ou ajuste inicial das políticas de segurança; d) orientação para definição dos pacotes e dos parâmetros de instalação dos agentes; e) orientação para integração da solução com o ambiente tecnológico da Administração; f) apoio à configuração dos mecanismos de implantação remota, silenciosa e centralizada; g) apoio à validação da comunicação entre os agentes e a console de gerenciamento; h) orientação para remoção ou substituição da solução anteriormente instalada, observadas as ferramentas e os procedimentos oficialmente disponibilizados pelos respectivos fabricantes; e i) apoio ao diagnóstico de falhas diretamente relacionadas à ativação, configuração inicial e comunicação dos agentes durante a fase de implantação.

8.3	A instalação e a distribuição dos agentes nos equipamentos serão executadas pela equipe técnica da Administração, utilizando os mecanismos disponibilizados pela solução, cabendo à empresa fornecedora prestar as orientações e o apoio técnico remoto necessários durante a fase inicial.
8.4	O apoio técnico remoto poderá ser executado pela CONTRATADA, pelo fabricante da solução ou por parceiro tecnicamente habilitado, admitida a combinação dessas modalidades, permanecendo a CONTRATADA integralmente responsável pelo cumprimento da obrigação.
8.5	Durante a configuração inicial, deverá ser realizado repasse remoto de conhecimento à equipe da Administração, abrangendo, no mínimo: a) acesso e utilização básica da console; b) criação, aplicação e alteração de políticas de segurança; c) acompanhamento da situação dos endpoints; d) consulta de eventos, detecções, alertas e relatórios; e) execução de verificações de segurança, consulta e tratamento de objetos detectados e atualização ou reaplicação de políticas de segurança; e f) abertura e acompanhamento de chamados técnicos.
8.6	O repasse de conhecimento não será caracterizado como treinamento formal, não sendo exigidos carga horária mínima, realização presencial, avaliação, certificação ou emissão de certificado.
8.7	Durante todo o período de licenciamento, a Administração deverá ter acesso aos canais regulares de suporte técnico disponibilizados para a solução ofertada, os quais poderão ser mantidos pela empresa fornecedora, pelo fabricante ou por parceiro autorizado, bem como à documentação técnica e à base de conhecimento disponibilizadas pelo fabricante para a edição e o nível de licenciamento fornecidos.
8.8	O suporte regular previsto no item anterior destina-se ao registro e ao tratamento de dúvidas, falhas ou inconsistências relacionadas ao funcionamento da solução, às licenças, aos agentes, à console de gerenciamento e aos demais componentes fornecidos.
8.9	Não será exigida modalidade premium de suporte, atendimento dedicado ou plano comercial específico, desde que sejam assegurados o suporte regular associado ao licenciamento e o apoio técnico remoto à implantação estabelecido neste item.

APÊNDICE A – MATRIZ DE COMPROVAÇÃO DOS REQUISITOS TÉCNICOS

1. Finalidade

1.1. A presente matriz tem por finalidade subsidiar a análise técnica da solução ofertada pela licitante provisoriamente classificada em primeiro lugar, mediante comprovação documental de requisitos essenciais do Anexo II – Especificações Técnicas Mínimas.

1.2. A matriz contém somente os requisitos considerados prioritários para a classificação técnica da solução. Seu preenchimento não afasta a obrigatoriedade de atendimento integral a todos os requisitos estabelecidos no Anexo II.

1.3. Para cada bloco, a licitante deverá indicar documentação técnica oficial do fabricante correspondente à solução, à edição, ao nível de licenciamento, aos módulos e aos componentes efetivamente ofertados, incluindo manual, guia técnico, ficha técnica, matriz de funcionalidades, base oficial de conhecimento ou página oficial do produto.

1.4. A referência deverá identificar o título do documento ou o endereço eletrônico oficial e a página, o capítulo, a seção ou o tópico em que a informação possa ser localizada. Poderão ser indicadas múltiplas referências na mesma linha.

1.5. Não serão consideradas suficientes, isoladamente, declarações emitidas pela própria licitante, materiais de revendedores ou distribuidores, publicações em blogs ou páginas sem vínculo oficial com o fabricante.

1.6. A Administração poderá realizar diligências para esclarecer ou confirmar as informações apresentadas e o atendimento a qualquer requisito do Anexo II, inclusive àqueles não individualizados nesta matriz, observadas as disposições do edital e da legislação aplicável. A diligência poderá incluir a solicitação de documentação complementar preexistente, declaração técnica do fabricante ou de parceiro oficialmente autorizado e, quando previsto no edital, demonstração das funcionalidades da solução, sem alteração da edição, dos módulos ou dos componentes originalmente ofertados.

1.7. A documentação indicada deverá corresponder à solução, à edição, ao nível de licenciamento, aos módulos e aos componentes efetivamente incluídos na proposta, não sendo aceita comprovação baseada exclusivamente em funcionalidade pertencente a edição superior, módulo adicional ou componente não ofertado.

2. Identificação da Solução Ofertada

INFORMAÇÃO	PREENCHIMENTO PELA LICITANTE
Razão Social da Licitante	
Fabricante da Solução	
Nome Comercial Completo da Solução	
Edição ou Nível de Licenciamento	

Módulos e componentes incluídos	
Código/SKU da solução ofertada	
Endereço Eletrônico oficial da solução	

3. Matriz de Comprovação

Nº	ITENS DO ANEXO II	REQUISITO TÉCNICO ESSENCIAL	ATENDE	DOCUMENTO OFICIAL, PÁGINA/SEÇÃO OU URL
1	1.1 a 1.7; 6.1.1; 6.1.13	Plataforma corporativa integrada de proteção de endpoints, composta por EPP e EDR, com agentes, módulos e console centralizada administrados pela mesma plataforma, sem necessidade de console independente.	☐ Sim ☐ Não	
2	2.1 a 2.4	Agentes compatíveis com Microsoft Windows 11, em suas edições de 64 bits e versões oficialmente suportadas pela Microsoft e pelo fabricante, Windows Server 2016, 2019 e 2022 e Ubuntu Server 22.04 LTS e 24.04 LTS, com proteção antimalware em tempo real no Linux, verificações programadas e sob demanda, atualização automática, registro de eventos e gerenciamento pela mesma console.	☐ Sim ☐ Não	
3	2.5; 3.3 a 3.5	Integração ou sincronização com Microsoft Active Directory, incluindo unidades organizacionais, computadores ou grupos, com organização dos endpoints e aplicação centralizada de políticas.	☐ Sim ☐ Não	
4	4.1 a 4.5	Implantação remota e silenciosa dos agentes, com pacotes de instalação configuráveis e registro automático dos endpoints na console, sem intervenção individual dos usuários.	☐ Sim ☐ Não	
5	4.8 a 4.11; 7.4	Distribuição segmentada de atualizações e versões dos agentes, por grupos, políticas, etapas ou mecanismo equivalente e mecanismo de distribuição local intermediada para pacotes, atualizações e componentes, reduzindo o consumo de banda de internet.	☐ Sim ☐ Não	
6	3.16 a 3.20	Controle de acesso administrativo com diferentes perfis ou níveis de permissão, autenticação multifator para acesso à console e registro das ações administrativas.	☐ Sim ☐ Não	
7	4.14 e 4.15; 5.8.1 a 5.8.7	Autoproteção dos agentes em Windows e Windows Server, incluindo proteção de processos, serviços, arquivos e configurações e impedimento de desinstalação por administrador local sem senha, token ou autorização específica.	☐ Sim ☐ Não	

8	5.1.1 a 5.1.10 e 5.2.1 a 5.2.5	Proteção multicamada mediante utilização combinada de assinaturas, análise heurística, análise comportamental e aprendizado de máquina para ameaças conhecidas, desconhecidas e de dia zero.	☐ Sim ☐ Não	
9	5.2.6 a 5.2.13; 5.4.1 a 5.4.7	Proteção contra ataques sem arquivo, uso malicioso de PowerShell ou mecanismos de script, execução maliciosa em memória e exploração de vulnerabilidades conhecidas e desconhecidas.	☐ Sim ☐ Não	
10	5.3.1 a 5.3.10	Proteção específica contra ransomware, com detecção comportamental, bloqueio automático e restauração de arquivos locais por cópias protegidas, reversão ou rollback, sem dependência exclusiva de backup externo.	☐ Sim ☐ Não	
11	5.5.3 a 5.5.8	Administração centralizada da quarentena, com consulta, restauração e exclusão de objetos por usuário autorizado e identificação de ameaças não tratadas ou falhas de remediação.	☐ Sim ☐ Não	
12	5.6.1 a 5.6.9	Proteção web executada no endpoint, com reputação de endereços, bloqueio de phishing e downloads maliciosos, controle por categorias e funcionamento fora da rede corporativa.	☐ Sim ☐ Não	
13	5.7.1 a 5.7.8	Controle centralizado de dispositivos de armazenamento removíveis, com permissões de acesso permitido ou bloqueado, exceções por identificação individual e registro das violações de política.	☐ Sim ☐ Não	
14	6.1.1 a 6.1.7 e 6.1.13	EDR integrado à plataforma e administrado pela mesma console da solução de proteção de endpoints, com análise de causa raiz, correlação dos eventos associados à ameaça e representação gráfica da cadeia de execução ou do desenvolvimento da ameaça.	☐ Sim ☐ Não	
15	6.1.8 a 6.1.12	Execução centralizada de ações de contenção, resposta e remediação, incluindo isolamento remoto do endpoint afetado, verificações de segurança, tratamento de objetos detectados, atualização ou reaplicação de políticas e registro das ações executadas.	☐ Sim ☐ Não	
16	6.2.1 a 6.2.6	Serviços integrados de reputação e inteligência de ameaças mantidos pelo fabricante, com consulta automática por hashes ou metadados e utilização dos vereditos pelos mecanismos de proteção.	☐ Sim ☐ Não	

4. Declaração de Atendimento Integral

A licitante declara que a solução ofertada atende integralmente a todos os requisitos estabelecidos no Anexo II – Especificações Técnicas Mínimas, inclusive aqueles não individualizados nesta Matriz de Comprovação, e que todos os produtos, módulos e níveis de licenciamento necessários encontram-se incluídos na proposta apresentada.

Local e data: _____

Razão social: _____

Nome do representante: _____

Assinatura: _____