ESTADO DE MINAS GERAIS

SECRETARIA DE ESTADO DE PLANEJAMENTO E GESTÃO

Central de Compras

Versão v.30.11.2020.

Processo SEI nº 1500.01.0113446/2022-67

EDITAL DE LICITAÇÃO

PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇOS Nº 287/*2022*

PLANEJAMENTO SIRP Nº 287/2022

Regime de Execução Indireta: *Empreitada por preço global*- Prestação de Serviços (sem dedicação exclusiva de mão de obra)

Critério de Julgamento: *menor preço por lote*

Modo de disputa: Aberto e fechado

Licitação com lote(s) aberto (s) à ampla concorrência

Objeto: Aquisição de licenças de uso de solução corporativa de Segurança de Endpoint's e Servidores para múltiplas plataformas incluindo garantia, suporte e atualização para utilização no parque tecnológico do Governo do Estado de Minas Gerais, sob demanda, futura e eventual

EDITAL

1. PREÂMBULO

O ESTADO DE MINAS GERAIS, por intermédio do Secretaria de Estado de Planejamento e Gestão torna pública a realização de licitação na modalidade pregão eletrônico do tipo menor preço, no modo de disputa aberto e fechado, em sessão pública, por meio do site www.compras.mg.gov.br, visando o registro de preços para eventual contratação de serviços de licenças de uso de solução corporativa de Segurança de Endpoint's e Servidores para múltiplas plataformas incluindo garantia, suporte e atualização para utilização no parque tecnológico do Governo do Estado de Minas Gerais, sob demanda, futura e eventual , nos termos da **Lei Federal** n° 10.520, de 17 de Julho de 2002 e da **Lei Estadual** n°. 14.167, de 10 de Janeiro de 2002 e dos **Decretos Estaduais** n° 48.012, de 22 de julho de 2020 e nº 46.311 de 16 de setembro de 2013.

Este pregão será amparado pela **Lei Complementar** nº. 123, de 14 de dezembro de 2006 e pelas **Leis Estaduais** nº. 13.994, de 18 de setembro de 2001, nº. 20.826, de 31 de julho de 2013, pelos **Decretos Estaduais** nº. 45.902, de 27 de janeiro de 2012, nº 46.559, de 16 de julho de 2014, nº 47.437, 26 de junho de 2018, nº. 47.524, de 6 de novembro de 2018, nº. 37.924, de 16 de maio de 1996, nº 47.727, de 02 de outubro de 2019, pela **Resolução SEPLAG** nº 93, de 28 novembro de 2018, pelas **Resoluções Conjuntas SEPLAG/SEF** n.º 3.458, de 22 de julho de 2003 e nº 8.898 de 14 de junho 2013, pela **Resolução Conjunta SEPLAG/SEF/JUCEMG** n.º 9.576, de 6 de julho 2016, aplicando-se subsidiariamente, a **Lei Federal n° 8.666,** de 21 de Junho de 1993, e as condições estabelecidas nesse edital e seus anexos, que dele constituem parte integrante e inseparável para todos os efeitos legais.

1.1. O pregão será realizado por Pregoeiro e Equipe de Apoio designados na Resolução nº 077, de 20 de outubro de 2022.

1.1.1. A sessão de pregão terá início **no dia 19 de abril de 2023, às 10:00 horas.** Todas as referências de tempo no Edital, no aviso e durante a sessão pública, observarão obrigatoriamente o horário de Brasília - DF e, dessa forma, serão registradas no sistema e na documentação relativa ao certame.

1.2. A sessão de pregão será realizada no sítio eletrônico de compras do Governo do Estado de Minas Gerais: www.compras.mg.gov.br.

2. DO OBJETO

2.1. A presente licitação tem por objeto o registro de preços para a eventual contratação dos serviços de aquisição de licenças de uso de solução corporativa de Segurança de Endpoint's e Servidores para múltiplas plataformas incluindo garantia, suporte e atualização para utilização no parque tecnológico do Governo do Estado de Minas Gerais, sob demanda, futura e eventual, conforme especificações constantes no Anexo I - Termo de Referência, e de acordo com as exigências e quantidades estabelecidas neste edital e seus anexos.

2.2. Em caso de divergência entre as especificações do objeto descritas no Portal de Compras e as especificações técnicas constantes no Anexo I - Termo de Referência, o licitante deverá obedecer a este último.

3. DOS ÓRGÃOS PARTICIPANTES E NÃO PARTICIPANTE

3.1. Órgão/entidade Gerenciador(a):

3.1.1. O órgão/entidade gerenciador(a) será o/a Secretaria de Planejamento e Gestão, por intermédio do Centro de Serviços Compartilhados (CSC).

3.2. Órgãos participantes:

3.2.1. Os órgãos e entidades da Administração Pública a seguir são participantes e integram todo o procedimento licitatório e a Ata de Registro de Preços:

3.2.1.1. **ADVOCACIA GERAL DO ESTADO**

3.2.1.2. **SECRET. DE ESTADO DE INFRAESTRUTURA E MOBILIDADE**

3.2.1.3. **SECRETARIA DE ESTADO DA SAUDE**

3.2.1.4. **CORPO DE BOMBEIROS MILITAR DE MINAS GERAIS**

3.2.1.5. **SECRETARIA DE ESTADO DE JUSTICA E SEGURANCA PUBLICA**

3.2.1.6. **SECRETARIA DE ESTADO DE GOVERNO**

3.2.1.7. **FUNDACAO JOAO PINHEIRO**

3.2.1.8. **FUND. DE AMPARO A PESQ. DO ESTADO DE MINAS GERAIS**

3.2.1.9. **FUNDACAO HOSPITALAR DO ESTADO DE MINAS GERAIS**

3.2.1.10. **DEPARTAMENTO DE EDIFICACOES E ESTRADAS DE RODAGEM**

3.2.1.11. **UNIVERSIDADE ESTADUAL DE MONTES CLAROS**

3.2.1.12. **FUNDACAO CENTRO DE HEMATOLOGIA E HEMOTERAPIA DE MG**

3.2.1.13. **INSTITUTO DE METROLOGIA E QUALIDADE DE MG**

3.2.1.14. **UNIVERSIDADE DO ESTADO DE MINAS GERAIS**

3.2.1.15. **SECRETARIA DE ESTADO DE CULTURA E TURISMO**

3.2.1.16. **FUNDACAO EDUCACIONAL CAIO MARTINS**

3.3. Órgãos não participantes:

3.3.1. A Ata de Registro de Preços, durante sua vigência, poderá ser utilizada por qualquer órgão ou entidade da Administração Pública Direta, Autárquica e Fundacional do Estado de Minas Gerais, que não tenha participado do certame licitatório, mediante consulta prévia para manifestação sobre a possibilidade de adesão e autorização do órgão gerenciador, inclusive quanto ao quantitativo, e submeter à anuência do fornecedor beneficiário, o qual deve optar pela aceitação ou não do

fornecimento decorrente da adesão, desde que não prejudique as obrigações presentes e futuras decorrentes da Ata, assumidas com o órgão gerenciador e os órgãos participantes.

3.3.2. A Administração Pública Direta, Autárquica e Fundacional de outros entes federativos, poderão igualmente utilizar-se da Ata de Registro de Preços, como órgão ou entidade não participante, mediante prévia anuência do órgão gerenciador, desde que observadas as condições estabelecidas no item 3.3.1 e no Decreto Estadual nº 46.311, de 16 de setembro de 2013.

3.3.3. A adesão deverá ser devidamente justificada no processo administrativo do órgão ou entidade não participante, pertinente à licitação, demonstrando a vantagem econômica na adesão à Ata, mencionando ainda a similitude de condições, tempestividade do prazo, suficiência das quantidades e qualidades dos serviços a serem prestados, respeitando, no que couber, as condições e as regras estabelecidas no Decreto Estadual nº 46.311, de 16 de setembro de 2013, e na Lei Federal nº 8.666, de 21 de junho de 1993.

3.3.4. Cada adesão por outros órgãos/entidades de direito público não poderá exceder ao quantitativo total registrado para cada item na Ata de Registro de Preços, devendo o órgão gerenciador especificar o quantitativo que autoriza adesão, mantendo registro no procedimento licitatório.

3.3.5. As adesões à ata de registro de preços são limitadas, ainda, em sua totalidade, ao quíntuplo do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e órgãos participantes, independentemente do número de órgãos não participantes que eventualmente aderirem.

3.3.6. Ao órgão ou entidade não participante que aderir à presente ata e ao órgão ou entidade partícipe competem, nos respectivos procedimentos instaurados, os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação às suas próprias contratações, informando todas as ocorrências ao órgão gerenciador, em especial acerca de eventual recusa do fornecedor em atender às condições estabelecidas no edital, firmadas na Ata de Registro de Preços, as divergências relativas às especificações dos serviços licitados, bem como a recusa em aceitar a ordem de serviço ou documento equivalente para a prestação de serviços.

3.4. As quantidades previstas para os itens com preços registrados poderão ser remanejadas ou redistribuídas pelo órgão gerenciador entre os órgãos participantes e não participantes do procedimento licitatório para registro de preços, observada como limite máximo a quantidade total registrada para cada item.

3.4.1. Para o remanejamento de quantidades entre órgãos participantes do procedimento licitatório não será necessária autorização do beneficiário da Ata de Registro de Preços.

3.4.2. O órgão gerenciador somente poderá reduzir o quantitativo inicialmente informado pelo órgão participante, com a sua anuência.

4. DO PEDIDO DE ESCLARECIMENTOS E DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO

4.1. Os pedidos de esclarecimentos e os registros de impugnações referentes a este processo licitatório deverão ser enviados ao Pregoeiro, até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, exclusivamente por meio eletrônico, no site http://www.compras.mg.gov.br/.

4.1.1. Os pedidos de esclarecimento e registros de impugnação serão realizados, em caso de indisponibilidade técnica ou material do sistema oficial do Estado de Minas Gerais, alternativamente, via e-mail comprascentrais@planejamento.mg.gov.br, observados os prazos previstos no item 4.1.

4.1.2. É obrigação do autor do pedido de esclarecimento ou do registro de impugnação informar ao órgão/entidade gestor(a) a indisponibilidade do sistema.

4.2. O pedido de esclarecimento ou registro de impugnação pode ser feito por qualquer pessoa no Portal de Compras na página do pregão, em campo próprio (acesso via botão “Esclarecimentos/Impugnação”).

4.2.1. Nos pedidos de esclarecimentos ou registros de impugnação os interessados deverão se identificar (CNPJ, Razão Social e nome do representante que pediu esclarecimentos, se pessoa jurídica e CPF para pessoa física) e disponibilizar as informações para contato (endereço completo, telefone e e-mail).

4.2.2. Podem ser inseridos arquivos anexos com informações e documentações pertinentes as solicitações.

4.2.3. Após o envio da solicitação, as informações não poderão ser mais alteradas, ficando o pedido registrado com número de entrada, tipo (esclarecimento ou impugnação), data de envio e sua situação.

4.2.4. A resposta ao pedido de esclarecimento ou ao registro de impugnação também será disponibilizada via sistema. O solicitante receberá um e-mail de notificação e a situação da solicitação alterar-se-á para “concluída”.

4.3. O pregoeiro responderá no prazo de 02 (dois) dias úteis, contados da data de recebimento, e poderá requisitar subsídios formais aos responsáveis pela elaboração do edital e dos anexos.

4.4. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

4.5. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

4.5.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.

4.6. As respostas aos pedidos de impugnações e esclarecimentos aderem a este Edital tal como se dele fizessem parte, vinculando a Administração e os licitantes.

4.7. Qualquer modificação no Edital exige divulgação pelo mesmo instrumento de publicação em que se deu o texto original, reabrindo-se o prazo inicialmente estabelecido, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

4.8. As denúncias, petições e impugnações anônimas ou não fundamentadas não serão analisadas e serão arquivadas pela autoridade competente.

4.9. A não impugnação do edital, na forma e tempo definidos nesse item, acarreta a decadência do direito de discutir, na esfera administrativa, as regras do certame.

4.10. Na contagem dos prazos estabelecidos neste edital, exclui-se o dia do início e inclui-se o do vencimento, e consideram-se os dias úteis. Só se iniciam e expiram os prazos em dia de expediente na Administração.

5. DAS CONDIÇÕES DE PARTICIPAÇÃO

5.1. Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento regular no termos do Decreto Estadual nº 47.524, de 6 de novembro de 2018 e Resolução SEPLAG nº 93, de 28 de novembro de 2018, no Cadastro Geral de Fornecedores – CAGEF.

5.2. É vedado a qualquer pessoa, física ou jurídica, representar mais de um licitante na presente licitação.

5.3. Para fins do disposto neste edital, o enquadramento dos beneficiários indicados no caput do art. 3º do Decreto Estadual nº 47.437, de 26

de junho de 2018 se dará da seguinte forma:

5.3.1. microempresa ou empresa de pequeno porte, conforme definido nos incisos I e II do caput e § 4º do art. 3º da Lei Complementar Federal nº 123, de 14 de dezembro de 2006;

5.3.2. agricultor familiar, conforme definido na Lei Federal nº 11.326, de 24 de julho de 2006;

5.3.3. produtor rural pessoa física, conforme disposto na Lei Federal nº 8.212, de 24 de julho de 1991;

5.3.4. microempreendedor individual, conforme definido no § 1º do art. 18-A da Lei Complementar Federal nº 123, de 14 de dezembro de 2006;

5.3.5. sociedade cooperativa, conforme definido no art. 34 da Lei Federal nº 11.488, de 15 de junho de 2007, e no art. 4º da Lei Federal nº 5.764, de 16 de dezembro de 1971.

5.4. **NÃO PODERÃO PARTICIPAR** as empresas que:

5.4.1. Encontrarem-se em situação de falência, concurso de credores, dissolução, liquidação;

5.4.2. Enquadrarem-se como sociedade estrangeira não autorizada a funcionar no País;

5.4.3. Estiverem suspensas temporariamente de participar de licitações ou impedidas de contratar com a Administração, sancionadas com fundamento no art. 87, III, da Lei Federal nº 8.666, de 21 de junho de 1993;

5.4.4. Estiverem impedidas de licitar e contratar com o Estado de Minas Gerais, sancionadas com fundamento no art. 7º da Lei Federal nº 10.520, de 17 de julho de 2002;

5.4.5. Forem declaradas inidôneas para licitar e contratar coma Administração Pública Federal, Estadual ou Municipal, sancionadas com fundamento no art. 87, IV, da Lei Federal nº 8.666, de 21 de junho de 1993;

5.4.6. Empresas que tenham como proprietários controladores ou diretores membros dos poderes legislativos da União, Estados ou Municípios ou que nelas exerçam funções remuneradas, conforme art. 54, II, “a”, c/c art. 29, IX, ambos da Constituição da República;

5.4.7. Estiverem inclusas em uma das situações previstas no art.9° da Lei Federal nº 8.666, de 21 de junho de 1993;

5.4.8. Empresas reunidas em consórcio.

5.5. A observância das vedações para não participação é de inteira responsabilidade do licitante que se sujeitará às penalidades cabíveis, em caso de descumprimento.

5.6. Como condição para participação no Pregão, a licitante assinalará, no momento de cadastramento de sua proposta, “sim” ou “não” em campo próprio do sistema eletrônico, relativo às seguintes declarações:

5.6.1. que cumpre os requisitos para a habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;

5.6.1.1. Alternativamente ao campo disposto no item 5.6.1, que, para fins de obtenção do tratamento diferenciado e simplificado de que trata a Lei Complementar 123, de 14 de dezembro de 2006 e o artigo 15 da Lei Estadual 20.826, de 31 de julho de 2013, registra que possui restrição no (s) documento (s) de regularidade fiscal, com o compromisso de que irá promover a sua regularização caso venha a formular o lance vencedor, cumprindo plenamente os demais requisitos de habilitação, conforme determina o inciso XIII do art. 9º da Lei Estadual nº 14.167/2002.

5.6.2. que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

5.7. Além das declarações prestadas via sistema, o licitante deverá anexar, juntamente com a documentação de habilitação, as seguintes

declarações constantes do anexo III do Edital:

5.7.1. que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apta a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, quando for o caso;

5.7.2. que está ciente e das condições contidas no Edital e seus anexos;

5.7.3. que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

5.7.4. que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

6. DO CREDENCIAMENTO

6.1. Para acesso ao sistema eletrônico o fornecedor deverá credenciar-se, nos termos do Decreto Estadual nº 47.524, de 6 de novembro de 2018 e Resolução SEPLAG nº 93, de 28 de novembro de 2018, por meio do site **www.compras.mg.gov.br**, na opção **Cadastro de Fornecedores**, no prazo mínimo de 02 (dois) dias úteis antes da data da sessão do Pregão.

6.1.1. Cada fornecedor deverá credenciar, no mínimo, um representante para atuar em seu nome no sistema, sendo que o representante receberá uma senha eletrônica de acesso.

6.2. O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

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

6.3.1. A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação.

6.4. O fornecimento da senha é de caráter pessoal e intransferível, sendo de inteira responsabilidade do fornecedor e de cada representante qualquer transação efetuada, não podendo ser atribuídos ao provedor ou ao gestor do sistema eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

6.4.1. O fornecedor se responsabiliza por todas as transações realizadas em seu nome, assumindo como firmes e verdadeiras as propostas e os lances efetuados por seu representante, sendo que o credenciamento do representante do fornecedor implicará responsabilidade pelos atos praticados e a presunção de capacidade técnica para a realização das transações, sob pena da aplicação de penalidades.

6.5. Informações complementares a respeito do cadastramento serão obtidas no *site* **www.compras.mg.gov.br** ou pela Central de Atendimento aos Fornecedores, via e- mail: cadastro.fornecedores@planejamento.mg.gov.br,com horário de atendimento de Segunda-feira a Sexta-feira das 08:00h às 16:00h.

6.6. O fornecedor enquadrado dentre aqueles listados no subitem 5.3 que desejar obter os benefícios previstos no Capítulo V da Lei Complementar Federal nº 123, de 14 de dezembro de 2006, disciplinados no Decreto Estadual nº.47.437, de 2018 e pela Resolução Conjunta SEPLAG/SEF/JUCEMG nº 9.576, de 6 de julho de 2016 deverá comprovar a condição de beneficiário no momento do seu credenciamento ou quando da atualização de seus dados cadastrais no Cadastro Geral de Fornecedores – CAGEF, desde que ocorram em momento anterior ao cadastramento da proposta comercial.

6.6.1. Não havendo comprovação, no CAGEF, da condição de beneficiário até o momento do registro de proposta, o fornecedor não fará jus aos benefícios listados no Decreto Estadual nº 47.437, de 26 de junho

de 2018.

7. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

7.1. Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.

7.1.1. Os arquivos referentes à proposta comercial e à documentação de habilitação deverão ser anexados no sistema, por upload, separadamente em campos próprios.

7.1.1.1. Os arquivos referentes à proposta comercial e os documentos de habilitação deverão, preferencialmente, ser assinados eletronicamente.

7.1.1.1.1. Para assinatura eletrônica, poderá ser utilizado o Portal de Assinatura Digital disponibilizado pelo Governo de Minas Gerais, de acesso gratuito, disponível em: http://www.portaldeassinaturas.mg.gov.br. Dúvidas com relação à utilização do Portal de Assinaturas Digital podem ser encaminhadas para o e-mail comprascentrais@planejamento.mg.gov.br. A realização da assinatura digital importará na aceitação de todos os termos e condições que regem o processo eletrônico, conforme Decreto nº 47.222, de 26 de julho de 2017, e demais normas aplicáveis, admitindo como válida a assinatura eletrônica, tendo como consequência a responsabilidade pelo uso indevido das ações efetuadas e das informações prestadas, as quais serão passíveis de apuração civil, penal e administrativa.

7.1.2. As orientações para cadastro de proposta e envio dos documentos de habilitação encontram-se detalhadas no Manual Pregão Eletrônico - Decreto nº 48.012/2020 acessível pelo Portal de Compras.

7.2. O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

7.3. Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do Certificado de Registro Cadastral emitido pelo CAGEF, cuja consulta é pública. Nesse caso os licitantes assinalarão em campo próprio no sistema a opção por utilizar a documentação registrada no CAGEF, não sendo necessário o envio dos documentos que estiverem vigentes.

7.4. Os documentos que constarem vencidos no CAGEF e os demais documentos exigidos para a habilitação, que não constem do CAGEF, deverão ser anexados em até 5 arquivos de 20 Mb cada.

7.5. As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da Lei Complementar nº 123/2006.

7.6. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

7.7. Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema;

7.8. Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

7.9. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

7.10. O prazo de validade da proposta será de 60 (sessenta) dias contados da data de abertura da sessão pública estabelecida no preâmbulo deste Edital e seus anexos, podendo substituí-la ou retirá-la até a abertura da sessão.

8. DO PREENCHIMENTO DA PROPOSTA

8.1. O licitante deverá encaminhar sua proposta mediante o preenchimento, no sistema eletrônico, dos campos abaixo, bem como, realizar o upload sua proposta comercial, conforme modelo constante no Anexo II - Proposta Comercial.

8.1.1. Valor unitário e total do item.

8.1.2. Anexar em PDF arquivo referente à Proposta Comercial contendo especificações do objeto, bem como outras informações pertinentes presentes no Anexo I- Termo de Referência.

8.1.3. O preenchimento dos campos do sistema bem como o arquivo referente a Proposta Comercial anexada deverá se referir, individualmente, a cada lote.

8.1.4. A licitante vencedora deverá encaminhar prospectos, catálogos, folders, fichas técnicas e demais documentos para comprovação de que os itens ofertados atendem às especificações técnicas solicitadas no edital.

8.1.5. Deve ser enviado a proposta comercial contendo as Patr Number (SKU) e a quantidade listados no item 1.2 do Termo de Referência e que irá disponibilizar as licenças conforme prazo mencionado no Termo de Referência.

8.1.6. A licitante vencedora deverá apresentar documento emitido pelo fabricante ou consulta ao sítio que comprove estar apta e autorizada a comercializar licenças de software ou indicar o distribuidor/revenda autorizado do qual fará a compra dos softwares.

8.1.7. Será exigido comprovação por meio de uma planilha ponto a ponto, ou outro tipo de comparativo com manuais ou folders da solução para fins de desclassificação da proposta.

8.2. Todas as especificações do objeto contidas na proposta vinculam a Contratada.

8.3. Nos preços propostos deverão estar incluídos todos os tributos, encargos sociais, financeiros e trabalhistas, taxas e quaisquer outros ônus que porventura possam recair sobre a execução do objeto da presente licitação, os quais ficarão a cargo única e exclusivamente da CONTRATADA.

8.3.1. Deverá ser apresentada planilha que expresse a composição de todos os custos unitários do itens envolvidos em cada lote do presente certame.

8.3.2. Todos os preços ofertados deverão ser apresentados em moeda corrente nacional, em algarismos com duas casas decimais após a vírgula.

8.4. Os fornecedores estabelecidos no Estado de Minas Gerais que forem isentos do ICMS, conforme dispõe o Decreto nº 43.080, de 2002, deverão informar na proposta, conforme anexo presente no Portal de Compras, os valores com e sem ICMS que serão classificados conforme itens abaixo.

8.4.1. Os fornecedores mineiros deverão informar nas propostas enviadas, pelo sistema eletrônico, as informações relativas ao produto e ao preço resultante da dedução do ICMS, conforme Resolução conjunta SEPLAG/SEF nº 3.458, de 22 de julho de 2003, alterada pela Resolução conjunta SEPLAG/SEF nº 4.670, de 5 de junho de 2014.

8.4.2. A classificação das propostas, etapa de lances, o julgamento dos preços, o registro dos preços e a homologação serão realizados a partir dos preços dos quais foram deduzidos os valores relativos ao ICMS.

8.4.3. Os fornecedores mineiros não optantes pelo Simples Nacional farão suas propostas conforme as disposições contidas nos subitens 8.4.1. e 8.4.2.

8.4.4. O disposto nos subitens 8.4.1. e 8.4.2 não se aplica aos

contribuintes mineiros optantes pelo regime do Simples Nacional.

8.4.5. Os fornecedores mineiros de que trata o subitem 8.4.4 deverão anexar às suas propostas comerciais a ficha de inscrição estadual, na qual conste a opção pelo Simples Nacional, podendo o pregoeiro, na sua falta, consultar a opção por este regime através do site: http://www8.receita.fazenda.gov.br/SimplesNacional/.

8.4.6. O fornecedor mineiro isento de ICMS, caso seja vencedor, deverá enviar, quando solicitado pelo Pregoeiro, via chat, após a negociação, sua proposta comercial assinada e atualizada com os valores finais ofertados durante a sessão deste Pregão, informando na proposta, além do preço resultante da dedução do ICMS, o preço com ICMS.

9. DA SESSÃO DO PREGÃO E DO JULGAMENTO

9.1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

9.2. O Pregoeiro verificará as propostas apresentadas, preservado o sigilo do licitante, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis ou não apresentem as especificações técnicas exigidas no Termo de Referência.

9.2.1. A análise da proposta que trata o item anterior é uma análise prévia, e não poderá implicar quebra de sigilo do fornecedor, bem como não exime a Administração da verificação de sua conformidade com todas as especificações contidas neste edital e seus anexos, quando da fase de aceitabilidade da proposta do licitante detentor do menor preço para cada lote.

9.2.2. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

9.2.3. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

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

9.3.1. Durante o transcurso da sessão pública, serão divulgados, em tempo real, o valor e horário do menor lance apresentado pelos licitantes, bem como todas as mensagens trocadas no “chat” do sistema, sendo vedada a identificação do fornecedor.

9.3.2. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

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

9.4.1. O lance deverá ser ofertado pelo valor total do lote.

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

9.6. O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ele ofertado e registrado pelo sistema.

9.7. Será adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto e fechado” em que os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

9.8. A etapa de envio de lances da sessão pública terá duração de quinze minutos. Após esse prazo, o sistema encaminhará o aviso de fechamento iminente dos lances e transcorrido o período de tempo, aleatoriamente determinado, de até dez minutos, a recepção de lances será automaticamente encerrada.

9.9. Encerrando o prazo previsto no subitem anterior, o sistema abrirá a

oportunidade para que o licitante da oferta de valor mais baixo e os autores das ofertas com valores de até dez por cento superiores àquela possam ofertar um lance final e fechado em até cinco minutos, que será sigiloso até o encerramento deste prazo.

9.9.1. Não havendo pelo menos três ofertas nas condições definidas acima, poderão os licitantes dos melhores lances, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, que será sigiloso até o encerramento do prazo.

9.10. Após o término dos prazos estabelecidos acima, o sistema ordenará os lances conforme sua vantajosidade.

9.10.1. Na ausência de lance final e fechado classificado na forma estabelecida nos subitens anteriores, haverá o reinício da etapa fechada, para que os demais licitantes, até o máximo de três, na ordem de classificação, possam ofertar um lance final e fechado em até cinco minutos, que será sigiloso até o encerramento deste prazo.

9.11. Poderá o pregoeiro, auxiliado pela equipe de apoio, justificadamente, admitir o reinício da etapa fechada, caso nenhum licitante classificado na etapa de lance fechado atenda às exigências de habilitação.

9.12. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

9.13. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

9.14. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

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

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

9.17. **Do empate ficto**

9.17.1. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação junto ao CAGEF do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto Estadual nº 47.437/2018.

9.17.2. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

9.17.3. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

9.17.4. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

9.17.5. No caso de equivalência dos valores apresentados pelas

microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

9.18. **Do empate real**

9.18.1. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

9.18.2. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, aos serviços prestados:

9.18.2.1. no país;

9.18.2.2. por empresas brasileiras;

9.18.2.3. por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

9.18.2.4. por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.

9.18.3. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas ou os lances empatados.

9.19. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro deverá encaminhar, pelo sistema eletrônico, via chat, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital.

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

9.19.2. O pregoeiro solicitará ao licitante melhor classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

9.20. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

9.21. **DA ACEITABILIDADE DA PROPOSTA VENCEDORA.**

9.21.1. O critério de julgamento será o de menor preço por lote, apurado de acordo com o Anexo II - Proposta Comercial.

9.21.2. Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao valor estimado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no § 9º do art. 26 do Decreto n.º 48.012/2020.

9.21.2.1. A proposta cujo preço unitário de item do lote estiver acima do custo unitário do item relacionado na planilha de referência da Administração (ou do item individualmente considerado, superior a qualquer dos lances apresentados), poderá ter seus valores adequados das seguintes formas:

9.21.2.1.1. Aplicação de desconto percentual linear nos preços unitários da proposta inicial, calculado a partir da diferença entre o valor global da proposta vencedora e o valor global da respectiva proposta inicial, dividida pelo valor global inicial;

9.21.2.1.2. Readequação não linear dos preços unitários, a critério do licitante, respeitado como limite máximo o valor global final ofertado, desde que os preços unitários finais sejam menores ou iguais aos preços unitários da proposta inicial.

9.21.2.2. Será desclassificada a proposta ou o lance vencedor, para

todos os fins aqui dispostos, que não atender às exigências fixadas neste Edital, contenha vícios insanáveis, manifesta ilegalidade ou apresentar preços manifestamente inexequíveis.

9.21.2.3. Considera-se inexequível a proposta que apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

9.21.2.3.1. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3° do artigo 43 da Lei n° 8.666, de 1993 para que a empresa comprove a exequibilidade da proposta.

9.21.2.3.2. Quando o licitante apresentar preço final inferior a 30% (trinta por cento) da média dos preços ofertados para o mesmo item, e a inexequibilidade da proposta não for flagrante e evidente pela análise da planilha de custos, não sendo possível a sua imediata desclassificação, será obrigatória a realização de diligências para aferir a legalidade e exequibilidade da proposta.

9.21.3. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita;

9.21.4. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata;

9.21.5. O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade de diligência disponível no sistema, no prazo de 2 (duas) horas, sob pena de não aceitação da proposta.

9.21.5.1. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

9.21.5.2. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham as características do serviço ofertado, bem como as planilhas de custo readequadas com o valor final ofertado, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo Pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

9.21.6. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

9.21.7. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a sua continuidade.

9.21.7.1. Também nas hipóteses em que o Pregoeiro não aceitar a proposta e passar à subsequente, poderá negociar com o licitante para que seja obtido preço melhor.

9.21.8. Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital.

9.21.9. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo licitante, no prazo indicado pelo Pregoeiro, desde que não haja majoração do preço global nem dos unitários.

10. DA PROVA DE CONCEITO

10.1. O licitante classificado em primeiro lugar será convocado a apresentar prova de conceito para realização dos testes necessários à verificação do atendimento das especificações definidas no Termo de Referência.

10.2. A apresentação e avaliação da prova de conceito não substitui a verificação para fins de recebimento e aceite, prevista no art. 73, da Lei nº 8.666/1993.

10.3. A data e o local da análise será informada pelo pregoeiro a todos os licitantes por meio do Portal de Compras do Estado - http://www.compras.mg.gov.br/#.

10.4. A data e local da será pelo pregoeiro a todos os http://www.compras.mg.gov.br/#.

10.5. Para fins de publicidade, todo e qualquer licitante poderá ter acesso às informações de cada uma das provas de conceito.

10.6. A não apresentação da prova de conceito sem justificativa ou fora do prazo do Edital implicará desclassificação da proposta.

10.7. Se a prova de conceito apresentada pelo primeiro classificado não for aceita, o pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da prova de conceito, observada a ordem de classificação, e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

11. DA VERIFICAÇÃO DA HABILITAÇÃO

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

a) CADIN – Cadastro Informativo de Inadimplência em relação à Administração Pública do Estado de Minas Gerais acessível pelo site http://consultapublica.fazenda.mg.gov.br/ConsultaPublicaCADIN/consultaSituacaoPublica.do;

b) CAGEF/CAFIMP – Cadastro de Fornecedores Impedidos acessível pelo site https://www.fornecedores2.mg.gov.br/portalcompras/fornecedoresimpedidoscon.do;

c) Lista de Inidôneos mantidos pelo Tribunal de Contas da União - TCU;

d) Sistema de Cadastramento Unificado de Fornecedores - SICAF, do Ministério da Economia (https:www3.comprasnet.govweb/public/pages/consultas/c

11.1.1. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

11.1.1.1. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

11.1.1.2. A tentativa de burlar será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

11.1.1.3. O licitante será convocado para manifestação previamente à sua inabilitação.

11.1.2. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

11.1.3. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

11.2. Caso atendidas as condições de participação, a habilitação dos licitantes será verificada por meio do CAGEF, nos documentos por ele abrangidos em relação à habilitação jurídica, à regularidade fiscal e trabalhista, à qualificação econômica financeira e habilitação técnica, conforme o disposto no Decreto nº 47.524/2018.

11.2.1. O interessado, para efeitos de habilitação prevista nesse edital mediante utilização do sistema, deverá atender às condições exigidas no cadastramento no CAGEF até (2) dias úteis anteriores à data prevista para recebimento das propostas;

11.2.2. É dever do licitante atualizar previamente as comprovações constantes do CAGEF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta, a respectiva documentação atualizada.

11.2.2.1. Caso as comprovações constantes do CAGEF vençam entre a data de envio da documentação concomitante ao cadastro da proposta e o momento da verificação da habilitação, deverá ser solicitado pelo pregoeiro ao licitante o envio da documentação atualizada, por meio de documentação complementar via sistema.

11.2.3. O descumprimento do subitem acima implicará a inabilitação do licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto 48.012/20.

11.3. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de 2 (duas) horas horas, sob pena de inabilitação.

11.4. A apresentação de documentos físicos originais somente será exigida se houver dúvida quanto à integridade do arquivo digitalizado.

11.5. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

11.6. Ressalvado o disposto no item 7.3, os licitantes deverão encaminhar, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação:

11.7. HABILITAÇÃO JURÍDICA:

11.7.1. Documento de identificação, com foto, do responsável pelas assinaturas das propostas comerciais constantes no Anexo III - Proposta Comercial e das declarações constantes no Anexo II - Modelos de Declarações.

11.7.1.1. Se for o caso, apresentar procuração conferindo poderes ao(s) responsável(is) pela empresa para praticar atos junto à Administração Pública.

11.7.2. Registro empresarial na Junta Comercial, no caso de empresário individual;

11.7.3. Ato constitutivo, estatuto ou contrato social e suas alterações posteriores ou instrumento consolidado, devidamente registrado na Junta Comercial, em se tratando de sociedades empresárias, cooperativas ou empresas individuais de responsabilidade limitada e, no caso de sociedade de ações, acompanhado de documentos de eleição ou designação de seus administradores;

11.7.4. Ato constitutivo devidamente registrado no Registro Civil de Pessoas Jurídicas em se tratando de sociedade não empresária, acompanhado de prova da diretoria em exercício;

11.7.5. Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País.

11.7.6. Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva;

11.8. REGULARIDADE FISCAL E TRABALHISTA:

11.8.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda - CNPJ;

11.8.2. Prova de inscrição no Cadastro de Contribuintes Estadual ou Municipal, relativo à sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto do certame;

11.8.3. Prova de regularidade perante as Fazendas Federal, Estadual sede do licitante, Municipal e perante a Fazenda Estadual de MG;

11.8.3.1. A prova de regularidade fiscal e seguridade social perante a Fazenda Nacional será efetuada mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil – RFB e pela Procuradoria-Geral da Fazenda Nacional – PGFN, referente a todos os tributos federais e à Dívida Ativa da União – DAU por elas administrados, bem como das contribuições previdenciárias e de terceiros.

11.8.3.2. Se o fornecedor não estiver inscrito no cadastro de contribuintes do Estado de Minas Gerais deverá comprovar a inexistência de débitos relativos a tributos estaduais em Minas Gerais por meio de Certidão de Débito Tributário – CDT, que poderá ser emitida pelo site: www.fazenda.mg.gov.br.

11.8.4. Certificado de Regularidade relativa à seguridade social e perante o Fundo de Garantia por Tempo de Serviço – FGTS.

11.8.5. 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 da Lei Federal nº 12.440, de 7 de julho de 2011, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

11.8.6. A comprovação da regularidade fiscal e/ou trabalhista deverá ser efetuada mediante a apresentação das competentes certidões negativas de débitos, ou positivas com efeitos de negativas.

11.8.7. Caso o fornecedor seja considerado isento dos tributos estaduais relacionados ao objeto licitado, deverá comprovar tal condição mediante a apresentação de declaração do domicílio ou sede do fornecedor, ou outra equivalente, na forma da lei.

11.9. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA:

11.9.1. Certidão negativa de falência expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida pelo distribuidor do domicílio da pessoa física, emitida nos últimos 06 (seis) meses;

11.10. QUALIFICAÇÃO TÉCNICA:

11.10.1. Comprovação de aptidão para prestação de serviços compatíveis com as características e quantidades do objeto da licitação, estabelecidas no Termo de Referência ANEXO a este Edital, por meio da apresentação de atestados de desempenho anterior, fornecidos por pessoa jurídica de direito público ou privado, comprobatório da capacidade técnica para atendimento ao objeto da presente licitação, vedado o autoatestado, compreendendo os requisitos abaixo relacionados:

11.10.1.1. **Para todos os lotes:** Atestado(s) comprobatório(s) da capacidade técnica da Licitante para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, atendendo ao quantitativo mínimo de 10% (dez por cento) ou com o item pertinente apresentadas no Anexo I - Termo de Referência;

11.10.2. Os atestados deverão conter:

11.10.2.1. Nome empresarial e dados de identificação da instituição emitente (CNPJ, endereço, telefone).

11.10.2.2. Local e data de emissão.

11.10.2.3. Nome, cargo, telefone, e-mail e a assinatura do responsável pela veracidade das informações.

11.10.2.4. Período da execução da atividade.

11.10.3. Para atendimento do quantitativo indicado nos subitens do item 11.10.1, é admitido o somatório de atestados, desde que compatíveis com as características do objeto da licitação.

11.10.3.1. O licitante deve disponibilizar, quando solicitado pelo pregoeiro, todas as informações necessárias à comprovação da legitimidade dos atestados solicitados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da CONTRATANTE e local em que foram executadas as atividades.

11.11. DISPOSIÇÕES GERAIS DA HABILITAÇÃO:

11.11.1. O licitante que possuir o Certificado de Registro Cadastral (CRC) emitido pela Unidade Cadastradora da Secretaria de Estado de Planejamento e Gestão – SEPLAG poderá utilizá-lo como substituto de documento dele constante, exigido para este certame, desde que este esteja com a validade em vigor no CRC. Caso o documento constante no CRC esteja com a validade expirada, tal não poderá ser utilizado, devendo ser apresentado documento novo com a validade em vigor.

11.11.1.1. Serão analisados no CRC somente os documentos exigidos para este certame, sendo desconsiderados todos os outros documentos do CRC, mesmo que estejam com a validade expirada.

11.11.2. Os documentos exigidos para habilitação serão apresentados no momento do cadastramento da proposta, conforme instruções do Portal de Compras http://www.compras.mg.gov.br/, e serão analisados após a classificação das propostas.

11.11.2.1. Para fins de habilitação, é facultada ao pregoeiro a verificação de informações e o fornecimento de documentos que constem de sítios eletrônicos de órgãos e entidades das esferas municipal, estadual e federal, emissores de certidões, devendo tais documentos ser juntados ao processo. A Administração não se responsabilizará pela eventual indisponibilidade dos meios eletrônicos, no momento da verificação. Ocorrendo essa indisponibilidade e não sendo apresentados os documentos necessários para verificação, o licitante será inabilitado.

11.11.3. Todos os documentos apresentados para a habilitação deverão conter, de forma clara e visível, o nome empresarial, o endereço e o CNPJ do fornecedor.

11.11.3.1. Se o fornecedor figurar como estabelecimento matriz, todos os documentos deverão estar em nome da matriz;

11.11.3.2. Se o fornecedor figurar como filial, todos os documentos deverão estar no nome da filial;

11.11.3.3. Na hipótese de filial, podem ser apresentados documentos que, pela própria natureza, comprovadamente são emitidos em nome da matriz;

11.11.3.4. Em qualquer dos casos, atestados de capacidade técnica ou de responsabilidade técnica podem ser apresentados em nome e com o número do CNPJ(MF) da matriz ou da filial da empresa licitante.

11.11.4. O não atendimento de qualquer das condições aqui previstas provocará a inabilitação do licitante vencedor, sujeitando-o, eventualmente, às punições legais cabíveis.

11.11.5. Aos beneficiários listados no item 5.3 será concedido prazo de 05 (cinco) dias úteis, prorrogáveis por igual período, a critério da administração, para regularização da documentação fiscal e/ou trabalhista, contado a partir da divulgação da análise dos documentos de habilitação do licitante melhor classificado, conforme disposto no inciso I, do § 2º, do art. 6º do Decreto Estadual nº 47.437, de 26 de junho de 2018.

11.11.5.1. A não regularização da documentação deste item implicará a inabilitação do licitante vencedor, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de

classificação, seguir-se outra microempresa, empresa de pequeno porte ou sociedade cooperativa com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

11.11.5.2. Se houver a necessidade de abertura do prazo para o beneficiário regularizar sua documentação fiscal e/ou trabalhista, o pregoeiro deverá suspender a sessão de pregão para o lote específico e registrar no "*chat*" que todos os presentes ficam, desde logo, intimados a comparecer no dia e horário informados no site www.compras.mg.gov.br para a retomada da sessão de pregão do lote em referência.

12. DOS RECURSOS

12.1. Declarado o vencedor e decorrida a fase de regularização fiscal e trabalhista da licitante qualificada como microempresa ou empresa de pequeno porte, se for o caso, será concedido o prazo de no mínimo trinta minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

12.2. Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

12.2.1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

12.2.2. A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito.

12.2.3. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de três dias úteis para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros três dias úteis, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

12.2.4. A apresentação de documentos complementares, em caso de indisponibilidade ou inviabilidade técnica ou material da via eletrônica, devidamente identificados, relativos aos recursos interpostos ou contrarrazões, se houver, será efetuada mediante envio para o e-mail comprascentrais@planejamento.mg.gov.br, e identificados com os dados da empresa licitante e do processo licitatório (nº. do processo e lote), observados os prazos previstos no item 12.1.

12.3. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

12.4. Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.

13. DA REABERTURA DA SESSÃO PÚBLICA

13.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

13.1.1. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

13.1.2. A convocação se dará por meio do sistema eletrônico ("chat"), e-mail, de acordo com a fase do procedimento licitatório.

13.1.3. A convocação feita por e-mail dar-se-á de acordo com os dados contidos no CAGEF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

14. DO REGISTRO DE PREÇO E DA HOMOLOGAÇÃO

14.1. Constatado o atendimento pleno às exigências editalícias, o pregoeiro declarará o licitante vencedor e o sistema gerará ata circunstanciada da sessão,

na qual serão registrados todos os atos do procedimento e as ocorrências relevantes, disponível para consulta no site www.compras.mg.gov.br.

14.2. O Pregoeiro registrará o preço do licitante vencedor quando inexistir recurso ou quando reconsiderar sua decisão, com a posterior homologação do resultado pela autoridade competente.

14.3. Decididos os recursos porventura interpostos e constatada a regularidade dos atos procedimentais pela autoridade competente, esta registrará o preço do licitante vencedor e homologará o procedimento licitatório.

14.4. Todos os participantes estão convidados e incentivados a realizarem o registro adicional de preços para compor o cadastro de reserva, mesmo que não tenham sido vencedores dos lotes disputados, seguindo a ordem de classificação e desde que manifestem esta intenção ao final da sessão de lances e aceitem fornecer nas mesmas condições e preço do licitante vencedor do certame.

14.4.1. Os licitantes que desejarem ter seus preços registrados deverão apresentar toda a documentação exigida para comprovação da condição de habilitação em pleno atendimento das condições deste edital.

15. DA FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS

15.1. Os licitantes classificados que manifestarem a intenção de registrar preços, para compor o Cadastro de Reserva à Ata de Registro de Preços, terão suas propostas e documentação de habilitação analisadas e, para tal, deverão encaminhar os referidos documentos, conforme disposto no item 7 do edital.

15.2. O registro adicional de preços em Ata estará condicionado à análise e aceitabilidade da proposta e dos documentos de habilitação.

15.2.1. Seguir-se-á com a análise da amostra verificando se atende às especificações constantes no Termo de Referência.

15.3. A convocação dos licitantes que registraram seus preços adicionais, para compor o cadastro reserva, respeitará a ordem de classificação constante da ata e ocorrerá, sucessivamente, sempre que seja cancelado ou suspenso o registro do preço do beneficiário da ata.

15.4. Homologado o resultado da licitação, o órgão gerenciador, respeitada a ordem de classificação e a quantidade de fornecedores a serem registrados, convocará os interessados para, no prazo de até 05 (cinco) dias úteis, contados da data da convocação, procederem à **assinatura eletrônica da Ata de Registro de Preços**, a qual, após cumpridos os requisitos de publicidade, terá efeito de compromisso de fornecimento nas condições estabelecidas.

15.4.1. O instrumento de contratação, e demais atos firmados com a Administração, serão assinados de maneira eletrônica, por intermédio do Sistema Eletrônico de Informações do Governo do Estado de Minas Gerais - SEI/MG.

15.4.1.1. Para a assinatura eletrônica, caso ainda não possua cadastro, o(s) licitante(s) interessado(s) deverá(ão) acessar o Sistema Eletrônico de Informações do Governo do Estado de Minas Gerais – SEI/MG, por meio do link www.sei.mg.gov.br/usuarioexterno, e clicar em "Clique aqui se você ainda não está cadastrado".

15.4.1.2. Dúvidas com relação ao cadastro no SEI podem ser encaminhadas para o e-mail: atendimentosei@planejamento.mg.gov.br.

15.4.1.3. A realização do cadastro como Usuário Externo no SEI/MG importará na aceitação de todos os termos e condições que regem o processo eletrônico, conforme Decreto Estadual nº 47.222, de 26 de julho de 2017, e demais normas aplicáveis, admitindo como válida a assinatura eletrônica na modalidade cadastrada (login/senha), tendo como consequência a responsabilidade pelo uso indevido das ações efetuadas e das informações prestadas, as quais serão passíveis de apuração civil, penal e administrativa.

15.5. O prazo previsto para assinatura da Ata poderá ser prorrogado uma vez, por igual período, quando, durante o seu transcurso, for solicitado pelo

licitante convocado, desde que ocorra motivo justificado e aceito pelo órgão gerenciador.

15.6. O licitante que, convocado para assinar a ata, deixar de fazê-lo no prazo fixado, dela será excluído, na forma do art. 81 da Lei Federal nº 8.666, de 21 de junho de 1993, sem prejuízo das sanções previstas em lei.

15.7. É facultado à Administração, quando o convocado não assinar a Ata de Registro de Preços no prazo e condições estabelecidos, convocar os licitantes remanescentes, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições propostas pelo primeiro classificado.

16. DA VIGÊNCIA DA ATA

16.1. A Ata de Registro de Preços terá vigência de **12 (doze) meses** a contar da data de sua publicação.

17. DA CONTRATAÇÃO

17.1. Publicada a ata, a contratação será formalizada por instrumentos hábeis, tais como termo de contrato, ordem de serviço, ou documento equivalente, sendo o fornecedor convocado para aceitar ou retirar o documento, de acordo com os arts. 62 e 64 da Lei Federal nº 8.666, de 21 de junho de 1993 e Lei Federal nº 10.520, de 17 de julho de 2002, e ainda, obedecidas as disposições pertinentes do Decreto Estadual nº 46.311, de 16 de setembro de 2013 do Decreto 48.012, de 22 de julho de 2020.

17.1.1. O fornecedor detentor do preço registrado, na contratação, deverá comprovar a manutenção das condições demonstradas para habilitação.

17.1.2. Caso o fornecedor detentor do preço registrado não apresente situação regular no ato da emissão do termo de contrato, ordem de serviço, ou documento equivalente, não compareça quando convocado ou não retire o documento no prazo estipulado, será cancelado seu registro na ata e convocados os fornecedores registrados com base nos arts. 11 e 12 do Decreto Estadual nº 46.311, de 16 de setembro de 2013 e, não os havendo, os licitantes remanescentes, observada a ordem de classificação, conforme item 15.7.

17.1.3. É facultado à Administração, quando o convocado não aceitar ou retirar o termo de contrato, ordem de serviço, ou documento equivalente no prazo e condições estabelecidos, convocar os licitantes remanescentes, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições propostas pelo primeiro classificado, inclusive quanto aos preços atualizados de conformidade com o ato convocatório, ou revogar a licitação independentemente da cominação prevista no art. 81 da Lei Federal nº 8.666, de 21 de junho de 1993.

17.2. O representante legal do licitante que tiver registrado em ata a proposta vencedora deverá aceitar ou retirar o termo de contrato, ordem de serviço, ou documento equivalente, dentro do prazo máximo de 05 (cinco) dias úteis a contar do recebimento da comunicação, através de fax, carta postal ou e-mail, sem prejuízo das sanções previstas no Edital e das demais cominações legais, conforme disposto no art. 48, § 2º do Decreto Estadual nº 48.012/ 2020.

17.3. Qualquer solicitação de prorrogação de prazo para aceitar ou retirar o termo de contrato, ordem de serviço, ou documento equivalente, decorrentes desta licitação, somente será analisada se apresentada antes do decurso do prazo para tal e devidamente fundamentada.

18. DA SUBCONTRATAÇÃO

18.1. É vedado à CONTRATADA subcontratar total ou parcialmente o fornecimento ora ajustado.

19. DA GARANTIA FINANCEIRA DA EXECUÇÃO

19.1. A CONTRATADA, no prazo máximo de 10 (dez) dias após a assinatura do Contrato, prestará garantia no valor correspondente a 5% (cinco) do valor do Contrato, que será liberada de acordo com as condições

previstas neste Edital, conforme disposto no art. 56 da Lei Federal nº 8.666, de 21 de junho de 1993, desde que cumpridas as obrigações contratuais.

19.2. A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de mais 03 (três) meses após o término da vigência contratual.

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

19.3.1. prejuízos advindos do não cumprimento do objeto do contrato;

19.3.2. prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;

19.3.3. multas moratórias e punitivas aplicadas pela Administração à CONTRATADA; e

19.3.4. obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela CONTRATADA, quando couber.

19.4. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, observada a legislação que rege a matéria.

19.5. A garantia em dinheiro deverá ser efetuada em banco oficial em conta específica com correção monetária, em favor do CONTRATANTE;

19.6. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições.

19.7. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.

19.8. A CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

19.9. Será considerada extinta a garantia:

19.9.1. com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da CONTRATANTE, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato;

19.9.2. no prazo de 03 (três) após o término da vigência, caso a CONTRATANTE não comunique a ocorrência de sinistros.

20. DO PAGAMENTO

20.1. Para os Órgãos/Entidades da Administração Direta ou Indireta do Estado de Minas Gerais, o pagamento será efetuado através do Sistema Integrado de Administração Financeira - SIAFI/MG, por meio de ordem bancária emitida por processamento eletrônico, a crédito do beneficiário em um dos bancos que o fornecedor indicar, no prazo de 30 (trinta) dias corridos da data do recebimento definitivo, com base nos documentos fiscais devidamente conferidos e aprovados pela CONTRATANTE. Para os demais participantes, o pagamento será realizado a crédito do beneficiário em um dos bancos que o fornecedor indicar, de acordo com normativo próprio a que se sujeita, mantendo-se os prazos e condições estabelecidas no edital e seus anexos.

20.1.1. Para efeito de pagamento, a CONTRATADA encaminhará à CONTRATANTE, após a execução do objeto, a respectiva nota fiscal/fatura, acompanhada do relatório da execução do objeto do período a que o pagamento se referir, bem como, demais documentos necessários para a efetiva comprovação da execução do objeto, se houver.

20.1.2. A Administração receberá o Documento Auxiliar da Nota Fiscal Eletrônica (DANFE) juntamente com o objeto e deverá realizar a verificação da validade da assinatura digital e a autenticidade do arquivo digital da NF-e (o destinatário tem à disposição o aplicativo “visualizador”, desenvolvido pela Receita Federal do Brasil) e a concessão da Autorização de Uso da NF-e, mediante consulta eletrônica à Secretaria da Fazenda o Portal Nacional da

NF-e.

20.1.3. O pagamento da Nota Fiscal fica vinculado à prévia conferência pelo gestor.

20.1.4. As Notas Fiscais que apresentarem incorreções serão devolvidas à CONTRATADA e o prazo para o pagamento passará a correr a partir da data da reapresentação do documento considerado válido pela CONTRATANTE.

20.1.5. Ocorrendo atraso de pagamento por culpa exclusiva da Administração, o valor devido será atualizado financeiramente, entre as datas do vencimento e do efetivo pagamento, de acordo com a variação do Sistema Especial de Liquidação e Custódia – SELIC.

20.2. A CONTRATADA deve garantir a manutenção dos requisitos de habilitação previstos no Edital.

20.3. Eventuais situações de irregularidades fiscal ou trabalhista da CONTRATADA não impedem o pagamento, se o objeto tiver sido executado e atestado. Tal hipótese ensejará, entretanto, a adoção das providências tendentes ao sancionamento da empresa e rescisão contratual.

21. DAS SANÇÕES ADMINISTRATIVAS

21.1. A licitante/adjudicatária que cometer qualquer das infrações, previstas na Lei Federal nº 8.666, de 21 de junho de 1993, na Lei Federal nº 10.520, de 17 de julho de 2002, Lei Estadual n.º 14.167, de 10 de janeiro de 2002 e no Decreto Estadual nº. 45.902, de 27 de janeiro de 2012 e no do Decreto 48.012, de 22 de julho de 2020, ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

21.1.1. Advertência por escrito;

21.1.2. Multa de até 20% (vinte por cento) sobre o valor estimado do(s) lote(s) dos quais o licitante tenha participado e cometido a infração;

21.1.3. Suspensão do direito de participar de licitações e impedimento de contratar com a Administração, pelo prazo de até 2 (dois)anos;

21.1.4. Impedimento de licitar e contratar com a Administração Pública Estadual, nos termos do art. 7º da Lei Federal nº 10.520, de 17 de julho de 2002;

21.1.5. Declaração de inidoneidade para licitar ou contratar com a Administração Pública;

21.2. A sanção de multa poderá ser aplicada cumulativamente às demais sanções previstas nos itens 21.1.1, 21.1.3, 21.1.4, 21.1.5.

21.3. A multa será descontada da garantia do contrato, quando houver, e/ou de pagamentos eventualmente devidos ao infrator e/ou cobrada administrativa e/ou judicialmente.

21.4. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo incidental apensado ao processo licitatório ou ao processo de execução contratual originário que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto no Decreto Estadual nº. 45.902, de 27 de janeiro de 2012, bem como o disposto na Lei Federal nº 8.666, de 21 de junho de 1993 e Lei Estadual nº 14.184, de 31 de janeiro de 2002.

21.5. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

21.5.1. Não serão aplicadas sanções administrativas na ocorrência de casos fortuitos, força maior ou razões de interesse público, devidamente comprovados.

21.6. A aplicação de sanções administrativas não reduz nem isenta a obrigação da CONTRATADA de indenizar integralmente eventuais danos causados a Administração ou a terceiros, que poderão ser apurados no mesmo processo administrativo sancionatório.

21.7. As sanções relacionadas nos itens 21.1.3, 21.1.4 e 21.1.5 serão obrigatoriamente registradas no Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual – CAFIMP e no CAGEF.

21.8. As sanções de suspensão do direito de participar em licitações e impedimento de licitar e contratar com a Administração Pública poderão ser também aplicadas àqueles que:

21.8.1. Retardarem a execução do objeto;

21.8.2. Comportar-se de modo inidôneo;

21.8.2.1. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances;

21.8.3. Apresentarem documentação falsa ou cometerem fraude fiscal.

21.9. As sanções dispostas também se aplicam aos integrantes do cadastro de reserva, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente.

21.10. Durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei Federal nº 12.846, de 1º de agosto de 2013, e pelo Decreto Estadual nº 46.782, de 23 de junho de 2015, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à Controladoria-Geral do Estado, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

22. DISPOSIÇÕES GERAIS

22.1. Este edital deverá ser lido e interpretado na íntegra, e após encaminhamento da proposta não serão aceitas alegações de desconhecimento.

22.2. É facultado ao Pregoeiro ou à Autoridade Superior, em qualquer fase do julgamento, promover diligência destinada a esclarecer ou complementar a instrução do processo e a aferição do ofertado, bem como solicitar a elaboração de pareceres técnicos destinados a fundamentar as decisões.

22.3. O objeto desta licitação deverá ser executado em conformidade com o Anexo I - Termo de Referência, correndo por conta da CONTRATADA as despesas de seguros, transporte, tributos, encargos trabalhistas e previdenciários decorrentes da execução do objeto da contratação.

22.4. É vedado ao licitante retirar sua proposta ou parte dela após aberta a sessão do pregão.

22.5. O pregoeiro, no julgamento das propostas e da habilitação, poderá relevar omissões puramente formais e sanar erros ou falhas que não alterem a substância das propostas, dos documentos e de sua validade jurídica, mediante despacho fundamentado, acessível a todos os interessados, sendo possível a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo.

22.6. A presente licitação somente poderá ser revogada por razão de interesse público decorrente de fato superveniente devidamente comprovado, ou anulada, no todo ou em parte, por ilegalidade, de ofício ou por provocação de terceiros, mediante parecer escrito e devidamente fundamentado.

22.7. Fica eleito o foro da Comarca de Belo Horizonte, Estado de Minas Gerais, para dirimir eventuais conflitos de interesses decorrentes desta licitação, valendo esta cláusula como renúncia expressa a qualquer outro foro, por mais privilegiado que seja ou venha a ser.

22.8. Os interessados poderão examinar ou retirar gratuitamente o presente Edital de Licitação e seus anexos no site: www.compras.mg.gov.br.

JAFER ALVES JABOUR

Superintendente Central de Compras Governamentais

Centro de Serviços Compartilhados

Secretaria de Planejamento e Gestão

Documento assinado eletronicamente por **Jafer Alves Jabour**, **Superintendente**, em 31/03/2023, às 13:55, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **63372781** e o código CRC **C44CA0BC**.

Referência: Processo nº 1500.01.0113446/2022-67 SEI nº 63372781

ESTADO DE MINAS GERAIS

SECRETARIA DE ESTADO DE PLANEJAMENTO E GESTÃO

Diretoria Central de Gestão de Serviços e Infraestrutura de TIC

Versão v.20.09.2020.

ANEXO I - TERMO DE REFERÊNCIA

DATA	ÓRGÃO SOLICITANTE	NÚMERO DA UNIDADE DE COMPRAS
28/03/2023	SEPLAG	1501566

RESPONSÁVEL PELA SOLICITAÇÃO	SUPERINTENDÊNCIA OU DIRETORIA
Nome: Rosalvo França Júnior E-mail: rosalvo.franca@planejamento.mg.gov.br Ramal para contato: 31 97125-0204	Diretoria Central de Gestão de Serviços e Infraestrutura de TIC

1. OBJETO

O presente termo de referência tem por objeto o Registro de Preços para aquisição de licenças de uso de solução corporativa de Segurança de Endpoint's e Servidores para múltiplas plataformas incluindo garantia, suporte e atualização para utilização no parque tecnológico do Governo do Estado de Minas Gerais, sob demanda, futura e eventual, conforme especificações, exigências e quantidades estabelecidas neste documento.

LOTE	ITEM	CÓDIGO DO ITEM NO SIAD	QUANTIDADE	UNIDADE DE AQUISIÇÃO (OU DE MEDIDA)	DESCRIÇÃO DO ITEM NO CATMAS	PERÍODO
01 (Ampla Participação)	01	000119750	29.156	1 unidade	Subscrição de licença de proteção de endpoint para CLIENTES WINDOWS	12 meses
	02	000119768	733	1 unidade	Subscrição de licença de software de proteção de endpoint para SERVIDORES WINDOWS	12 meses
	03	000119776	631	1 unidade	Subscrição de licença de software de proteção de endpoint para LINUX	12 meses
	04	000119784	60	1 unidade	Subscrição de licença de software de proteção de endpoint para MAC	12 meses
	05	000119792	474	1 unidade	Subscrição de licença de software de proteção para MOBILE	12 meses
	06	000119806	13.726	1 unidade	Serviço de instalação, configuração e migração da solução	

	06	000119806	15.720	1 unidade	atualmente em uso para a solucao fornecida	-
	07	000119814	45	1 unidade	Capacitação e Treinamento em Solucao de Endpoint	-

1.1. **ESPECIFICAÇÃO DO OBJETO:**

1.1.1. O detalhamento técnico do objeto encontra-se descrito no Anexo I (A) - Detalhamento do Objeto, deste TERMO DE REFERÊNCIA.

1.2. **INFORMAÇÕES COMPLEMENTARES AO OBJETO:**

1.2.1. Os itens 01, 02, 03, 04 e 05: Licenciamento com assistência técnica, garantia, suporte, garantia e atualização de versão por 12 (doze) meses foram assim agrupados porque para esse tipo de aquisição, os serviços de garantia do fabricante e atualização de versão são incluídos no valor do Software e Licenciamento.

1.2.2. Os itens 06 e 07: Suporte Técnico especializado, a instalação, configuração e migração e o treinamento são serviços necessários e complementares aos itens 01, 02, 03 04 e 05.

1.2.3. Os Softwares descritos nos itens anteriores deverá possuir uma mídia de instalação original (CD ou DVD) ou liberação de usuário e senha de acesso ao site do fabricante para download da imagem ou programa de instalação original, para cada Endpoint e servidor demandado.

1.2.4. Desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;

1.2.5. Caberá a cada órgão ou entidade contratante junto à Contratada, efetivar análise técnica do recebimento e instalação do software.

2. LOTES

2.1. **DO AGRUPAMENTO DE ITENS EM LOTES:**

2.1.1. Observando os critérios de divisibilidade, informamos que o agrupamento dos itens respeitam a legislação vigente e garantem a ampla participação das empresas existentes no mercado, sem prejuízo para o projeto ou perda de economia de escala, propiciando o fornecimento de diversos itens licitados de forma autônoma.

2.2. **LOTES EXCLUSIVOS PARA MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE:**

2.2.1. Não será reservado à participação de ME/EPP fundamentados pelo art. 48, inciso I, da LC 123/2006 c/c art. 8º do Decreto Estadual nº 47.437/2018 e art. 48, inciso III, da LC 123/2006 c/c art. 11 do Decreto Estadual nº 47.437/2018.

3. JUSTIFICATIVA DA CONTRATAÇÃO

3.1. A aquisição de licenças de solução de segurança para Endpoint’s e servidores possui, como intuito, prevenir a contaminação por vírus, malwares, suas variantes e demais ameaças cibernéticas, nos computadores da Contratante que podem pôr em risco o sigilo, a integridade e a disponibilidade das informações.

3.2. Devido à grande utilização de e-mails e acesso a páginas de internet, a aquisição de software de antivírus passa a ser necessária para fornecer segurança à infraestrutura de rede dos órgãos do Governo Estadual, sendo este licenciamento imprescindível para os ambientes informatizados.

3.3. Estas aquisições buscam proporcionar maior proteção aos computadores dos órgãos, resguardando problemas que possam prejudicar os serviços prestados aos cidadãos. Portanto, é uma questão de segurança, que possibilita garantir o desempenho das estações de trabalho e, por conseguinte, disponibilizar aos funcionários condições para a realização de suas atividades. A aquisição destas licenças é essencial para que estas tarefas sejam executadas com êxito.

3.4. Dessa forma, justifica-se a necessidade de aquisição dessas ferramentas para promover e realizar as atividades demandadas para o governo nos próximos anos.

4. JUSTIFICATIVA DA MODALIDADE

4.1. Será realizado Pregão Eletrônico considerando que este é aplicado para aquisições de bens e serviços comuns pelo menor preço. Aliado a isso, ao se adotar o sistema de registro de preço, fica assegurada uma maior possibilidade de se obter menores preços a serem adquiridos pelos os órgãos/entidades participantes e não participantes que aderirem a Ata de Registro de Preços. Para corroborar tal entendimento o Decreto Estadual nº 46.311 de 16 de setembro de 2013 estabelece que:

> Art. 4º Será adotado, preferencialmente, o SRP quando:
>
> II – For conveniente a compra de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade ou a programas de Governo.

4.2. O Decreto Estadual nº 46.311, de 16 de setembro de 2013, em seu art. 3º, caput, define o Registro de Preços como um conjunto de procedimentos para registro formal de preços, objetivando contratações futuras pela Administração Pública. Assim, considerando que Registro de Preços não é modalidade de licitação, o referido diploma legal estabelece no art. 3º, § 2º que para registro de preços de bens e serviços comuns será utilizada, obrigatoriamente, a modalidade pregão, salvo o disposto em legislação específica.

4.3. O Decreto Estadual nº 48.012 de 22 de julho de 2020, que regulamenta a licitação, na modalidade pregão, na forma eletrônica estabelece:

> Art. 1º – Este decreto regulamenta a licitação na modalidade de pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, no âmbito da Administração Pública direta, autárquica e fundacional do Poder Executivo.
>
> § 1º – É obrigatória a utilização da modalidade de pregão, na forma eletrônica, pelos órgãos da Administração direta, pelas autarquias, pelas fundações e pelos fundos especiais nas licitações de que trata o caput.
>
> § 2º – Será admitida, excepcionalmente, mediante prévia justificativa da autoridade competente, a utilização da modalidade de pregão, na forma presencial, nas licitações de que trata o caput, desde que fique comprovada a inviabilidade técnica ou a desvantagem para a Administração na realização da forma eletrônica.
>
> § 3º – As empresas públicas, as sociedades de economia mista e suas subsidiárias, nos termos do regulamento interno de que trata o art. 40 da Lei Federal nº 13.303, de 30 de junho de 2016, poderão adotar, no que couber, as disposições deste decreto.

4.4. Sobre a caracterização do objeto como sendo serviço comum, o mesmo diploma legal considera bens e serviços comuns aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos no objeto do edital, por meio de especificações reconhecidas e usuais praticadas no mercado. Sendo assim, uma vez que as especificações do objeto deste Termo de

Referência são usuais no mercado e os padrões de desempenho e qualidade podem ser objetivamente definidos no Edital de Licitação, entendemos pela caracterização de serviços comuns, possibilitando assim, a licitação na modalidade de Pregão Eletrônico para Registro de Preços.

4.5. Justificativa da escolha:

4.5.1. Melhoria da qualidade técnica dos documentos preliminares ao certame, tais como: especificações técnicas, alinhamento estratégico com o planejamento dos órgãos e condições jurídicas para a contratação;

4.5.2. Redução do esforço administrativo para a realização de diversos processos licitatórios sendo que a execução conjunta culmina em um único certame;

4.5.3. Padronização do parque tecnológico na Administração Pública;

4.5.4. Redução de custos de manutenção e melhor eficiência pelo uso racional dos recursos, uma vez que estes foram definidos de forma a atender precisamente as necessidades do usuário;

4.5.5. Ganho de economia de escala, pois, ao prospectar grandes volumes licitados, a Administração Pública amplia seu poder de compra junto aos fornecedores e consegue reduções consideráveis de preços, fato que certamente não ocorreria quando do fracionamento de certames.

5. DA PARTICIPAÇÃO DE CONSÓRCIOS:

5.1. Não será permitida a participação de empresas reunidas em consórcio, devido à baixa complexidade do objeto a ser adquirido, considerando que as empresas que atuam no mercado têm condições de prestar os serviços de forma independente.

6. QUALIFICAÇÃO TÉCNICA:

6.1. Atestado(s) comprobatório(s) da capacidade técnica da Licitante para prestação dos serviços ofertados, atendendo ao quantitativo mínimo de 10 % (dez por cento) das quantidades apresentadas neste Anexo I;

6.2. Para atendimento do quantitativo indicado acima, é admitido o somatório de atestados, desde que compatíveis com as características do objeto da licitação.

7. CRITÉRIOS DA ACEITABILIDADE DA PROPOSTA:

7.1. **Requisitos de aceitabilidade**

7.1.1. A licitante vencedora deverá encaminhar prospectos, catálogos, folders, fichas técnicas e demais documentos para comprovação de que os itens ofertados atendem às especificações técnicas solicitadas no edital.

7.1.2. Deve ser enviado a proposta comercial contendo os Part Number (SKU) e a quantidade listados no item 1.2 e que irá disponibilizar as licenças conforme prazo mencionado no Termo de Referência.

7.1.3. A licitante vencedora deverá encaminhar uma planilha indicando, ponto a ponto, a comprovação das especificações técnicas e a fonte para consulta.

8. DA PROVA DE CONCEITO:

8.1. A critério da administração, poderá ser solicitada prova de conceito para comprovação de que os serviços ofertados atendem às especificações técnicas solicitadas no edital.

8.1.1. **Para os lote 1, no prazo de até 02 (dois) dias úteis, após a suspensão da sessão de lances, o fornecedor detentor da**

melhor oferta deverá encaminhar um acesso da licença ofertada, devidamente identificado, para realização de Recepção Técnica com objetivo de averiguação do atendimento às especificações técnicas indicadas neste Termo de Referência.

8.1.2. A licença deverá ser encaminhada ou direcionada para a Diretoria Central de Gestão de Recursos de TIC/Superintendência Central de Governança Eletrônica no seguinte endereço: Rodovia Papa João Paulo II, 3.777, Serra Verde, Belo Horizonte, MG – CEP 31630-903 – Prédio Gerais – SEPLAG, no horário de 08H00MIN (oito) às 17H00MIN (dezessete) horas **e/ou** para os e-mails rosalvo.franca@planejamento.mg.gov.br e weslley.costa@planejamento.mg.gov.br.

8.1.3. As características definidas no Lote 01 deverá ser comprovadas por meio de documentação técnica a elas referenciada e por meio da realização de testes de aceitação a serem efetivados pela área demandante: Diretoria Central de Gestão de Recursos de TIC/Superintendência Central de Governança Eletrônica/SEPLAG em conjunto com a Companhia de Tecnologia da Informação do Estado de Minas Gerais – PRODEMGE/MG.

8.1.4. O endereço da efetivação da Recepção Técnica será na Sede da PRODEMGE: Rua da Bahia, 2277 - Lourdes - BH/MG.

8.2. Os testes de aceitação serão definidos pela área técnica de acordo com o item 1.1 - **ESPECIFICAÇÃO DO OBJETO** deste Termo de Referência.

8.3. Serão escolhidos de forma aleatória 05 testes práticos para validação entre os requisitos descritos no item 1.1 deste Termo de Referência.

8.4. A Especificação do Ambiente de Testes é:

- 01 Máquina Virtual (VM) para o módulo gerenciador com a seguinte configuração: 02 vCPUs, 08 GB de vRAM e 100 GB de vDISK (ou vHD);
- 01 VM para a estação de trabalho virtual que irá cumprir o papel de cliente onde será instalado o antimalware client com a seguinte configuração: 01 vCPU, 04 GB de vRAM e 60 GB de vDISK (ou vHD).

8.5. As VMs terão comunicação via rede IP para testes das funções de atualização e gerenciamento.

8.6. Todos os componentes de software da solução deverão ser instalados nessa configuração. Caso a solução ofertada seja composta de equipamento do tipo Appliance, este deverá ser disponibilizado e configurado pela proponente com a melhor oferta nos mesmos prazos anteriormente informados e deverá ser retirado após a realização da recepção técnica. Nem a PRODEMGE e nem a SEPLAG poderão se responsabilizar pela guarda dos equipamentos entregues à sua posse durante o período em que os mesmos estiverem disponíveis para testes. Nesse sentido é essencial que o equipamento disponibilizado seja objeto de seguro específico contra furto, roubo, descargas elétricas, intempéries, quedas, transporte e manejo inadequados e riscos afins. O licitante detentor do melhor preço, nesse caso, se obriga a informar com antecedência mínima de 02 (dois) dias úteis, sobre todos os requisitos necessários para a correta instalação física, elétrica e lógica dos equipamentos. Além disso, informará também sobre a necessidade adicional de criação e configuração de máquinas virtuais a serem providas pela PRODEMGE/SEPLAG.

8.7. O prazo para conclusão da Recepção Técnica é de 05 (cinco) dias úteis, a contar do recebimento da amostra pelo fornecedor da melhor oferta.

8.8. Após a Recepção Técnica, a licença encaminhada em meio físico deverá ser retirada pelo fornecedor.

9. DA EXECUÇÃO DO OBJETO

9.1. Prazo da prestação dos serviços:

9.1.1. O prazo máximo para implementação de toda a solução é de,

no máximo, 30 (trinta) dias corridos, contados do recebimento da Nota de Empenho e/ou da requisição de fornecimento

9.1.2. Devidamente justificado e antes de finalizado o prazo de entrega, o fornecedor do produto poderá solicitar prorrogação da entrega, ficando a cargo da área demandante aceitar a solicitação, desde que não haja prejuízo para a rede da CONTRATANTE.

9.2. **Os produtos serão recebidos:**

9.2.1. Provisoriamente, no ato da entrega, para efeito de posterior verificação da conformidade do material com a especificação, oportunidade em que se observarão apenas as informações constantes da fatura e das embalagens, em confronto com a respectiva nota de empenho;

9.2.2. Definitivamente, após a verificação da qualidade e quantidade do material e consequente aceitação, que deverá acontecer em até 10 (dez) dias úteis, contados a partir do recebimento provisório.

9.2.3. O descarregamento do produto ficará a cargo do fornecedor, devendo ser providenciada a mão-de-obra necessária.

9.2.4. Será considerada cumprida a entrega da quantidade de licenças adquiridas e a instalação das mesmas.

9.2.5. O recebimento/aprovação do(s) produto(s) pelo Órgão/Entidade não exclui a responsabilidade civil do fornecedor por vícios de quantidade ou qualidade do(s) produto(s) ou disparidades com as especificações estabelecidas, verificadas posteriormente, garantindo-se a Administração as faculdades previstas no art. 18 da Lei n.º 8.078/90.

9.3. **DO LOCAL DA PRESTAÇÃO DOS SERVIÇOS:**

9.3.1. As entregas deverão ser feitas a partir da demanda da Contratante.

9.3.2. Todos os produtos especificados no objeto deste Termo de Referência, exceto para as Caronas, deverão ser entregues, para os Órgãos Participantes, dentro dos limites territoriais do Estado de Minas Gerais em horário comercial, nos locais indicados pelos órgãos Contratantes, observando o disposto no art. 74 da Lei Federal n° 8.666/93.

9.3.3. Os locais corretos serão descritos pelos órgãos e entidades contratantes, conforme Autorização de Fornecimento ou Ordem de Serviço emitidos.

9.3.4. Provisoriamente, para efeito de posterior verificação da conformidade do objeto com as especificações, e caso seja encontrada alguma irregularidade, será fixado prazo para correção pela Contratada.

9.3.5. Definitivamente, após recebimento provisório, para verificação da integridade e realização de testes de funcionamento, se for o caso, e sendo aprovados, nos exatos termos do edital e da proposta vencedora, será efetivado o recebimento definitivo mediante expedição de termo circunstanciado e recibo aposto na Nota Fiscal (1ª e 2ª vias), que ocorrerá em até 10 (dez) dias úteis.

9.4. **CONDIÇÕES DE RECEBIMENTO:**

9.4.1. A emissão da Nota Fiscal/Fatura deve ser precedida do recebimento definitivo dos serviços, nos termos abaixo.

9.4.2. No prazo de até 2 dias corridos do adimplemento da parcela, a CONTRATADA deverá entregar toda a documentação comprobatória do cumprimento da obrigação contratual;

9.4.3. O recebimento provisório será realizado pelo fiscal técnico e setorial ou pela equipe de fiscalização após a entrega da documentação

acima, da seguinte forma:

9.4.3.1. A contratante realizará inspeção minuciosa de todos os serviços executados, por meio de profissionais técnicos competentes, acompanhados dos profissionais encarregados pelo serviço, com a finalidade de verificar a adequação dos serviços e constatar e relacionar os arremates, retoques e revisões finais que se fizerem necessários.

9.4.3.1.1. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

9.4.3.1.2. A Contratada fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

9.4.3.1.3. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

9.4.3.2. No prazo de até 7 dias corridos a partir do recebimento dos documentos da CONTRATADA, cada fiscal ou a equipe de fiscalização deverá elaborar Relatório Circunstanciado em consonância com suas atribuições, e encaminhá-lo ao gestor do contrato.

9.4.3.2.1. Quando a fiscalização for exercida por um único servidor, o relatório circunstanciado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

9.4.3.2.2. Será considerado como ocorrido o recebimento provisório com a entrega do relatório circunstanciado ou, em havendo mais de um a ser feito, com a entrega do último.

9.4.3.2.2.1. Na hipótese de a verificação a que se refere o parágrafo anterior não ser procedida tempestivamente, reputar-se-á como realizada, consumando-se o recebimento provisório no dia do esgotamento do prazo.

9.4.4. No prazo de até 7 dias corridos a partir do recebimento provisório dos serviços, o Gestor do Contrato deverá providenciar o recebimento definitivo, ato que concretiza o ateste da execução dos serviços, obedecendo as seguintes diretrizes:

9.4.4.1. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções;

9.4.4.2. Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, que comprove a adequação do objeto aos termos contratuais, com base nos relatórios e documentações apresentadas; e

9.4.4.3. Comunicar a empresa para que emita a Nota Fiscal ou

Fatura, com o valor exato dimensionado pela fiscalização, com base no Instrumento de Medição de Resultado (IMR), ou instrumento substituto.

9.4.5. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato, ou, em qualquer época, das garantias concedidas e das responsabilidades assumidas em contrato e por força das disposições legais em vigor.

9.4.6. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, às custas da Contratada, sem prejuízo da aplicação de penalidades.

10. DO PAGAMENTO:

10.1. O pagamento será efetuado através do Sistema Integrado de Administração Financeira - SIAFI/MG, por meio de ordem bancária emitida por processamento eletrônico, a crédito do beneficiário em um dos bancos que o fornecedor indicar, no prazo de até **30 (trinta)** dias corridos, contados a partir da data final do período de adimplemento a que se referir, com base nos documentos fiscais devidamente conferidos e aprovados pela CONTRATANTE.

11. DO CONTRATO:

11.1. Encerrado o procedimento licitatório, o representante legal do licitante declarado vencedor será convocado para firmar o termo de contrato, aceitar ou retirar o instrumento equivalente, de acordo com os art. 62, da Lei 8.666/93 e art. 4º, XXI, da Lei 10.520/2002.

11.2. O contrato tem vigência por 12 (doze) meses, a partir da publicação de seu extrato no Diário Oficial do Estado de Minas Gerais, podendo ser prorrogado por idêntico período até o limite máximo de 48 (quarenta e oito) meses, mediante celebração de termos aditivos, conforme dispõe o art. 57, IV da lei n.º 8.666/93.

11.2.1. Para os itens 1, 2, 3, 4, 5 do Lote 1 , o contrato celebrado será de 12 meses com possibilidade de prorrogação por idêntico período até o limite máximo de 48 (quarenta e oito).

11.2.2. Para os itens 6 e 7 do Lote 1 , o contrato celebrado será de 12 meses sem possibilidade de prorrogação.

12. PROCEDIMENTOS DE FISCALIZAÇÃO E GERENCIAMENTO DA RELAÇÃO JURÍDICA:

12.1. Atendendo às exigências contidas no inciso III do art. 58 e §§ 1º e 2º, do artigo 67 da Lei nº. 8.666 de 1993, será designado pela autoridade competente, agente para acompanhar e fiscalizar o contrato, como representante da Administração.

12.2. Em caso de eventual irregularidade, inexecução ou desconformidade na execução do contrato, o agente fiscalizador dará ciência à CONTRATADA, por escrito, para adoção das providências necessárias para sanar as falhas apontadas.

12.3. A fiscalização de que trata esta cláusula não exclui, nem reduz a responsabilidade da CONTRATADA por quaisquer irregularidades, inexecuções ou desconformidades havidas na execução do objeto, aí incluídas imperfeições de natureza técnica ou aquelas provenientes de vício redibitório, como tal definido pela lei civil.

12.4. O CONTRATANTE reserva-se o direito de rejeitar, no todo ou em

parte, o objeto da contratação, caso o mesmo afaste-se das especificações do Edital, seus anexos e da proposta da CONTRATADA.

12.5. Constatada a ocorrência de descumprimento total ou parcial de contrato, que possibilite a aplicação das sanções previstas neste instrumento, deverão ser observadas as disposições do art. 40 (e seguintes) do Decreto Estadual nº 45.902, de 27 de janeiro de 2012.

12.6. As decisões e providências que ultrapassarem a competência do Fiscal do Contrato serão encaminhadas à autoridade competente da CONTRATANTE para adoção das medidas convenientes, consoante disposto no § 2º do art. 67, da Lei nº.8.666/93.

12.6.1. Caberá ao gestor os controles administrativos/financeiros necessários ao pleno cumprimento do contrato.

13. DAS GARANTIAS:

13.1. Conforme item DA GARANTIA FINANCEIRA DA EXECUÇÃO definido no Edital.

14. SUPORTE TÉCNICO E GARANTIA

14.1. Contratada deverá prestar suporte técnico às licenças adquiridas durante todo o período de vigência contratual e Garantia.

14.2. Durante o período de vigência da garantia, a CONTRATANTE terá direito a atualização de versão de todos os softwares contratados.

14.3. A CONTRATADA deverá dispor de equipe técnica qualificada para a entrega, instalação, configuração, repasse de conhecimento, suporte técnico e garantia.

14.4. O serviço de suporte técnico deverá ser prestado no idioma português.

14.5. Toda a manutenção da solução (licenças) durante o período de garantia, será de inteira responsabilidade da contratada, nos termos e condições especificados neste termo de referência.

14.6. Todas as entregas, instalações, configurações, personalizações, atualizações, manutenções, correções, entre outros, ficarão todos a cargo única e exclusivamente da futura empresa a ser CONTRATADA.

14.7. A total responsabilidade pela garantia e manutenção da solução a ser disponibilizada e de todos os serviços prestados, serão de única e exclusiva responsabilidade da futura empresa a ser CONTRATADA.

14.8. Garantia e manutenção das licenças durante o período de vigência

14.9. Excepcionalmente, na ocorrência de incidentes tais como o comprometimento sistêmico de uma defensoria ou comprometimento da solução ofertada (indisponibilidade de serviço que afete a efetividade da solução de forma significativa ou que acarrete em parada das atividades dos usuários).

14.10. Os chamados de suporte técnico serão classificados tendo como referência os níveis de severidade apresentados no Anexo I (B) - Níveis de Serviços.

14.11. A Contratada deverá atender aos chamados respeitando os prazos apresentados na tabela apresentada no Anexo I (B) - Níveis de Serviços.

14.12. A CONTRATADA deverá providenciar a coleta e transmissão dos arquivos de diagnóstico que o fabricante necessite para diagnosticar e solucionar o problema.

14.13. A CONTRATADA deverá verificar a disponibilização de releases de versões, patches ou atualizações de softwares da solução e informar o CONTRATANTE.

14.14. Caso haja necessidade de atualização de versão da solução, a

CONTRATADA deverá confeccionar o plano de mudança do parque institucional, informando as melhorias e os impactos no ambiente do CONTRATANTE. O plano de mudança deve ser devidamente documentado e entregue no prazo máximo de 1 mês, a contar da oficialização de pedido, para análise e aprovação da equipe técnica do CONTRATANTE.

14.15. Fica sob responsabilidade da CONTRATADA acompanhar a atualização do parque de endpoints junto com as equipes técnicas do CONTRATANTE.

14.16. O CONTRATANTE deverá fornecer lista de contatos de suas equipes técnicas para a CONTRATADA, atualizando-a sempre que necessário.

14.17. Fica sob responsabilidade da CONTRATADA a entrega do software de toda plataforma de gerência (locais e central) da solução fornecida atualizada e devidamente configurada, no prazo máximo de 1 mês, após aprovação do plano de mudança.

15. DA SUBCONTRATAÇÃO:

15.1. Não será permitido a subcontratação do objeto desta Ata de Registro de Preços.

16. OBRIGAÇÕES ESPECÍFICAS DAS PARTES:

16.1. DA CONTRATADA:

16.1.1. Prestar os serviços nas quantidades, prazos e condições pactuadas, de acordo com as exigências constantes neste documento.

16.1.2. Emitir faturas no valor pactuado, apresentando-as ao CONTRATANTE para ateste e pagamento.

16.1.3. Atender prontamente as orientações e exigências inerentes à execução do objeto contratado.

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

16.1.5. Todas as entregas, instalações, configurações, personalizações, atualizações, manutenções, correções, entre outros, ficarão todos a cargo única e exclusivamente da CONTRATADA.

16.1.6. Fica sob responsabilidade da CONTRATADA a entrega e instalação do software (locais e central) atualizado e devidamente configurado.

16.1.7. Assegurar ao CONTRATANTE o direito de sustar, recusar, mandar desfazer ou refazer qualquer serviço/produto que não esteja de acordo com as normas e especificações técnicas recomendadas neste documento.

16.1.8. Assumir inteira responsabilidade pela prestação dos serviços, responsabilizando-se por eventual transporte, acondicionamento e descarregamento dos materiais necessários a prestação, se houver.

16.1.9. Todos os custos da capacitação técnica com o instrutor serão de responsabilidade da CONTRATADA, incluindo transporte, hospedagem e alimentação.

16.1.10. Fornecer o material didático escrito (manuais) ou eletrônico (arquivo digital).

16.1.11. Prestar serviços de assistência técnica e suporte, compreendendo o diagnóstico e identificação de problemas, o apoio técnico na utilização, correção de erros, defeitos (bugs) ou mau funcionamento sobre qualquer funcionalidade, recurso, componente ou módulo disponível

de forma nativa ou decorrente de qualquer adaptação ou ajuste (customização) efetuado por ela.

16.1.12. Responsabilizar-se por todos os custos decorrentes do serviço de suporte técnico ofertado pela solução.

16.1.13. Garantir a confidencialidade, disponibilidade e integridade dos dados da CONTRATANTE gerenciados pela solução.

16.1.14. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade mínimas especificadas neste Termo de Referência e em sua proposta.

16.1.15. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado ao Estado ou à entidade estadual, devendo ressarcir imediatamente a Administração em sua integralidade, ficando a Contratante autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos.

16.1.16. Responsabilizar-se pela garantia dos materiais empregados na prestação dos serviços, dentro dos padrões adequados de qualidade, segurança, durabilidade e desempenho, conforme previsto na legislação em vigor e na forma exigida neste termo de referência.

16.1.17. Responsabilizar-se pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do objeto deste Termo de Referência.

16.1.18. Não transferir para o CONTRATANTE a responsabilidade pelo pagamento dos encargos estabelecidos no item anterior, quando houver inadimplência da CONTRATADA, nem onerar o objeto deste Termo de Referência.

16.1.19. Manter, durante toda a execução do objeto, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

16.1.20. Manter preposto, caso necessário, aceito pela Administração, para representá-lo no local da execução do objeto contratado.

16.2. **DA CONTRATANTE:**

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

16.2.2. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta

16.2.3. Rejeitar, no todo ou em parte os serviços prestados, se estiverem em desacordo com a especificação e da proposta comercial da CONTRATADA.

16.2.4. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas.

16.2.5. Conceder prazo de 03 (três) dias úteis, após a notificação, para a CONTRATADA regularizar as falhas observadas.

16.2.6. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA.

16.2.7. Aplicar à CONTRATADA as sanções regulamentares.

16.2.8. Exigir o cumprimento dos recolhimentos tributários, trabalhistas e previdenciários através dos documentos pertinentes.

16.2.9. Disponibilizar local adequado para a prestação do serviço, caso necessário.

17. SANÇÕES ADMINISTRATIVAS

17.1. A CONTRATADA que cometer qualquer das infrações, previstas na Lei Federal nº 8.666, de 21 de junho de 1993, na Lei Federal nº 10.520, de 17 de julho de 2002, Lei Estadual n.º 14.167, de 10 de janeiro de 2002 e no Decreto Estadual nº. 45.902, de 27 de janeiro de 2012, e no Decreto Estadual nº 48.012, de 22 de julho de 2020, ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

17.1.1. advertência por escrito;

17.1.2. multa de até:

17.1.2.1. 0,3% (três décimos por cento) por dia, até o trigésimo dia de atraso, sobre o valor do objeto não executado;

17.1.2.2. 10 % (dez por cento) sobre o valor da nota de empenho ou do contrato, em caso de recusa do adjudicatário em efetuar o reforço de garantia financeira de execução exigida ou por ocasião da prorrogação;

17.1.2.3. 20% (vinte por cento) sobre o valor do fornecimento depois de ultrapassado o prazo de 30 dias de atraso, ou no caso de não entregado objeto, ou entrega com vícios ou defeitos ocultos que o torne impróprio ao uso a que é destinado, ou diminua-lhe o valor ou, ainda fora das especificações contratadas;

17.1.2.4. 2 % (dois por cento) sobre o valor total do contrato ou instrumento equivalente, em caso de descumprimento das demais obrigações contratuais ou norma da legislação pertinente.

17.1.3. Suspensão do direito de participar de licitações e impedimento de contratar com a Administração, pelo prazo de até 2 (dois) anos;

17.1.4. Impedimento de licitar e contratar com a Administração Pública Estadual, nos termos do art. 7º da lei 10.520, de 2002;

17.1.5. Declaração de inidoneidade para licitar ou contratar com a Administração Pública;

17.2. A sanção de multa poderá ser aplicada cumulativamente às demais sanções previstas nos itens 17.1.3, 17.1.4, 17.1.5.

17.3. A multa será descontada da garantia do contrato, quando houver, e/ou de pagamentos eventualmente devidos ao INFRATOR e/ou cobrada administrativa e/ou judicialmente.

17.4. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo incidental apensado ao processo licitatório ou ao processo de execução contratual originário que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto no Decreto Estadual nº. 45.902, de 27 de janeiro de 2012, bem como o disposto na Lei 8.666, de 1993 e Lei Estadual nº 14.184, de 2002.

17.5. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

17.5.1. Não serão aplicadas sanções administrativas na ocorrência de casos fortuitos, força maior ou razões de interesse público, devidamente comprovados.

17.6. A aplicação de sanções administrativas não reduz nem isenta a obrigação da CONTRATADA de indenizar integralmente eventuais danos causados a Administração ou a terceiros, que poderão ser apurados no mesmo processo administrativo sancionatório.

17.7. As sanções relacionadas nos itens 17.1.3, 17.1.4 e 17.1.5 serão obrigatoriamente registradas no Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual –CAFIMP e no Cadastro Geral de Fornecedores no âmbito da administração direta, autárquica e fundacional do Poder Executivo de Minas Gerais - CAGEF.

17.8. As sanções de suspensão do direito de participar em licitações e impedimento de licitar e contratar com a Administração Pública poderão ser também aplicadas àqueles que:

17.8.1. Retardarem a execução do objeto;

17.8.2. Comportar-se de modo inidôneo;

17.8.2.1. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

17.8.3. Apresentarem documentação falsa ou cometerem fraude fiscal.

17.9. Durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei Federal nº 12.846, de 2013, e pelo Decreto Estadual nº 46.782, de 2015, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à Controladoria-Geral do Estado, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo de Responsabilização – PAR.

18. ESTIMATIVA DE PREÇOS E PREÇOS REFERENCIAIS

18.1. O custo estimado da contratação será tornado público apenas e imediatamente após o encerramento do envio de lances (art. 7º, § 3º, da Lei Federal nº 12.527/2014)", tendo em vista o art. 15, § 1º, do Decreto Estadual nº 48.012/2020: *§ 1º – O caráter sigiloso do valor estimado ou do valor máximo aceitável para a contratação será fundamentado no § 3º do art. 7º da Lei Federal nº 12.527, de 18 de novembro de 2011.*

Rosalvo França Junior

Diretoria Central de Gestão de Serviços e Infraestrutura de TIC

Superintendência Central de Governança Eletrônica

Weslley Costa Nogueira

Diretor Central de Gestão de Serviços e Infraestrutura de TIC

Superintendência Central de Governança Eletrônica

Documento assinado eletronicamente por **Rosalvo Franca Junior**, **Servidor(a) Público(a)**, em 28/03/2023, às 16:10, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Weslley Costa Nogueira**, **Diretor**, em 28/03/2023, às 16:30, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Anexo nº I (A) - Detalhamento do Objeto/SEPLAG/DCGSITIC/2023

PROCESSO Nº 1500.01.0113446/2022-67

1. SOLUÇÃO DE ENDPOINT:

1.1. **Itens 1** (Cod SIRP **000119750**), **2** (Cod SIRP **000119768**), **3** (Cod SIRP **000119776**), **4** (Cod SIRP **000119784**) e **5** (Cod SIRP **000119792**) 12 meses:

1.1.1. **Característica da Solução de Antivírus**

1.1.1.1. As licenças devem contemplar módulos e agentes das chamadas soluções de proteção de Endpoint e Servidores de nova geração;

1.1.1.2. Prover segurança para estações de trabalho sejam físicas, ou em ambiente virtualizado e também prover segurança para ambientes virtualizados com a utilização ou não de agentes (VDIO direito de uso das licenças dos softwares contempla o direito de atualização das versões, das bases de dados (lista de vírus e vacinas), e os serviços de suporte pelo período de 12 (doze) meses;

1.1.1.3. Possuir console central única de gerenciamento das configurações do Antivírus, Anti-spyware, Firewall, Proteção Contra Intrusos, controle de Dispositivos e Controle de Aplicações deverão ser realizadas através da mesma console.

1.1.1.4. Dar suporte total aos sistemas operacionais clientes (Estações de trabalho e Servidores) baseados nas plataformas:

a. Windows
b. Windows Server
c. Red Hat Enterprise Linux e distribuições
d. Mac OS

1.1.1.5. A solução ofertada deve estar na linha atual de comercialização e suporte do fabricante.

1.1.1.6. O antivírus deverá promover mecanismos de customização de instalação em clientes e servidores, com possibilidade de uso de pacotes de instalação auto executáveis xe), instalação silenciosa, definição de módulos através de políticas a serem instalada.

1.1.1.7. Possibilidade de instalação do software em servidores, estações de trabalho, máquinas virtualizadas, dispositivos moveis, via console de gerenciamento, com opção de remoção de soluções antivírus previamente instaladas;

1.1.1.8. A console deve suportar arquitetura On-Premise OU arquitetura Cloud-Based e deve ser acessada via WEB (HTTPS) ou MMC;

1.1.1.9. As licenças deverão permanecer funcional utilizando as últimas definições recebidas para a proteção contra códigos maliciosos após o vencimento do contrato;

1.1.2. **Módulo de Proteção Anti-Malware**

1.1.2.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

a. Windows
b. Windows Server
c. Red Hat Enterprise Linux 7 e distribuições
d. Mac OS

1.1.2.2. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;

1.1.2.3. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;

1.1.2.4. A solução deve ser capaz de bloqueio e monitoramento de KeyLoggers, anonimizadores de proxy, crackers de senhas e ameaças semelhantes.

1.1.2.5. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:

- Processos em execução em memória principal (RAM);
- Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);
- Arquivos compactados automaticamente, em pelo menos três dos seguintes formatos: zip, exe, arj, MIME/uu, CAB;

1.1.2.6. Arquivos recebidos por meio de programas de comunicação instantânea (MSN Messenger, yahoo messenger, google talk, icq, dentre outros Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como JavaScript, VBSscript/Activex;

1.1.2.7. Deve possuir detecção heurística de vírus desconhecidos;

1.1.2.8. Deve permitir configurar o consumo de CPU que será utilizada para uma varredura manual ou agendada; OU Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

1.1.2.9. Deve permitir diferentes configurações de detecção (varredura ou rastreamento):

1.1.2.9.1. Em tempo real de arquivos acessados pelo usuário;

1.1.2.9.2. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;

1.1.2.9.3. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

1.1.2.9.4. Automáticos do sistema com as seguintes opções:

- Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;
- Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);
- Frequência: horária, diária, semanal e mensal;
- Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreado

1.1.2.9.5. Deve possuir mecanismo de cache de informações dos arquivos já escaneados;

1.1.2.9.6. Em caso de arquivos suspeitos, a solução deve ter a capacidade de enviar o artefato para um ambiente de sandbox do próprio fabricante para identificar ameaças desconhecidas;

1.1.2.9.7. O módulo de análise de artefatos desconhecidos (sandbox) deve estar integrada à solução de anti-malware, sem necessidade de plug-ins adicionais;

1.1.2.9.8. O módulo de sandbox deve permitir a análise de arquivos submetidos diretamente dos agentes;

1.1.2.9.9. Em caso de ameaças desconhecidas detectadas pela sandbox, a solução deve ter a capacidade de adicionar os objetos suspeitos (hash de arquivo, IP, domínio e URL) numa lista de bloqueio automaticamente;

1.1.2.9.10. Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

1.1.2.9.11. Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL’s maliciosas, de modo a prover, rápida detecção de novas ameaças;

1.1.2.9.12. Deve ser capaz de aferir a reputação das URL’s acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;

1.1.2.9.13. Deve ser capaz de detectar variantes de malware que possam ser geradas em tempo real na memória da estação de trabalho ou notebook;

1.1.2.9.14. Deve possuir capacidade de escaneamento de arquivos compactados e, em caso de identificação de um arquivo malicioso, apenas este deve ser removido, mantendo osdemais intactos;

1.1.2.9.15. Deve ser capaz de bloquear o acesso a sites maliciosos mesmo que não previamente analisados pelo fabricante;

1.1.2.9.16. Deve permitir a restauração de maneira granular de

arquivos quarentenados sob suspeita de representarem risco de segurança;

1.1.2.9.17. Deve permitir a restauração dos arquivos quarentenados e a adição as listas de exclusão, de modo a evitar novas detecções dos arquivos;

1.1.2.9.18. Deverá ter funcionalidade de Machine Learning para detectar e tomar ações sobre ameaças desconhecidas e suspeitas;

1.1.2.9.19. Deve fornecer a cadeia de ataque de forma compreensiva de cada simulação que descreva as ações e respectivos metadados, bem como, o veredito emitido pela tecnologia de Machine Learning;

1.1.2.9.20. Deve bloquear processos comuns associados a ransomware;

1.1.2.9.21. Em casos de ataques de ransomware, a solução deve ter a capacidade de interromper o processo de criptografia e restaurar os arquivos originais aos seus respectivos diretórios;

1.1.2.9.22. Deve possuir funcionalidade de detecção de malwares conhecidos e desconhecidos por comportamento;

1.1.2.9.23. Deve permitir a integração com solução de análise de artefatos suspeitos (sandbox) do próprio fabricante.

1.1.3. **Função: Atualização**

1.1.3.1. Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência(no mínimo diária) e horários definidos pelo administrador da solução;

1.1.3.2. Deve permitir atualização incremental da lista de definições de vírus;

1.1.3.3. Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

1.1.3.4. Deve permitir o rollback das atualizações das listas de definições de vírus e politicas;

1.1.3.4.1. Não se aplica as soluções de Next-Generation Endpoint em nuvem, tais soluções utilizam-se de camadas adicionais de segurança como Inteligência Artificial, Anti-Exploit , AntiRansonware e ameaças zero-day que tem sua efetividade em detecção em tempo real e detecção comportamental, não trabalhando com listas de vacinas e vírus que podem ter sua eficácia comprometida diante ameaças novas.

1.1.3.5. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utilizá-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;

1.1.3.6. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix ou configurações específicas de domínios/grupos da árvore de gerenciamento;

1.1.3.7. O agente replicador de atualizações e configurações, deve ser

capaz de armazenar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização.

1.1.4. **Função: Administração**

1.1.4.1. Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;

1.1.4.2. Deve possibilitar instalação "silenciosa";

1.1.4.3. Deve permitir o bloqueio por nome de arquivo;

1.1.4.4. Deve permitir o rastreamento e bloqueio de infecções;

1.1.4.5. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;

1.1.4.6. Quando On-premise, deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado, podendo ou não ser necessário à sua reinicialização;

1.1.4.7. Em caso de soluções em nuvem (Cloud), será aceita utilização de ferramenta do próprio fabricante para efetuar a instalação remota nas estações de trabalho;

1.1.4.8. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;

1.1.4.9. Deve permitir a desinstalação através da console de gerenciamento da solução;

1.1.4.10. Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;

1.1.4.11. Deve ter a possibilidade de determinar a capacidade de armazenamento da área de quarentena;

1.1.4.12. Deve permitir a deleção dos arquivos quarentenados;

1.1.4.13. Deve permitir remoção automática de clientes inativos por determinado período de tempo;

1.1.4.14. Deve permitir integração com serviço de autenticação como Active Directory para acesso a console de administração;

1.1.4.15. Quando on-premise, identificar através da integração com o Active Directory, quais máquinas estão sem a solução de anti-malware instalados;

1.1.4.16. Em caso de soluções em nuvem (Cloud), será aceita utilização de ferramenta do próprio fabricante para varredura local;

1.1.4.17. Deve permitir criação de diversos perfis e usuários para acesso a console de administração;

1.1.4.18. Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

1.1.4.19. Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;

1.1.4.20. Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory, tipo ou IP;

1.1.4.21. Deve permitir criação de grupos consecutivos dentro da árvore de gerenciamento;

1.1.4.22. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

1.1.4.23. Deve registrar no sistema de monitoração da console de anti-malware informações relativas ao usuário logado no sistema operacional;

1.1.4.24. Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;

1.1.4.25. Deve prover criptografia para as comunicações entre o servidor e os agentes de proteção;

1.1.4.26. Deve permitir a criação de usuários locais de administração da console de anti-malware;

1.1.4.27. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;

1.1.4.28. Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;

1.1.4.29. Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;

1.1.4.30. Deve permitir a gerência de domínios separados para usuários previamente definidos;

1.1.4.31. Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração;

1.1.4.32. Deve permitir configuração do serviço de proteção de sites da web, em níveis de segurança: Baixo, Recomendado e Alto.

1.1.5. **Função: Controle de Dispositivos**

1.1.5.1. As configurações da funcionalidade de controle de dispositivos devem ser aplicadas por usuário;

1.1.5.2. Deve permitir políticas e ações diferentes para dispositivos conectados à rede interna e aqueles utilizados na rede externa (conectado à Internet, por exemplo);

1.1.5.3. Deve possuir controle de acesso a discos removíveis

reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;

1.1.5.4. Deve possuir o controle de acesso a drives de mídias de armazenamento externo tais como CD-ROM, DVD, PENDRIVE e OUTROS, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

1.1.5.5. Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle permitindo ou não o acesso ao dispositivo;

1.1.5.6. Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, CD-ROM);

1.1.5.7. Para ação de restrição como o bloqueio, a solução deve permitir adicionais dispositivos USB autorizados, bem como apontar executáveis específicos como exceção ao bloqueio;

1.1.5.8. Deve ter a capacidade de bloquear a função de Autorun nos dispositivos;

1.1.5.9. Deve permitir controle de permissão ou bloqueio para dispositivos que não armazenam dados tendo, pelo menos, os seguintes tipos de dispositivos: adaptadores bluetooth, modems, interfaces wireless externas, cartões PCMCIA, dispositivos infravermelhos e portas COM/LP

1.1.6. **Função de HIPS – Host IPS e Host Firewall**

1.1.6.1. Deve ser capaz de realizar a detecção/proteção contra exploração de vulnerabilidades nos seguintes sistemas operacionais:

- Windows 7 SP1 (x86/x64);
- Windows 8.1 (x86/x64);
- Windows 10 (x86/x64);
- Windows 11 (x64).

1.1.6.2. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de hostIPS e host firewall;

1.1.6.3. As regras de vulnerabilidades deverão possuir a opção de criar exceção;

1.1.6.4. Todas as regras das funcionalidades de firewall e IPS de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

1.1.6.5. Deve permitir ativar e desativar o produto sem a necessidade de remoção;

1.1.6.6. Deve permitir que o usuário altere as configurações de níveis de segurança e exceções;

1.1.6.7. O modulo de HIPS deverá possuir perfis pré-determinados baseados em performance ou segurança;

1.1.6.8. O modulo de HIPS deverá possuir regras para proteger contra ameaças do tipo Ransomware;

1.1.6.9. O modulo de HIPS deverá conter regras contra exploit, vulnerabilidades e genéricas protegendo contra ameaças conhecidas ou

desconhecidas;

1.1.6.10. módulo de HIPS deverá permitir que o administrador monitore apenas ou realize o bloqueio das tentativas de exploração de vulnerabilidades;

1.1.6.11. A solução ofertada deve ser capaz de possibilitar visualizar as aplicações existentes, as vulnerabilidades de software encontradas e os CVE's relacionados as mesmas.

1.1.7. **Módulo – Controle de Aplicações**

1.1.7.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

- Windows 7 SP1 (x86/x64);
- Windows (x86/x64);
- Windows 10 (x64);
- Windows 11 (x64).

1.1.7.2. As regras de controle de aplicação devem permitir as seguintes ações:

- Permissão de execução;
- Bloqueio de execução;
- Bloqueio de novas instalações.

1.1.7.3. A regra de liberação para o controle de aplicação deverá analisar o programa liberado, analisando a criação de outros processos;

1.1.7.4. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos(logs), sem a efetivação da ação regra;

1.1.7.5. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:

- Assinatura MD5 ou SHA-1 e SHA-256 do executável;
- Atributos do certificado utilizado para assinatura digital do executável
- Caminho lógico do executável;
- Base de assinaturas de certificados digitais válidos e seguro

1.1.7.6. As regras de controle de aplicação devem possuir categorias pré-determinadas de aplicações;

1.1.7.7. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações;

1.1.7.8. O módulo de controle de aplicativos deve:

1.1.7.8.1. Possuir uma lista de aplicações mal-intencionados para bloqueio e monitoramento; OU Possuir lista pré-definida de aplicações, atualizadas automaticamente pelo fabricante, para que se possa utilizar regras de blacklist ou whitelist.

1.1.7.8.2. Permitir também criar listas de aplicações que não são permitidas efetuando o bloqueio das mesmas ou criar lista de aplicações internas para que não sejam bloqueadas pela aplicação.

1.1.7.8.3. Permitir a busca por aplicações ou fabricante destas;

1.1.7.8.4. Possuir ferramenta para extrair o hash de executáveis, também deve permitir a importação destes hashes.

1.2. **Tecnologias e Versões suportadas pela Ferramenta - Detalhamento**

1.2.1. **Servidor de Administração e Console Administrativa**

1.2.1.1. Compatibilidade:

- Microsoft Windows Server 2012 Standard / Core / Foundation / Essentials / Datacenter x64;
- Microsoft Storage Server 2012 e 2012 R2 x64;
- Microsoft Windows Server 2012 R2 Standard / Core / Foundation / Essentials / Datacenter x64;
- Microsoft Windows Server 2016 Standard / Core / Datacenter x64;
- Microsoft Windows Server 2019 Standard / Core / Datacenter x64;
- Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;
- Microsoft Windows 8 SP1 Professional / Enterprise x32/x64;
- Microsoft Windows 8 R2 Professional / Enterprise x64;
- Microsoft Windows 8.1 R2 Professional / Enterprise x32;
- Microsoft Windows 8.1 R2 Professional / Enterprise x64;
- Microsoft Windows 10 x32;
- Microsoft Windows 10 x64;
- Windows 10 21H1 31-bit/64-bit;

1.2.1.1.1. Suporta as seguintes Plataformas Virtuais:

- VMware: Workstation 16.2.3 ou superior, vSphere 6.5 ou superior;
- Microsoft Hyper-V: 2012, 2012 R2, 2016, 2019 x64;

1.2.1.2. Características:

- A console deve ser acessada via WEB (HTTPS) ou MMC;
- A console deve suportar arquitetura on-premise ou arquitetura cloud-based;
- Console deve ser baseada no modelo cliente/servidor;
- A console deve suportar autenticação de dois fatores;

a. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;

b. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;

1.2.1.2.1. Deve permitir incluir usuários do AD para logar em no console de administração;

1.2.1.2.2. Console deve ser totalmente integrada com suas funções

e módulos;

1.2.1.2.3. As licenças deverá permanecer funcional mesmo após expirado a validade da mesma para a proteção contra códigos maliciosos utilizando as ultimas definições recebidas no momento da expiração da licença;

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

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

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

1.2.1.2.7. Deve armazenar histórico das alterações feitas em políticas;

1.2.1.2.8. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada OU por clonagem;

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

1.2.1.2.10. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

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

1.2.1.2.12. A solução de gerência centralizada deve permitir visualizar eventos, gerenciar políticas e adicionar relatórios.

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

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

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

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

1.2.1.2.17. Capacidade de criação de grupos de computadores com políticas distintas dos demais grupos;

1.2.1.2.18. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;

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

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

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

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

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

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

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

1.2.1.2.25. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;

1.2.1.2.26. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

1.2.1.2.27. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;

1.2.1.2.28. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

1.2.1.2.29. Deve fornecer as seguintes informações dos computadores:

- Se o antivírus está instalado;
- Se o antivírus está iniciado;
- Se o antivírus está atualizado;
- Minutos/horas desde a última conexão da máquina com o servidor administrativo;
- Minutos/horas desde a última atualização de vacinas;
- Data e horário da última verificação executada na máquina;
- Versão do antivírus instalado na máquina;
- Se é necessário reiniciar o computador para aplicar mudanças;
- Data e horário de quando a máquina foi ligada;

- Quantidade de vírus encontrados (contador) na máquina;
- Nome do computador;
- Domínio ou grupo de trabalho do computador;
- Data e horário da última atualização de vacinas;
- Sistema operacional com Service Pack;
- Sessões de usuários, com informações de contato (caso disponíveis no Active Directory);
- Endereço IP;
- Vulnerabilidades de aplicativos instalados na máquina;

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

1.2.1.2.31. Para soluções On-Premise, capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

- Alteração de Gateway Padrão;
- Alteração de sub redes;
- Alteração de domínio;
- Alteração de servidor DHCP;
- Alteração de servidor DNS;
- Alteração de servidor WINS;
- Resolução de Nome;
- Disponibilidade de endereço de conexão SSL;

1.2.1.2.32. Para soluções Cloud, capacidade de reconectar máquinas clientes ao servidor administrativo por meio da nuvem do fabricante:

- Alteração de Gateway Padrão;
- Alteração de sub redes;
- Alteração de domínio;
- Alteração de servidor DHCP;
- Alteração de servidor DNS;
- Alteração de servidor WINS;
- Resolução de Nome;
- Disponibilidade de endereço de conexão SSL;

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

1.2.1.2.34. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

1.2.1.2.35. Capacidade de relacionar servidores em estrutura de

hierarquia para obter relatórios sobre toda a estrutura de antivírus;

1.2.1.2.36. A console de gerenciamento deve suportar funções de controle de acesso com base na função (RBAC – Controle de acesso baseado em funções) para a hierarquia de servidores;

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

1.2.1.2.38. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

1.2.1.2.39. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;

1.2.1.2.40. Capacidade de exportar relatórios PARA NO MÍNIMO DE DOIS dos seguintes tipos de arquivos: PDF, HTML , XML e CSV;

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

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

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

1.2.1.2.43.1Deve encontrar computadores na rede através de no mínimo três formas:

- Domínio,
- Active Directory
- Subredes;

1.2.1.2.44. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server R2;

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

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

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

1.2.1.2.48. Deve permitir a configuração de senha no endpoint e configurar quando queserá necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de Scan for criada localmente no endpoint);

1.2.1.2.49. Capacidade de realizar atualização incremental de vacinas

nos computadores;

1.2.1.2.50. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

- Nome do vírus;
- Nome do arquivo infectado;
- Data e hora da detecção;
- Nome da máquina ou endereço IP;

1.2.1.2.51. Ação realizar Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

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

1.2.1.2.53. Capacidade de voltar (rollback) para versão de atualização anterior através de procedimento especifico na console de gerenciamento e/ou backup realizada.

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

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

1.2.1.2.56. Capacidade de diferenciar máquinas virtuais de máquinas física.

1.2.2. **Estações Windows**

- Microsoft Windows 7 Professional/Enterprise/Home SP1 x86 / x64;
- Microsoft Windows 8 Professional/Enterprise x86 / x64;
- Microsoft Windows 8.1 Professional / Enterprise x86 / x64;
- Microsoft Windows 10 Pro / Enterprise / Home / Education x86 / x64;
- Microsoft Windows Server 2019 Essentials / Standard / Datacenter;
- Microsoft Windows Server 2016 Essentials / Standard / Datacenter;
- Microsoft Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Microsoft Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Microsoft Windows Server 2008 R2 Foundation / Essentials / Standard / Datacenter SP1;
- Microsoft Windows Small Business Server 2011 Standard / Standard x64;
- Microsoft Windows MultiPoint Server 2011 x64;

1.2.2.1. Características:

1.2.2.1.1. Deve prover as seguintes proteções ou capacidade de escolher quais módulos serão instalados, tanto na instalação local

quanto na instalação remota e/ou através de política;

- Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etque verifique qualquer arquivo criado, acessado ou modificado;
- Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
- Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
- O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
- Firewall com IDS;
- Autoproteção (contra-ataques aos serviços/processos do antivírus);
- Controle de dispositivos externos;
- Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc
- Controle de acesso a sites por horário;
- Controle de acesso a sites por usuários;
- Controle de acesso a websites por dados, ex: Bloquear websites com conteúdo de vídeo e áudio;
- Controle de execução de aplicativos;
- Controle de vulnerabilidades do Windows e dos aplicativos instalados;
- Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota e/ou através de política;
- As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
- Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação, e/ou fazer a remoção do outro antivírus caso o pacote não seja gerado para permitir coexistência
- Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação
- Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (exemplo: “Win3rojaanker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

1.2.2.1.2. Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;

1.2.2.1.3. Deverá possuir módulo dedicado para proteção contra

port scanning;

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

1.2.2.1.5. Deve ser capaz de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

1.2.2.1.6. Deve ser capaz de, no endpoint protegido, detectar de modo automático o tipo e versão do SO, detectando também as demais aplicações;

1.2.2.1.7. Deve proteger automaticamente contra exploração de vulnerabilidades existentes no SO e nas aplicações não necessitando da criação e configuração de regras ou tarefas específicas para isto;

1.2.2.1.8. Deve permitir aplicar automaticamente, mediante aprovação prévia, e também via configuração de tarefas as correções disponibilizadas pelos fabricantes para proteção contra vulnerabilidades detectadas;

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

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

1.2.2.1.11. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

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

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

a. Do objeto SHA256;
b. Do objeto MD5.

1.2.2.1.14. Capacidade de verificar somente arquivos novos e alterados;

1.2.2.1.15. Capacidade de verificar objetos usando heurística;

1.2.2.1.16. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias, através de política;

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

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

- Perguntar o que fazer, ou;
- Bloquear acesso ao objeto;
- Apagar o objeto ou tentar desinfetá-lo (de acordo com a

configuração pré-estabelecida pelo administrador);

- Caso positivo de desinfecção: Restaurar o objeto para uso;
- Caso negativo de desinfecção: Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

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

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

1.2.2.1.21. Capacidade de verificar links inseridos em e-mails contra phishings;

1.2.2.1.22. Capacidade de verificar tráfego nos browsers: Internet Explorer (Microsoft Edge), Firefox, Google Chrome Opera;

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

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

- Perguntar o que fazer, ou;
- Bloquear o e-mail;
- Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
- Caso positivo de desinfecção: Restaurar o e-mail para o usuário;
- Caso negativo de desinfecção: Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

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

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

1.2.2.1.27. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, et, usando heurísticas;

1.2.2.1.28. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;

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

- Perguntar o que fazer, ou;
- Bloquear o acesso ao objeto e mostrar mensagem sobre o bloqueio, ou;
- Permitir acesso ao objeto;

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

a. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo real, ou;
b. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;

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

1.2.2.1.32. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosa;

1.2.2.1.33. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

1.2.2.1.34. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;

1.2.2.1.35. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://wwntiphishinrg/);

1.2.2.1.36. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica ou gerenciando ou ativando caso necessário o FW do Windows;

1.2.2.1.37. Deve possuir módulo IDS (Intrusion Detection System) para proteção contraport scans e exploração de vulnerabilidades de software;

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

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

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

a. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
b. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizado Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

    - Discos de armazenamento locais;
    - Armazenamento removível;
    - Impressoras;

- CD/DVD;
- Drives de disquete;
- Modems;
- Dispositivos de fita;
- Dispositivos multifuncionais;
- Leitores de smart card;
- Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, et;
- Wi-Fi;
- Adaptadores de rede externos;
- Dispositivos MP3 ou smartphones;
- Dispositivos Bluetooth;
- Câmeras e Scanner

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

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

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

1.2.2.1.44. Deve permitir controlar o acesso a dispositivos externos com base em prioridade de regra;

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

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

1.2.2.1.47. Capacidade de limitar a execução de aplicativos por hash MD5 ou SHA-256, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);

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

a. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.
b. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
c. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;
d. Capacidade de, caso o computador cliente saia da rede

corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewal até controle de aplicativos, dispositivos e acesso à web. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiro.

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

f. Capacidade de integração com a Anti-malware Scan Interface (AMSI).Deve permitir realizar o gerenciamento por meio de integração via REST API. Deve permitir o gerenciamento remoto da solução por meio de aplicativos de administração remota."

1.2.3. **Anti–Malware para Mac OS**

1.2.3.1. O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais:

- MacOS 11.6 (Big Sur);
- MacOS 12.5 (Monterey);
- MacOS 10.14 (Mojave);
- MacOS 10.15 (Catalina);

1.2.3.2. Suporte ao Apple Remote Desktop para instalação remota da solução;

1.2.3.3. Gerenciamento integrado à console de gerência central da solução;

1.2.3.4. Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos;

1.2.3.5. Permitir a verificação das ameaças da maneira manual e agendada;

1.2.3.6. Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus;

1.2.3.7. Permitir a ações de reparar arquivo ou colocar em quarentena em caso desinfeções a arquivos;

1.2.4. **Estações Linux**

1.2.4.1. Compatibilidade:

1.2.4.1.1. Plataforma 64-bits:

- Red Hat® Enterprise Linux® 8 Server;
- CentOS 7.2;
- Ubuntu 20.04 LTS;
- Debian GNU / Linux 10.1;
- Oracle Linux 8;
- SUSE® Linux Enterprise Server 15;

1.2.4.2. Características:

1.2.4.2.1. Deve prover as seguintes proteções:

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

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

- Via linha de comando;
- Via console administrativa;
- Via GUI;
- Via web (remotamente);

1.2.4.2.3. Deve possuir funcionalidade de Scan de drives removíveis, tais como:

- CDs;
- DVDs;
- Discos Blu-ray;
- Flash drives (pen drives);
- HDs externos;

1.2.4.2.4. Deve fornecer os seguintes controles para dispositivos externos conectados ao computador:

- Por tipo de dispositivo;

1.2.4.2.5. Por barramento de conexão As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

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

- Capacidade de criar exclusões por local, máscara e nome da ameaça;
- Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
- Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

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

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

- Alta;

- Média;
- Baixa;
- Recomendado;

1.2.4.3. Gerenciamento de Quarentena:

1.2.4.3.1. Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

1.2.4.3.2. Verificação por agendamento:

- Procura de arquivos infectados e suspeitos(incluindo arquivos em escopos especificados);
- Análise de arquivos;
- Desinfecção ou remoção de objetos infectado

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

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

1.2.4.3.4. Capacidade de verificar objetos usando heurística;

1.2.4.3.5. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

1.2.4.3.6. Deve fornecer análise de todo o tráfego HTTP/HTTPS/FTP que chegar no computador do usuário.

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

- Detecção de phishing e sites maliciosos;
- Bloqueio de download de arquivos maliciosos;
- Bloqueio de adware;

1.2.4.3.8. Deve possuir módulo de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados e/ou definidos via política/configuração na console de gerenciamento;

1.2.4.3.9. Deve fornecer a possibilidade de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux Deve possuir módulo de proteção contra criptografia maliciosa.

1.2.5. **Servidores Windows**

1.2.5.1. Compatibilidade:

1.2.5.1.1. Plataforma 32-bits:

- Windows Server 2003, 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;
- Windows Server 2008 Standard /Enterprise/Datacenter SP1 e posterior;
- Windows Server 2008 Core Standard/Enterprise/Datacenter SP1

e posterior;

1.2.5.1.2. Plataforma 64-bits

- Microsoft Windows Server 2008 R2 Foundation / Standard / Enterprise / Data Center SP1 ou posterior;
- Microsoft Windows Server 2008 R2 Core Standard / Enterprise / Data Center SP1 ou posterior;
- Microsoft Small Business Server 2008 R2 Standard / Premium
- Microsoft Windows Hyper-V Server 2008 R2 SP1 e posterior;
- Microsoft out Small Business Server 2011 Essentials / Standard;
- Microsoft Windows MultiPoint Server 2011;
- Microsoft MultiPoint Server 2012 Standard / Premium;
- Microsoft Windows MultiPoint Server 2016
- Windows 10 Enterprise multi-session;
- Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;
- Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
- Microsoft Windows Server 2012, 2012 R2 Core Standard / Datacenter;
- Microsoft Windows Storage Server 2012, 2012 R2;
- Microsoft Windows Hyper-V Server 2012, 2012 R2;
- Windows Server 2016 Essentials /Standard / Datacenter;
- Windows Server 2016 Core Standard / Datacenter;
- Windows Storage Server 2016, 2019;
- Windows Hyper-V Server 2016, 2019;
- Windows Server 2019 Essentials/Standard / Datacenter /Core/Terminal;
- Compatibilidade com Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;

1.2.5.2. Características:

1.2.5.2.1. Deve prover as seguintes proteções:

- Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- Autoproteção contra-ataques aos serviços/processos do antivírus;
- Firewall com IDS;
- Controle de vulnerabilidades do Windows e dos aplicativos instalados;

1.2.5.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota, e/ou definidos via política/configuração na console de gerenciamento;

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

- Via console administrativa OU Cloud;
- Via web (remotamente);

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

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

- Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
- Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
- Leitura de configurações;
- Modificação de configurações;
- Gerenciamento de Backup e Quarentena;
- Visualização de logs;
- Gerenciamento de logs;
- Gerenciamento de ativação da aplicação;
- Gerenciamento de permissões (adicionar/excluir permissões acima);

1.2.5.2.6. Deve possuir bloqueio de inicialização de aplicativos baseado em whitelist O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

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

b. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

1.2.5.2.7. Capacidade de selecionar a opção de garantir performance na execução de funções de varredura em tempo real ou varredura sob demanda;

1.2.5.2.8. Bloquear malware tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede

1.2.5.2.9. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de

energia, erros, etc);

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

1.2.5.3. Deve ser capaz de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

1.2.5.4. Deve ser capaz de, no endpoint protegido, detectar de modo automático o tipo e versão do SO, detectando também as demais aplicações;

1.2.5.5. Deve proteger automaticamente contra exploração de vulnerabilidades existentes no SO e nas aplicações não necessitando da criação e configuração de regras ou tarefas específicas para isto;

1.2.5.6. Deve permitir aplicar automaticamente, mediante aprovação prévia, e também via configuração de tarefas as correções disponibilizadas pelos fabricantes para proteção contra vulnerabilidades detectadas;

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

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

1.2.5.6.3. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação;

1.2.5.6.4. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win3rojaanker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

1.2.5.6.5. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

1.2.5.6.6. Capacidade de verificar somente arquivos novos e alterados;

1.2.5.6.7. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, ST, arquivos compactados por compactadores binários, et;

1.2.5.6.8. Capacidade de verificar objetos usando heurística;

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

1.2.5.6.10. Capacidade de agendar uma pausa na verificação;

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

- Perguntar o que fazer, ou;
- Bloquear acesso ao objeto;

- Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
- Caso positivo de desinfecção: Restaurar o objeto para uso;
- Caso negativo de desinfecção: Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

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

1.2.5.6.13. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

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

1.2.5.6.15. Em caso de detecção de sinais de "Win3rojaanker" uma infecção ativa, deve possuir capacidade de, automaticamente:

a. Executar os procedimentos pré-configurados pelo administrador
b. Em caso de ausência de procedimentos pré-configurados, criar tais procedimentos e executá-los.

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

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

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

1.2.5.6.19. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

1.2.5.6.20. Deve possuir controle de dispositivos externo.

1.3. **Servidores Linux**

1.3.0.1. Compatibilidade:

1.3.0.1.1. Plataforma 64-bits:

- Red Hat Enterprise Linux 8 server;
- CentOS 7.2;
- Ubuntu 20.04 LTS;
- Debian GNU / Linux 10.1;
- Oracle Linux 8;
- SUSE® Linux Enterprise Server 15;
- Open SUSE® Leap 15;

1.3.0.2. Características:

1.3.0.2.1. Deve prover as seguintes proteções:

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

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

- Via linha de comando;
- Via console administrativa;
- Via GUI;
- Via web;

1.3.0.2.3. Deve possuir funcionalidade de Scan de drives removíveis, tais como:

- CDs;
- DVDs;
- Discos Blu-ray;
- Flash drives;
- HDs externos;
- Disquetes;

1.3.0.2.4. Deve fornecer os seguintes controles para dispositivos externos conectados ao computador:

- Por tipo de dispositivo;
- Por barramento de conexão.

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

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

1.3.0.2.7. Gerenciamento de Backup:

- Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar OU remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

1.3.0.2.8. Gerenciamento de Quarentena:

- Deve bloquear objetos suspeitos;
- Verificação por agendamento: procura de arquivos infectados e suspeitos(incluindo arquivos em escopos especificados);
- Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
- Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de

memória ou processamento;

- Capacidade de verificar objetos usando heurística;
- Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

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

- Alta;
- Média;
- Baixa;
- Recomendado;

1.3.0.3. Deve fornecer análise de todo o tráfego HTTP/HTTPS/FTP que chegar no computador do usuário.

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

- Detecção de Phishing e sites maliciosos;
- Bloqueio de download de arquivos maliciosos;
- Bloqueio de adware;

1.3.0.5. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux Deve possuir módulo de proteção contra criptografia maliciosa.

1.3.1. **Smart fones e Tablets**

1.3.1.1. O módulo de proteção de dispositivos móveis deve possuir agente para os seguintes sistemas operacionais:

- IOS e Android;

1.3.1.2. As funcionalidades estarão disponíveis de acordo com cada plataforma;

1.3.1.3. Deve permitir o provisionamento de configurações de:

- Wi-fi, Exchange Activesync, vpn, proxy http global e certificados;

1.3.1.4. Deve possuir proteção de anti-malware para Android;

1.3.1.5. Deve ser capaz de realizar escaneamento de malwares em tempo real, do cartão SD e após atualização de vacinas;

1.3.1.6. Possuir capacidade de detecção de spam proveniente de SMS;

1.3.1.7. Permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URL’s acessadas;

1.3.1.8. Permitir o controle de acesso a websites por meio de listas de bloqueio;

1.3.1.9. Possuir controle da política de segurança de senhas, com critérios mínimos de:

1.3.1.9.1. Padrão de senha;

1.3.1.9.2. Uso obrigatório de senha;

1.3.1.9.3. Tamanho mínimo;

1.3.1.9.4. Tempo de expiração;

1.3.1.9.5. Bloqueio automático da tela;

1.3.1.9.6. Bloqueio por tentativas inválida;

1.3.1.9.7. Controle de acesso à seguinte lista funções e status de ativação de funções dos dispositivos móveis:

- Bluetooth;
- Câmera;
- Cartões de memória;
- Wlan/wifi;
- Microsoft Activesync;
- MMS/SMS;
- Alto-falante;
- Armazenamento USB;

1.3.2. **Gerenciamento de Dispositivos Móveis (MDM) - Android**

1.3.2.1. Compatibilidade:

1.3.2.1.1. Dispositivos com os sistemas operacionais:

- Android 5.0 – 5.1.1
- Android 6.0 – 6.0.1
- Android 7.0 – 7.12
- Android 8.0, 9.0, 10.0;

1.3.2.1.2. Softwares de gerência de dispositivos:

- VMWare AirWatch 9.3;
- MobileIron 10.0;
- IBM Maas360 10.68;
- Microsoft Intune 1908;
- SOTI MobiControl 14.1.4 (1693);

1.3.2.2. Características:

1.3.2.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

1.3.2.2.2. Capacidade de ajustar as configurações de:

- Sincronização de e-mail;
- Uso de aplicativos;
- Senha do usuário;
- Criptografia de dados;

- Conexão de mídia removível;

1.3.2.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;

1.3.2.2.4. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;

1.3.2.2.5. Capacidade de desinstalar remotamente o antivírus do dispositivo;

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

1.3.2.2.7. Capacidade de sincronizar com Samsung Knox;

1.3.3. **Criptografia**

1.3.3.1. Compatibilidade:

- Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;
- Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;
- Microsoft Windows 7 Professional SP1 ou superior x86/x64;
- Microsoft Windows 8 Enterprise x86/x64;
- Microsoft Windows 8 Pro x86/x64;
- Microsoft Windows Pro x86/x64;
- Microsoft Windows Enterprise x86/x64;
- Microsoft Windows 10 Enterprise x86/x64;
- Microsoft Windows 10 Pro x86/x64;

1.3.3.2. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;

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

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

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

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

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

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

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

- Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
- Criptografar todos os arquivos individualmente;

- Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
- Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

1.3.3.10. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente;

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

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

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

1.3.3.14. Possibilita estabelecer parâmetros para a senha de criptografia;

1.3.3.15. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo

1.3.3.16. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

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

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

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

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

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

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

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

1.3.3.24. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pen drives, HD externo, etc;

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

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

1.3.3.27. Capacidade de fazer “Hardware encryption”;

1.3.4. **Módulo de Detecção e Resposta**

1.3.4.1. A solução deve ser compatível com os sistemas operacionais Windows.

1.3.4.2. O fabricante deve implementar e organizar os ataques

baseados no framework MITRE ATT&CK®, identificando técnicas e táticas dos ataques ou realizar o bloqueio que utilizem os mesmos procedimentos;

1.3.4.3. A solução deve possuir módulo de investigação e detecção integrados;

1.3.4.4. Deve fazer uso de inteligência artificial ou análise de comportamento do fabricante da solução para analisar e correlacionar as atividades maliciosas do ambiente;

1.3.4.5. Possuir painéis que apresentem visualização executiva dos principais eventos no ambiente com base nos usuários, aplicações acessadas e estações de trabalho;

1.3.4.6. Utilizar bases de inteligência de ameaças do fabricante para ajudar a identificar ameaças no ambiente;

1.3.4.7. Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;

1.3.4.8. Fornecer a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;

1.3.4.9. Capacidade de construir sequências de buscas poderosas ou indicadores de comprometimento para localizar os dados ou objetos em seu ambiente que você deseja examinar;

1.3.4.10. Permitir investigar os alertas gerados pelos modelos de detecção por meio de análise de impacto ou de causa-raiz;

1.3.4.11. O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados ou furtivos;

1.3.4.12. Os logs de detecções devem estar disponíveis na console por, pelo menos,30 dias;

1.3.4.13. A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;

1.3.4.14. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

1.3.4.15. Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta;

1.3.4.16. Deve permitir o envio de notificações para os administradores através de e-mail, API ou integrações com SIEMs;

1.3.4.17. Ao clicar em quaisquer dos objetos, a solução deve permitir realizar busca específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas;

1.3.4.18. Deve permitir terminar processos ativos executados nas estações de trabalhos e servidores;

1.3.4.19. Permitir coletar e fazer o download de um arquivo para investigação local detalhada;

1.3.4.20. Isolar a estação de trabalho desconectando-a da rede e permitindo se comunicar exclusivamente com a console de gerenciamento do fabricante;

1.3.4.21. Restaurar a conectividade da estação de trabalho com a rede;

1.3.4.22. Iniciar uma sessão de shell remoto na estação de trabalho selecionada para execução de comandos remotos para investigação;

1.3.4.23. Deve ser possível fazer o download do histórico da sessão após finalizar a sessão remota do shell na estação de trabalho para fins de auditoria.

1.3.5. **Criptografa de Disco**

1.3.5.1. Possuir a capacidade de realizar a criptografia nos seguintes sistemas operacionais:

- Windows 7 (x86/x64);
- Windows 10 (x86/x64);

1.3.5.2. Windows 10 (x86/x64Possuir módulo de criptografia para as estações de trabalho (desktops e notebooks), permitindo criptografia para:

- Disco completo (FDE – full disk encryption);
- Pastas e arquivos;
- Mídias removíveis;
- Anexos de e-mails ou Automática de disco;

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

1.3.5.4. Possuir a capacidade de exceções para criptografia automática;

1.3.5.5. Possuir compatibilidade de autenticação por múltiplos fatores;

1.3.5.6. Permitir atualizações do sistema operacional mesmo quando o disco está criptografado;

1.3.5.7. Possuir mecanismos para wipe (limpeza) remoto;

1.3.5.8. Possuir mecanismo que permita desfazer a criptografia do disco no evento em que se torne corrompido, impedindo a inicialização da estação/notebook;

1.3.5.9. Permitir, em nível de política, a indicação de pastas a serem criptografadas;

1.3.5.10. Permitir a escolha dos diretórios a serem criptografados em dispositivos de armazenamento USB;

2. SERVIÇOS:

2.1. Item 7 - Serviço de instalação, configuração e migração da solução atualmente em uso para a solução fornecida (Cod SIRP **000119806)**

2.1.1. Cada unidade aderida corresponde a uma instalação por licença.

2.1.2. A CONTRATADA deverá instalar a licença, suas funcionalidades, ajustes (tuning) e configurar o uso da solução proposta.

2.1.3. A CONTRATADA deverá ajustar a licença conforme exigências da equipe tecnica do órgão CONTRATANTE.

2.1.4. A equipe técnica do órgão deverá ter acesso direto às atualizações

de software, patches, documentação e ferramentas do fabricante.

2.2. **Item 8 - Treinamento/curso oficial do fabricante abrangendo todas as funcionalidades da solução (1 turma de 4 Analistas) (**Cod SIRP **000119814)** Capacitacao e Treinamento em Solucao de Endpoint

2.2.1. O treinamento será em apenas 1 (um) modulo;

2.2.2. Módulo Administrador: Turma única.

2.2.3. A definição da datas e horários em que ocorrerão os treinamentos serão acordados entre a CONTRATANTE e a CONTRATADA, sendo que deverão ocorrer obrigatoriamente em dias úteis, no horário comercial de 08:00 horas às 17:00 horas.

2.2.4. A carga horária diária não poderá ser inferior a 3 (três) horas e não poderá ultrapassar 6 (seis) horas.

2.2.5. A carga horária mínima de 18 horas de treinamento.

2.2.6. Estes limites somente poderão ser alterados em comum acordo e sem ônus adicional para a CONTRATANTE.

2.2.7. Os treinamentos deverão ser ministrados de forma remota, ou presencial, ao vivo, em turma fechada para a CONTRATANTE, utilizando ferramenta de vídeo conferência que permita a participação e interação dos participantes, sendo de responsabilidade dá CONTRATADA o fornecimento de toda a infraestrutura de videoconferência ou Webconferência necessária para o instrutor.

2.2.8. Seja remoto ou presencial, os custos com material, plataforma de treinamento, instrutor, hospedagem, alimentação, passagens e translado são de responsabilidade da CONTRATADA.

2.2.9. A CONTRATADA poderá realizar o treinamento de forma presencial, em comum acordo, desde que sem ônus adicional para a CONTRATANTE.

2.2.10. Todo treinamento será executado em idioma Português do Brasil.

2.2.11. A todo o material de treinamento utilizado pela CONTRATADA para a execução dos serviços de treinamento, incluindo material de apoio, como apresentações, apostilas, manuais, vídeos de demonstração, dentre outros correlatos, serão concedidos o direito de uso e de reprodução à CONTRATANTE, de forma irrestrita, para sua aplicação e uso em treinamentos internos para funcionários;

2.2.12. A CONTRATADA deverá fornecer o certificado de participação no curso, para todos os participantes.

2.2.13. Caso a avaliação seja classificada negativamente, a CONTRATANTE poderá requerer novo treinamento para aquela turma, sem custos. Além disso, caso a avaliação do instrutor seja negativa, a CONTRATANTE poderá solicitar que o treinamento seja ministrado por outro instrutor.

Anexo nº I (B) - Níveis de Serviços/SEPLAG/DCGSITIC/2023

PROCESSO Nº 1500.01.0113446/2022-67

1. NÍVEIS DE SERVIÇO

1.1. Suporte Técnico

1.1.1. A solução deverá estar disponível e acessível no regime 24x7x365 pelo suporte padrão do fabricante.

1.1.2. A disponibilidade mensal da solução deverá ser de, no mínimo, 99,8%.

1.1.3. A CONTRATADA oferecerá, dentro do período de contrato, os serviços de suporte técnico por meio de telefone e e-mail, em idioma Português do Brasil, durante o período do contrato pelo regime mínimo de 24x5x365.

1.1.4. O suporte técnico compreende o diagnóstico e identificação de problemas, apoio técnico na utilização, correção de erros, defeitos (bugs) ou mau funcionamento sobre qualquer funcionalidade, recurso, componente ou módulo disponível de forma nativa na solução, ou decorrente de qualquer adaptação (customização) e ajuste (tuning) efetuada pela CONTRATADA.

1.1.5. A CONTRATADA deverá disponibilizar os serviços de Suporte Técnico para manutenção, correção de erros, atualização de versão e releases, com compromisso de qualidade de atendimento.

1.1.6. O atendimento a um chamado de suporte técnico deverá ocorrer por qualquer uma das seguintes formas:

1. Atendimento presencial no local de instalação do software (on-site);
2. Acesso remoto;
3. Contato telefônico;
4. Envio de mensagem eletrônica (e-mail); ou
5. Acesso ao site web da CONTRATADA com controle de acesso por senha.

1.2. Níveis de Severidade

1.2.1. Para apuração do Índice de Disponibilidade e do Tempo de Atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a Tabela a seguir:

Severidade	Tempo de Atendimento	
	Tempo para o primeiro contato a partir da abertura do chamado	Tempo de Solução
1	1 hora útil	Até 2 horas úteis
2	1 hora útil	Até 4 horas

2	1 hora útil	úteis
3	4 horas úteis	Até 8 horas úteis
4	4 horas úteis	Até 12 horas úteis

1. **Severidade 01 (urgente**): Um problema catastrófico de produção que pode causar um impacto grave em seus sistemas de produção ou no qual seus sistemas de produção estão indisponíveis ou não estão funcionando. Os dados de produção estão perdidos e não há solução processual alternativa. Problemas de gravidade 01 também incluem problemas que resultam em condição de emergência que cause uma violação grave de segurança.
2. **Severidade 02 (alta)**: Um problema de alto impacto que interrompe sua operação, mas há capacidade de manter a produção e as operações necessárias ao nível do negócio. O nível de gravidade 02 também se aplica a situações menos graves de violação de segurança.
3. **Severidade 03 (média)**: Um problema com impacto de médio a baixo que envolve perda parcial, não crítica da funcionalidade. Um problema que impede algumas operações, mas que permite a continuação do funcionamento.
4. **Severidade 04 (baixa)**: Questões de uso geral, recomendações de futuras trocas de produto e chamadas com fins informativos. Não há impacto na qualidade, desempenho ou funcionalidade como resultado desses problemas.

1.2.2. Todos os chamados de suporte serão classificados em um nível de severidade, de acordo com o quadro a seguir:

Severidade	Escopo
1	Problema Grave – Paralização da operação
2	Problema Alto Impacto – interromper parcialmente a operação
3	Problema de Médio Impacto – Pode impedir alguma operação
4	Não é um problema e sim suporte para ajustes ou otimizações

1.3. **Cobertura**

1.3.1. No período de cobertura do contrato a CONTRATADA responderá,

no mínimo, 95% (noventa e cinco) dos chamados de severidade 1 e 2 dentro dos prazos mencionados, conforme definido no item de indicadores de qualidade, subitem 1.4.1 – Prazo de tempo de resposta.

1.3.1.1. A CONTRATANTE poderá obter informações sobre o andamento dos chamados através da central de atendimento da CONTRATADA

1.3.2. O descumprimento de qualquer um dos indicadores supracitados acarretará na aplicação de sanções administrativas, advertências, multas e suspensão, de acordo com a legislação em vigor.

1.3.3. Visando a efetividade da prestação dos serviços de suporte técnico e atualização de versão, a CONTRATADA deverá informar e manter atualizado o número de telefone e endereço de e-mail com atendimento 24x7x365, para o registro de chamados de suporte técnico.

1.3.4. A CONTRATADA também deverá manter, durante o período da vigência contratual o ambiente de produção com índice de disponibilidade de no mínimo 99% (noventa e cinco por cento), conforme definido no item de indicadores de qualidade, subitem 1.4.2 – Disponibilidade Mensal.

1.4. Indicadores de Qualidade

1.4.1. Prazo de Tempo de Resposta

ICSPP – Índice de Chamados Solucionados no Prazo Previsto	
Atributo	**Valor**
Descrição	Percentual dos chamados técnicos solucionados, nível de severidade 1 e 2, pela CONTRATADA, no prazo máximo previsto, em relação a todos os chamados técnicos efetuados durante o período de apuração.
Objetivo	Reduzir os atrasos na resolução de problemas, defeitos e no esclarecimento de dúvidas e questionamentos técnicos pela CONTRATADA.
Meta	Maior ou igual a 80%
Periodicidade	Mensal
Unidade de Representação	Valor percentual
Forma de Cálculo	**ICSPP = (TCP / TC) x 100**, **Onde:** TCP = Total de chamados de nível de severidade 1 e 2, solucionados dentro do prazo máximo definido neste Termo de Referência, durante o período de apuração. TC = Total de chamados com nível de severidade 1 e 2, solucionados durante o período de apuração.
Gestão do indicador (Coleta, Medição e Acompanhamento)	Conforme detalhado no item “**Gestão dos Níveis de Serviço”** deste anexo.
Proporcionalização do Pagamento	Meta não atingida implicará em desconto no valor do pagamento mensal, pela CONTRATANTE, dos valores mensais devidos ou da garantia contratual especificada neste Termo de Referência, caso o serviço correspondente tenha sido, de alguma forma, quitado pela CONTRATANTE antecipadamente. Considera-se a seguinte tabela para o cálculo do desconto referente a este indicador de qualidade:

	• Sem desconto, se 80% ≤ ICSSP ≤ 100% • Desconto de 5%, se 70% ≤ ICSSP < 80% • Desconto de 10%, se 60% ≤ ICSPP < 70% • Desconto de 20%, se ICSPP < 60%

1.4.2. Disponibilidade mensal:

DispH - Índice de disponibilidade mensal dos serviços ofertados	
Atributo	**Valor**
Descrição	Percentual de disponibilidade mensal dos serviços ofertados, pela CONTRATADA, durante o período de apuração.
Objetivo	Mensurar o nível de disponibilidade mensal dos serviços ofertados.
Meta	Maior ou igual a 95%
Periodicidade	Mensal
Unidade de Representação	Valor percentual
Forma de cálculo	DispH = ((Tdisp - Sdown) / Tdisp) * 100 Onde**:** DispH = Disponibilidade do serviço, medida em %. Tdisp = Tempo acordado para funcionamento da solução em horas, referente ao mês de medição (24 horas / dia). Sdown = Somatório dos tempos de falha (*downtime*), em horas. O tempo acordado para funcionamento (Tdisp), em horas, será calculado multiplicando o número de horas pela quantidade de dias no mês de apuração. Cada tempo de falha (*downtime*)

	será calculado considerando a data e hora de registro do chamado e de seu contingenciamento ou finalização. O somatório dos tempos de falha (Sdown) será dado pela soma de todos os tempos de falha ocorridos no mês de medição, sejam eles concluídos ou em estando ainda em aberto. Importante ressaltar que no cálculo da variável "Sdown" serão consideradas as regras definidas nos itens 1.4.1 e 1.4.2 deste termo de referência.
Gestão do Indicador (Coleta, Medição e companhamento)	Conforme detalhado no item "**Gestão dos Níveis de Serviço"** deste anexo.
Sanções Previstas	Meta não atingida implicará em desconto no valor do pagamento mensal, pela CONTRATANTE, dos valores mensais devidos ou da garantia contratual especificada neste Termo de Referência, caso o serviço correspondente tenha sido, de alguma forma, quitado pela CONTRATANTE antecipadamente. Considera-se a seguinte tabela para o cálculo do desconto referente a este indicador de

	qualidade: • Sem desconto, se 95% ≤ ICSSP ≤ 100% • Desconto de 5%, se 90% ≤ ICSSP < 95% • Desconto de 10%, se 85 ≤ ICSPP < 90% • Desconto de 10%, se 80 ≤ ICSPP < 85% • Desconto de 20%, se ICSPP < 80%

1.4.3. A soma dos descontos em função das sanções, referentes aos indicadores supracitados, não poderá ser maior que 20% dos valores mensais devidos ou da garantia contratual especificada neste Termo de Referência, caso o serviço correspondente tenha sido, de alguma forma, quitado pela CONTRATANTE antecipadamente.

1.4.4. Em caso de meta não atingida por 2 meses seguidos, sem uma justificativa plausível, a CONTRATANTE poderá abrir processo punitivo contra a CONTRATADA, conforme seu Regulamento Interno de Contratos e Licitações - RILC.

1.4.5. Em caso de adoção de solução de contingência, sem prejuízo da solução definitiva cabível, a CONTRATADA deve emitir laudos, na periodicidade exigida pela CONTRATANTE, informando sobre a evolução dos trabalhos para solucionar o problema de forma definitiva.

1.4.5.1. O chamado deverá continuar aberto, com status de contingenciado, até sua solução definitiva, que poderá vir com correções de código, nova release ou atualização de versão.

1.4.6. Paradas planejadas para manutenção da Solução não serão consideradas severidades.

1.4.6.1. Paradas planejadas são manutenções previamente agendadas, através de comunicação formal entre a CONTRATANTE e a CONTRATADA, para manutenções na solução. Estas paralisações devem ser solicitadas com um mínimo de 10 (dez) dias corridos de antecedência, ou de comum acordo entre as partes.

1.4.6.2. Somente serão consideradas como severidades se excederem os prazos pactuados para a manutenção e a responsabilidade por esta falha for comprovadamente da CONTRATADA.

1.5. **Gestão dos Níveis de Serviço:**

1.5.1. Pelo menos um dos seguintes mecanismos deve ser disponibilizado pela CONTRATADA para abertura (Registro) de chamados: telefone, mensagem eletrônica (e-mail), sítio na Internet.

1.5.2. No caso de ligações telefônicas, o número para contato para a abertura/ registro de CHAMADOS deverá ser de ligação nacional, com idioma português e único para todos os módulos, componentes e funcionalidades da solução.

1.5.3. Na abertura (Registro) dos chamados, o Órgão/Entidade irá comunicar, via mensagem eletrônica (e-mail), à CONTRATADA as seguintes informações:

- Data e hora de abertura do chamado.
- Código alfanumérico de identificação do chamado.
- Descrição do chamado.
- Nível de Severidade do chamado.
- Identificação (nome completo e matrícula) do solicitante do Órgão/Entidade.
- Identificação do atendente da CONTRATADA.

1.5.4. Caso o chamado tenha sido aberto via ligação telefônica, a CONTRATADA deverá confirmar, via mensagem eletrônica (e-mail), a abertura (registro) do chamado, incluindo as seguintes informações:

- Código alfanumérico de identificação do chamado.
- Data e hora de início do Atendimento.
- Descrição do serviço a executar.
- Identificação do responsável pelo serviço a executar.
- Data prevista para execução do serviço.

1.5.5. O Contingenciamento do chamado será confirmado através do aceite pelo Órgão/Entidade na ordem de serviço (OS) correspondente, desde que incluso as seguintes informações:

- Código alfanumérico de identificação do chamado.
- Data e hora de conclusão do contingenciamento.
- Descrição detalhada do serviço executado.

1.5.6. A conclusão definitiva do CHAMADO será confirmada através do aceite pelo Órgão/Entidade na ordem de serviço (OS) correspondente, desde que incluso as seguintes informações:

- Código alfanumérico de identificação do chamado.
- Data e hora de conclusão do serviço executado.
- Descrição detalhada do serviço executado.

eletrônica julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **63149171** e o código CRC **6397D265**.

Referência: Processo nº 1500.01.0113446/2022-67 SEI nº 63149171