AVISO

PREGÃO ELETRÔNICO nº 044/2020 - SEPLAG.
PROCESSO nº 01440/2020

Acha-se aberta, na Secretaria de Administração e Recursos Humanos/Comissão Permanente de Licitação, situada à Av. Brasil, 2001/6º andar, nesta cidade de Juiz de Fora – MG, LICITAÇÃO NA MODALIDADE DE **PREGÃO**, na forma **ELETRÔNICA**, tipo **MENOR PREÇO**, pelo **modo de disputa aberto**, com a finalidade de selecionar propostas objetivando **o fornecimento de Solução de Segurança da Informação, composta por software antivírus Kaspersky Advanced Security for Business com licenças de uso para 24 (vinte e quatro) meses e suporte da CONTRATADA, incluindo, ativação, configuração, gerenciamento centralizado, garantia de atualização contínua e suporte técnico,** cujas especificações detalhadas encontram-se nos Anexos que acompanham o Edital.

Regem a presente licitação, a Lei Federal nº 8.666/93, observadas as alterações posteriores, a Lei Federal nº 10.520/02, Lei Complementar nº 123/2006, com as alterações promovidas pela Lei Complementar nº 147/2014, Lei Municipal nº 10.214/2002, Lei Municipal nº 12.211/2011, Lei Municipal nº Lei nº 13.830/2019, Decreto Municipal nº 13.892/2020, Decreto Municipal nº 13.602/2019 e demais legislações aplicáveis.

Serão observados os seguintes horários e datas para os procedimentos que seguem:

Recebimento das Propostas e Documentos de Habilitação: **das 11:00h do dia 18/05/2020, às 08:30h do dia 28/05/2020**;

Início da Sessão de Disputa de Preços: **às 09:00h do dia 28/05/2020**, no endereço eletrônico ***https://www.portaldecompraspublicas.com.br***, horário de Brasília - DF.

Poderão participar da licitação pessoas jurídicas que atuam no ramo pertinente ao objeto licitado, observadas as condições constantes do edital.

O **Edital Completo** poderá ser obtido pelos interessados na SARH/CPL, em arquivo digital, mediante entrega de um pen-drive, de segunda a sexta-feira, no horário de 08:30 às 11:30 e de 14:30 às 17:30 horas ou pelo endereço eletrônico http://www.pjf.mg.gov.br. É necessário que, ao fazer download do Edital, seja informado, via e-mail - pregaoeletronico@pjf.mg.gov.br, a retirada do mesmo, para que possam ser comunicadas possíveis alterações que se fizerem necessárias. A subsecretaria não se responsabilizará pela falta de informações relativas ao procedimento àqueles interessados que não confirmarem, pelos meios expostos, a retirada do Edital. Quaisquer dúvidas contatar pelo telefone (32) 3690-8188/8187/8492.

Comissão Permanente de Licitação

EDITAL

PREGÃO ELETRÔNICO nº 044/2020 - SEPLAG
PROCESSO nº 01440/2020

Acha-se aberta, na Secretaria de Administração e Recursos Humanos/Comissão Permanente de Licitação, situada à Av. Brasil, 2001/6º andar, nesta cidade de Juiz de Fora – MG, LICITAÇÃO NA MODALIDADE DE **PREGÃO**, na forma **ELETRÔNICA**, tipo **MENOR PREÇO**, pelo modo de disputa aberto, cujas especificações detalhadas encontram-se nos Anexos que acompanham o Edital.

Regem a presente licitação, a Lei Federal nº 8.666/93, observadas as alterações posteriores, a Lei Federal nº 10.520/02, Lei Complementar nº 123/2006, com as alterações promovidas pela Lei Complementar nº 147/2014, Lei Municipal nº 10.214/2002, Lei Municipal nº 12.211/2011, Lei Municipal nº Lei nº 13.830/2019, Decreto Municipal nº 13.892/2020, Decreto Municipal nº 13.602/2019 e demais legislações aplicáveis.

I – DO OBJETO

1.1. Constitui objeto do presente Edital a seleção de sociedade empresária objetivando o **fornecimento de Solução de Segurança da Informação, composta por software antivírus Kaspersky Advanced Security for Business com licenças de uso para 24 (vinte e quatro) meses e suporte da CONTRATADA, incluindo, ativação, configuração, gerenciamento centralizado, garantia de atualização contínua e suporte técnico**, conforme condições descritas nos Anexos deste Edital.

1.1.1. Descrição do Objeto e Quantidades

Item	Descrição	Período	Quantidade
01	Renovação de licença de servidor	24 meses	01
02	Renovação de licença de uso de software antivírus corporativo	24 meses	2.700
03	Contratação de serviço de suporte técnico	24 meses	01

1.2. A empresa **CONTRATADA** deverá ser responsável pelo fornecimento das novas licenças e pela devida prestação do suporte técnico contratado.

1.3. O processo deve incluir ajustes no ambiente que forem identificados e considerados necessários.

1.4. Integra este Edital, como se nele estivesse transcrito os itens elencados abaixo do Termo de Referência - **Anexo I**, assim como todas as especificações neste contidas:

a) Item 6 - Características Gerais do Software;
b) Item 7 - Smartphones e tablets;
c) Item 8 - Gerenciamento de dispositivos móveis (MDM);
d) Item 9 - Criptografia, e;
e) Item 10 - Gerenciamento de Sistemas.

II - DOS RECURSOS ORÇAMENTÁRIOS

2.1. O valor proposto para as licenças do software antivírus corporativo, incluindo, ativação, configuração, gerenciamento centralizado, garantia de atualização contínua e suporte técnico, pelo período de no mínimo 24 (vinte e quatro) meses, partirá da fonte **0100600000** de natureza **nº 3.3.90.40.36** cuja dotação é **04.126.0001.1051.0000**.

III - DO CREDENCIAMENTO

3.1. O fornecedor deverá fazer sua adesão ao Portal de Compras Públicas, acessando o seguinte endereço: *https://www.portaldecompraspublicas.com.br*, onde qualquer pessoa física ou jurídica, que manifeste interesse e apresente a documentação e condições exigidas terá acesso ao Portal.

3.1.1. O credenciamento dar-se-á pela atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao sistema eletrônico.

3.1.2. O credenciamento da proponente junto ao provedor do sistema implica na responsabilidade legal da proponente ou de seu representante legal, bem como na presunção de sua capacidade técnica para a realização das transações inerentes ao pregão eletrônico.

3.2. A Administradora do Pregão Eletrônico conjuntamente com a CPL darão sequência ao processo de Pregão.

IV - DAS CONDIÇÕES DE PARTICIPAÇÃO

4.1. É vedada a participação de interessados:

4.1.1. que tenham sido declarados inidôneos ou punidos com suspensão do direito para licitar ou contratar com a Administração Pública;

4.1.2. que se encontrarem em débito para com a Fazenda do Município de Juiz de Fora-MG, nos termos do art. 41 do Código Tributário Municipal (Lei nº 5546/1978);

4.1.3. que não atendam às condições deste Edital e seu(s) anexo(s);

4.1.4. estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

4.1.5. que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666, de 1993;

4.1.6. que estejam sob falência, concurso de credores, concordata ou em processo de dissolução ou liquidação;

4.1.7. que estejam reunidas em consórcio;

***Nota Explicativa**: O presente edital não prevê as condições de participação de empresas reunidas em consórcio, vez que a experiência prática demonstra que as licitações que permitem essa participação são aquelas que envolvem serviços de grande vulto e/ou de alta complexidade técnica. Como o presente Edital foi elaborado com foco no dia a dia da Administração, consignou-se a vedação acima.*
Note-se que "...a aceitação de consórcios na disputa licitatória situa-se no âmbito do poder discricionário da administração contratante, conforme art. 33, caput, da Lei n. 8.666/1993, requerendo-se, porém, que sua opção seja sempre previamente justificada no respectivo processo administrativo, conforme entendimento dos Acórdãos de ns. 1.636/2006-P e 566/2006-P" - TCU Ac n. 2869/2012-Plenário (Item 1.7.1).
Em todo caso, a Administração deverá fundamentar qualquer opção adotada, vez que "...a vedação de empresas em consórcio, sem que haja justificativa razoável..." pode ser considerada restrição à competitividade do certame (TCU, Ac n. 963/2011-2ª Câmara, Item 9.2.1).

V - DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

5.1. 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.

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

5.3. 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 LC nº 123, de 2006.

5.4. 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.

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

5.6. 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.

5.7. 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.

VI - DO PREENCHIMENTO DA PROPOSTA

6.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

6.1.1. Valor unitário e total do item;

6.1.2. Marca, quando for o caso;

6.1.3. Descrição detalhada do objeto, contendo as informações especificadas no Termo de Referência: indicando, no que for aplicável, o modelo, prazo de validade ou de garantia, número do registro ou inscrição do bem no órgão competente, quando for o caso;

6.1.4. E-mail para fins de comunicação com o proponente.

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

6.2.1. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos bens.

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

6.2.3. O prazo de validade da proposta deverá ser de, no mínimo, **90 (noventa) dias corridos.**

6.2.4. Os preços unitários ofertados pelos proponentes não poderão ser superiores aos preços unitários levantados pela Prefeitura de Juiz de Fora.

VII – DA HABILITAÇÃO

7.1. Não serão aceitos protocolos, nem documentos com prazo de validade vencido.

7.1.1. Todos os documentos exigidos para habilitação deverão estar no prazo de validade. Caso o órgão emissor não declare a validade do documento, esta será de 60 (sessenta) dias corridos contados a partir da data de emissão, exceto o comprovante de inscrição no CNPJ e Atestado (s) de Capacidade Técnica.

7.2. Documentos que deverão ser apresentados relativos à habilitação jurídica:

7.2.1. Ato constitutivo, estatuto social em vigor, devidamente registrado, em se tratando de sociedades comerciais e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;

7.2.2. Cédula de Identidade e registro comercial, no caso de firma individual;

7.2.3. Decreto de autorização, em se tratando de sociedade empresária ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir;

7.2.4. Declaração de que a proponente não incorre em qualquer das condições impeditivas, especificando, conforme **Anexo VI**:

7.2.4.1. Que não foi declarada inidônea por ato do Poder Público;

7.2.4.2. Que não está impedido de transacionar com a Administração Pública;

7.2.4.3. Que não foi apenada com rescisão de contrato, quer por deficiência dos serviços prestados, quer por outro motivo igualmente grave, no transcorrer dos últimos 5 (cinco) anos;

7.2.4.4. Que não incorre nas demais condições impeditivas previstas no art. 9º da Lei Federal nº 8.666/93 consolidada pela Lei Federal nº 8.883/94.

7.2.4.5. E que, se responsabiliza pela veracidade e autenticidade dos documentos oferecidos, comprometendo-se a comunicar a PREFEITURA MUNICIPAL DE JUIZ DE FORA a ocorrência de quaisquer fatos supervenientes impeditivos da habilitação, ou que comprometam a idoneidade da proponente, nos termos do artigo 32, parágrafo 2º, e do artigo 97 da Lei 8.666/93, e suas alterações.

7.2.5. Declaração de atendimento à norma do inciso XXXIII do artigo 7º da Constituição Federal, com redação dada pela emenda constitucional nº 20/98, que proíbe trabalho noturno, perigoso ou insalubre aos menores de 18 anos e de qualquer trabalho a menores de 16 anos salvo na condição de aprendiz a partir de 14 anos, conforme **Anexo V**.

7.2.6. Declaração expressa de que o proponente preenche plenamente os requisitos de habilitação, bem como tem pleno conhecimento do objeto licitado e anuência das exigências constantes do Edital e seus anexos, conforme **Anexo IV**.

7.2.7. A proponente, microempresa ou empresa de pequeno porte, deverá apresentar declaração, sob as penas da lei, de que cumprem os requisitos legais para a qualificação como microempresas ou empresa de pequeno porte, estando aptas a usufruir do tratamento estabelecido na Lei Complementara nº 123/06, conforme **Anexo III**.

7.2.8. A proponente, microempresa ou empresa de pequeno porte, deverá apresentar declaração de que a empresa não incorre em nenhuma das hipóteses previstas no § 4º, do artigo 3º, da Lei Complementar nº 123/06, conforme **Anexo III**.

7.3. Documentos que deverão ser apresentados relativos à Regularidade Fiscal e Trabalhista:

7.3.1. Comprovante de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);

7.3.2. Prova de regularidade para com a Fazenda Federal e a Seguridade Social, mediante apresentação de

Certidão Conjunta de Débitos Relativos a Tributos Federais e à Dívida Ativa da União, emitida pela Secretaria da Receita Federal do Brasil e Procuradoria Geral da Fazenda Nacional.

7.3.3. Prova de regularidade para com a Fazenda Estadual;

7.3.4. Prova de regularidade para com a Fazenda Municipal;

7.3.4.1. Nos Municípios em que não há emissão de Certidão Municipal Conjunta, o licitante deverá, obrigatoriamente, apresentar tanto a certidão negativa de tributos mobiliários quanto a de tributos imobiliários.

7.3.4.2. Para os fins do art. 41 do Código Tributário Municipal, a habilitação dos proponentes não sediados no Município de Juiz de Fora/MG, ficará condicionada à verificação da regularidade fiscal perante este Município.

7.3.4.2.1. Nos termos da subcláusula anterior, o proponente, se desejar, poderá apresentar junto de sua documentação de habilitação, a Certidão Negativa de Débito Ampla expedida pela Prefeitura de Juiz de Fora/MG.

7.3.5. Prova de Regularidade de Situação (CRF) perante o Fundo de Garantia por Tempo de Serviço – FGTS;

7.3.6. Prova de inexistência de débitos inadimplidos perante a justiça do trabalho, mediante a apresentação de certidão negativa, nos termos do Título VII - Da consolidação das leis do trabalho, aprovada pelo Decreto – Lei 5.452, de 1º de maio de 1943.

7.3.7. A proponente, microempresa ou empresa de pequeno porte, deverá apresentar toda a documentação exigida para efeito de comprovação da regularidade fiscal, mesmo que esta apresente alguma restrição;

7.3.7.1. Havendo alguma restrição na comprovação da regularidade fiscal, será assegurado o prazo de 5 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que o proponente (ME ou EPP) for declarado o vencedor do certame, prorrogáveis por igual período, a critério da Administração, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de negativa.

7.3.7.2. A não–regularização da documentação no prazo previsto no subitem anterior implicará decadência do direito à contratação, sem prejuízo das sanções previstas no artigo 81, da Lei nº 8.666/93, sendo facultado à Administração convocar os licitantes remanescentes, na ordem de classificação, para a retirada da Nota de Empenho, ou revogar a licitação.

7.4. Documentos que deverão ser apresentados relativos à Qualificação Econômico-Financeira:

7.4.1. Balanço Patrimonial e demonstrações contábeis do último exercício, já exigíveis e apresentados na forma da Lei Federal nº 6.404/76 e Lei Federal nº 10.406/2002, que comprovem a boa situação financeira da sociedade empresária, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados monetariamente, quando encerrados há mais de três meses da data de apresentação da proposta, tomando como base a variação, ocorrida no período, do Índice de Preços ao Consumidor Amplo - IPCA ou outro indicador que o venha substituir.

7.4.1.1. Se necessária a atualização monetária do Balanço Patrimonial, deverá ser apresentado, juntamente com os documentos em apreço, o memorial de cálculo correspondente, assinado pelo Contador.

7.4.1.2. As sociedades empresárias com menos de um exercício financeiro devem cumprir a exigência deste item mediante apresentação de Balanço de Abertura ou do último Balanço Patrimonial levantado, conforme o caso.

7.4.1.3. Serão considerados aceitos como na forma da lei o Balanço Patrimonial (inclusive o de abertura) e demonstrações contábeis assim apresentados:
a) publicados em Diário Oficial; ou
b) publicados em Jornal; ou
c) por cópia ou fotocópia registrada ou autenticada na Junta Comercial da sede ou domicílio da proponente; ou
d) por cópia ou fotocópia do livro Diário, devidamente autenticado na Junta Comercial da sede ou domicílio da proponente ou em outro órgão equivalente, inclusive com os Termos de Abertura e de Encerramento, ou;
e) Por Escrituração Contábil Digital (ECD), através da apresentação de cópia do SPED, devidamente transmitido via eletrônica, e obrigatoriamente, observado o prazo de entrega estipulado no art. 1078 da Lei Federal nº 10.406/2002.

7.4.1.4. Os documentos relativos ao subitem **7.4.1** deverão ser apresentados contendo assinatura do representante legal da sociedade empresária proponente e do seu contador, ou, mediante publicação no Órgão de Imprensa Oficial, devendo, neste caso, permitir a identificação do veículo e a data de sua publicação. A indicação do nome do contador e do número do seu registro no Conselho Regional de Contabilidade – CRC – são indispensáveis.

7.4.2. A capacidade Financeira da Sociedade Empresária será avaliada mediante os seguintes indicadores:

Liquidez Corrente (LC) expressado da forma seguinte:

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

Para a capacidade econômico-financeira exigida, os participantes deverão atender obrigatoriamente, os seguintes requisitos:

LC ..... maior ou igual a 1(um)

7.4.2.1. O item **7.4.2** é somente considerado para fins de Qualificação Econômico-Financeira da proponente. Uma vez habilitada, a maior ou menor pontuação obtida pela concorrente não terá qualquer influência na sua classificação final.

7.4.3. Certidão Cível Negativa, abrangendo Falência e Recuperação Judicial ou Extrajudicial, expedida por distribuidor da sede do principal estabelecimento da pessoa jurídica na forma do que prescreve o artigo 3º, da Lei nº 11.101/05.

7.4.3.1. Caso a Certidão evidencie a existência de processo de recuperação judicial, a mesma deverá vir acompanhada de documento expedido pelo Poder Judiciário de que a interessada está autorizada a participar de procedimento licitatório.

7.4.3.2. Nas comarcas em que a Certidão emitida pelo cartório distribuidor não abranger os processos distribuídos no processo judicial eletrônico - PJE, o licitante deverá, obrigatoriamente, apresentar tanto a certidão expedida pelo cartório distribuidor, quanto a certidão específica para processos judiciais eletrônicos.

7.4.4. No caso da empresa apresentar índice contábil de Liquidez Corrente menor que 1(um), porém positivo, é exigida obrigatoriamente a comprovação de possuir Capital Social de no mínimo 10% (dez inteiros por cento) do valor estimado da Contratação, exigência esta prevista nos parágrafos 2° e 3°, do art. 31 da Lei nº 8.666/93, e devendo a comprovação ser feita relativamente à data da apresentação da proposta, e/ou através da apresentação do balanço Patrimonial do último exercício social, já exigível e apresentado na forma da Lei Federal n° 6.404/76 e Lei Federal n° 10.406/2002.

7.5. **Documentos que deverão ser apresentados relativos à qualificação técnica:**

7.5.1. Comprovação de aptidão para desempenho de atividade pertinente e compatível com o objeto da licitação através da apresentação de pelo menos 1 (um) atestado de capacidade técnica, emitido por pessoa jurídica de direito publico ou privado, que comprove a aptidão para desempenho a contento de objeto semelhante.

7.5.2. A proponente deverá comprovar que é fornecedor autorizada da solução antivírus fornecida, por meio de declaração emitida pelo fabricante do software antivírus.

7.5.3. A proponente deverá comprovar que possui pelo menos 02 (dois) profissionais certificados na solução pelo FABRICANTE, para prestação dos serviços de configuração necessários.

7.5.3.1. A comprovação de vínculo do profissional com o licitante poderá ser feita mediante a apresentação de um dos seguintes documentos:

7.5.3.1.1. Carteira de trabalho e previdência social (CTPS) do responsável técnico;
7.5.3.1.2. Contrato social da licitante, do qual conste o responsável técnico como integrante da sociedade;
7.5.3.1.3. Contrato de prestação de serviços;
7.5.3.1.4. Declaração de contratação futura do responsável técnico detentor do atestado apresentado, desde que acompanhada da anuência deste.

7.6. Não tendo a sociedade empresária classificada como vencedora do certame apresentado a documentação exigida, no todo ou em parte, será esta desclassificada, podendo a ela ser aplicada as penalidades previstas na legislação que rege o procedimento, e será convocada então a sociedade empresária seguinte na ordem de classificação.

7.7. A documentação, na fase pertinente, será rubricada pelo Pregoeiro e pela Equipe de Apoio e após examinada será anexada ao processo desta licitação, sendo inabilitados aqueles proponentes cuja documentação apresente irregularidades.

7.8. A documentação exigida para atender ao disposto nos itens 7.2.1, 7.2.2, 7.2.3, 7.3 e 7.4.1, poderá ser substituída, conforme disposto no parágrafo 3º do Art. 32 da Lei nº 8.666/93, pelo Certificado de Cadastro Geral de Licitantes do Município de Juiz de Fora - CAGEL, com validade plena; conforme Decreto 7.654 de 06 de dezembro de 2002; com ramo de atividade compatível com o objeto licitado.

7.9. Todos os documentos apresentados para habilitação deverão estar em nome do licitante, com o número do CNPJ e, preferencialmente, com endereço respectivo, devendo ser observado o seguinte (condição válida, também, para pagamento dos serviços, se for o caso):

7.9.1. se o licitante for a matriz, todos os documentos deverão ser apresentados em seu nome e de acordo com seu CNPJ, ou;

7.9.2. se o licitante for a filial, todos os documentos deverão ser apresentados em seu nome e de acordo com o número do CNPJ da filial, exceto quanto à certidão Negativa de Débito junto ao INSS, por constar no próprio documento que é válido para matriz e filiais, Certidão de Débito relativo aos Tributos Federais e à Dívida Ativa da União e CNDT;

7.9.3. se o licitante for a matriz e o fornecedor do bem ou prestadora dos serviços for a filial, os documentos deverão ser apresentados com o número de CNPJ da matriz e da filial, simultaneamente;

7.9.4. serão dispensados da apresentação de documentos com o número do CNPJ da filial aqueles documentos que, pela própria natureza, forem emitidos somente em nome da matriz;

7.9.5. o não atendimento de qualquer exigência ou condição deste, item, implicará na inabilitação do licitante.

7.10. Constatado o atendimento às exigências de habilitação fixadas no Edital, o licitante será declarado vencedor.

VIII - DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

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

8.2. O Pregoeiro verificará as propostas apresentadas, 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.

8.2.1. Também será desclassificada a proposta que identifique o licitante.

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

8.2.3. A não desclassificação da proposta não impede o seu julgamento definitivo na fase de aceitação.

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

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

8.5. 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.

8.5.1. O julgamento das propostas será feito pelo **MENOR VALOR GLOBAL** de acordo com o especificado no **Anexo I.**

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

8.7. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

8.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser fixado pelo pregoeiro.

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

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

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

8.12. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente.

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

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

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

8.16. 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.

8.17. 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.

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

8.19. 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.

8.20. 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.

8.21. 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.

8.22. 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.

8.23. 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 bens produzidos:
8.23.1. no país;
8.23.2. por empresas brasileiras;
8.23.3. por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;
8.23.4. 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.

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

8.25. O Pregoeiro poderá encaminhar, por meio do sistema eletrônico, contraproposta ao licitante que apresentou o lance mais vantajoso, com o fim de negociar a obtenção de melhor preço, vedada a negociação em condições diversas das previstas neste Edital.
8.25.1. 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.
8.25.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.
8.25.3. Nos itens não exclusivos para a participação de microempresas e empresas de pequeno porte, sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.

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

IX - DA ACEITABILIDADE DA PROPOSTA VENCEDORA

9.1. 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 máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no § 10 do art. 25 do Decreto Municipal nº 13.892/2020.

9.2. Será desclassificada a proposta ou o lance vencedor que apresentar preço final superior ao preço máximo fixado no Edital, desconto menor do que o mínimo exigido ou que apresentar preço manifestamente inexequível.

9.2.1. 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.

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

9.4. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no "*chat*" a nova data e horário para a sua continuidade.

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

X – DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

10.1. A proposta final do licitante declarado vencedor deverá ser encaminhada no prazo mínimo de **2 (duas) horas**, a contar da solicitação do Pregoeiro no sistema eletrônico e deverá:

10.1.1. ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo proponente.

10.1.2. conter a indicação do banco, número da conta e agência do licitante vencedor, para fins de pagamento.

10.2. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.

10.2.1. Todas as especificações do objeto contidas na proposta, tais como marca, modelo, tipo, fabricante e procedência, vinculam a Contratada.

10.3. Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso (art. 5º da Lei nº 8.666/93).

10.3.1. Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.

10.4. A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação.

10.5. A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante.

10.6. As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na internet, após a homologação.

XI – DO RECURSO

11.1. 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, o Pregoeiro fixará o prazo 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, **exclusivamente em campo próprio do sistema**.

11.2. 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.

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

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

11.2.3. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de três dias 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, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

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

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

XII – DA REABERTURA DA SESSÃO PÚBLICA

12.1. A sessão pública poderá ser reaberta:

12.1.1. 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.

12.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

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

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

XIII - DA HOMOLOGAÇÃO, ADJUDICAÇÃO E ASSINATURA DO CONTRATO

13.1. Após a declaração do vencedor da licitação, não havendo manifestação dos proponentes quanto à interposição de recurso, o Pregoeiro opinará pela adjudicação do objeto licitado, o que posteriormente será submetido à autoridade competente.

13.1.1. A autoridade competente homologará o resultado da licitação ao vencedor do certame.

13.2. Homologado o resultado da licitação, a Administração deverá encaminhar ao adjudicatário o contrato, por intermédio do e-mail informado em sua proposta, para que, no prazo de 10 (dez) dias consecutivos, contados a partir da data desta convocação, seja o referido instrumento assinado e devolvido via postal, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital. Se assim houver interesse, poderá o adjudicatário comparecer pessoalmente junto a Unidade Gestora demandante do contrato para assinatura.

13.2.1. A Administração não se responsabilizará pelo não recebimento do contrato encaminhado para o e-mail informado na proposta, devendo o proponente mantê-lo em condições de receber as mensagens que lhe forem encaminhadas relativas ao presente certame. Em caso de fato superveniente que venha a inviabilizar o recebimento de e-mails, deverá o proponente, em tempo hábil, comunicar a Administração.

13.3. A Administração poderá, quando o proponente vencedor, convocado dentro do prazo de validade de sua proposta, não apresentar situação regular ou se recusar injustificadamente a assinar o contrato, retomar a Sessão Pública e convidar os demais proponentes classificados, seguindo a ordem de classificação, ou revogar a licitação independentemente da cominação do Art. 81 da Lei Federal nº 8.666/93.

XIV - DO CONTRATO

14.1. O contrato formalizado regular-se-á, no que concerne a sua alteração, inexecução ou rescisão, pelas disposições da Lei nº 8.666, de 21 de junho de 1.993 observadas suas alterações posteriores, pelas disposições do Edital e pelos preceitos do direito público.

14.2. O contrato poderá, com base nos preceitos de direito público, ser rescindido pela autoridade gestora da despesa a todo e qualquer tempo, independentemente de interpelação judicial ou extrajudicial, mediante simples aviso, observadas as disposições legais pertinentes.

14.3. Farão parte integrante do contrato as condições previstas no Edital e na proposta apresentada pelo adjudicatário.

14.4. O contrato terá vigência de 24 (vinte e quatro) meses a partir da data de assinatura.

14.5. Ao final do período acima estipulado, poderá ser prorrogado por iguais e sucessivos períodos, através de Termo Aditivo, desde que não haja manifestação por escrito em contrário, por quaisquer das partes, no prazo de até 30 (trinta) dias antes de cada término de contrato/aditivo, ficando estabelecido que sua rescisão desobrigará as partes dos compromissos pactuados no aludido contrato.

14.6. Do reajuste do contrato:

14.6.1. O contrato poderá ter o seu valor reajustado, desde que seja observado o interregno mínimo de 01(um) ano, a contar da data da proposta, ou da data do orçamento a que a proposta se referir, conforme disposto no Decreto Municipal nº 8.542, de 09 de maio de 2005.

14.6.2. Para o reajuste do contrato será adotado como indicador o Índice de Preços ao Consumidor Amplo – IPCA, calculado pelo Instituto Brasileiro de Geografia e Estatística – IBGE, conforme disposto no Decreto Municipal nº 8.542, de 9 de maio de 2005.

14.6.3. O valor pactuado poderá ser revisto mediante solicitação da contratada, com vistas a restabelecer a equação econômico-financeira do contrato, na forma do inc. II, da alínea "d", do art. 65, da Lei nº. 8.666/93.

14.6.4. As eventuais solicitações deverão fazer-se acompanhar de comprovação de superveniência do fato imprevisível ou previsível, porém de consequências incalculáveis, bem como da demonstração analítica de seu impacto nos custos do Contrato.

XV - DA FISCALIZAÇÃO E ACOMPANHAMENTO

15.1. Observado o disposto no artigo 67 da Lei Federal nº 8.666/93, o acompanhamento, a fiscalização, o recebimento e a conferência do objeto será realizada pela Unidade Requisitante ou no caso de substituição, pelo que for indicado pelo gestor da Unidade Requisitante.

15.2. A Unidade Requisitante atestará, no documento fiscal correspondente, a execução dos serviços nas condições exigidas, constituindo tal atestação requisito para a liberação dos pagamentos ao contratado.

15.2.1. O recebimento definitivo do objeto deste instrumento, somente se efetivará com a atestação referida no item anterior.

15.3. Responsável pelo acompanhamento do contrato

15.3.1. Em conformidade com Art. 67 da Lei nº 8.666/93, será responsável pelo acompanhamento do contrato o Supervisor de Segurança da Informação do Departamento de Planejamento de Tecnologia da Informação da Subsecretaria de Tecnologia da Informação.

XVI – DA ENTREGA DO PRODUTO, SUPORTE TÉCNICO DURANTE TODA A VIGÊNCIA CONTRATUAL E MANUTENÇÃO DO SOFTWARE LICENCIADO

16.1. DA ENTREGA DO PRODUTO

16.1.1. As licenças do software antivírus corporativo deverão ser confirmadas e liberadas, no máximo de 15 (quinze) dias após a emissão da ordem de serviço emitida pela Subsecretaria de Tecnologia da Informação e enviadas à SEPLAG-JF/SSTI/DPTI/SSEG, situada à Av. Brasil, 2001 - 4º andar/Centro - 36.060-010 Juiz de Fora/MG, ou para o endereço eletrônico **seginfo@pjf.mg.gov.br.**

16.2. SUPORTE TÉCNICO DURANTE TODA A VIGÊNCIA CONTRATUAL

16.2.1. As licenças de uso devem incluir suporte técnico consistindo em:

16.2.1.1. Suporte remoto, via conexão de dados segura, ou presencial, prestado pela equipe habilitada pelo fabricante do produto, com certificação na solução;

16.2.1.2. Os chamados devem ser classificados de duas maneiras: aqueles onde haja parada no ambiente consumada, iminente ou forçada a acontecer por alguma decisão técnica e, aqueles onde não haja parada do ambiente, devendo haver tratamento de urgência diferenciado para as duas situações;

16.2.1.3. O suporte **"normal"** deve ser prestado em horário comercial com prazo de início de atendimento de até 24 (vinte e quatro) horas da abertura do chamado;

16.2.1.4. O suporte **"urgente"** deve ser prestado em qualquer horário e dia da semana, com prazo de início de atendimento de até 04 (quatro) horas da abertura do chamado;

16.2.1.5. Deve ser fornecido conta de acesso ao site do fabricante, onde se possa fazer o download dos componentes da solução e suas atualizações, bem como abrir tickets de atendimento.

16.3. MANUTENÇÃO DO SOFTWARE LICENCIADO

16.3.1. ACORDO DE NÍVEIS DE SERVIÇO

16.3.1.1. Entende-se como assistência técnica às correções de defeitos, ajustes e fornecimento de *releases* e versões (atualizações) do software.

16.3.1.2. São definidos como defeitos, os erros que provoquem funcionamento diferente daquele previsto na documentação do software.

16.3.1.3. São definidos como ajustes, alterações no software que melhore o seu desempenho nas aplicações da **CONTRATANTE.**

16.3.1.4. Entende-se por "*release"* pequenos ajustes no software. Neste caso, seu número de referência é incrementado, como por exemplo: de "11.1" para "11.2".

16.3.1.5. Entende-se por "versão" uma adição substancial dos recursos do software em questão; neste caso, seu número de referência é alterado de "11.1" para "12.0".

16.3.1.6. O fornecimento de nova "*release*" ou "versão" não implicará em custo adicional para a **CONTRATANTE**.

16.3.1.7. O serviço de suporte básico será realizado mediante solicitação da **CONTRATANTE**, em regime 8X5 (segunda à sexta em horário comercial).

16.3.1.8. Os problemas encontrados no software deverão ser descritos e notificados via uma das seguintes formas de contato: fac-símile, correio eletrônico (e-mail), skype e detalhados, se possível, com informações verbais pelo telefone.

16.3.1.9. Será fornecido à **CONTRATANTE** pela **CONTRATADA**, e sem custos adicionais, novo "release" do software na ocorrência de troca de versão do sistema operacional praticada no hardware onde está instalado o software. A **CONTRATADA** providenciará o envio do novo "release" no prazo máximo de 10 (dez) dias.

16.3.1.10. Toda despesa decorrente dos treinamentos (instrutores, elaboração do material didático, deslocamento, alimentação e hospedagem dos instrutores, etc.) será de exclusiva responsabilidade da **CONTRATADA**.

16.3.1.11. Somente o corpo técnico da **CONTRATADA** ou equipe habilitada pelo fabricante do produto com certificação na solução, poderá realizar os serviços a que se refere o contrato.

16.3.1.12. Os serviços contratados não incluem a correção de defeitos do software, decorrentes do uso indevido, negligência ou imperícia dos usuários ou problemas do sistema operacional ou do hardware onde o software esteja instalado e/ou decorrentes de qualquer modificação feita no software por qualquer um que não seja a própria **CONTRATADA** ou sem o seu consentimento.

16.3.1.13. Não faz parte da cobertura visitas de técnicos da **CONTRATADA** às instalações da **CONTRATANTE**, em virtude de problemas causados por imperícia ou desconhecimento, pelos usuários, das instruções ou normas básicas de operação e funcionamento do sistema, que, quando identificados pelo técnico escalado, serão cobradas integralmente da **CONTRATANTE**, ao valor de homem/hora de análise.

16.3.1.14. Quando, comprovadamente, as falhas detectadas no software coberto, sejam de responsabilidade da **CONTRATADA**, as correspondentes correções serão feitas sem ônus à **CONTRATANTE**.

XVII - DAS OBRIGAÇÕES

17.1. OBRIGAÇÕES DA CONTRATANTE

17.1.1. Receber o objeto no prazo e condições estabelecidas no contrato;

17.1.2. Verificar minuciosamente, no prazo fixado, a conformidade do produto recebido com as especificações constantes no Termo de Referência e Contrato;

17.1.3. Propiciar a **CONTRATADA** as condições necessárias à perfeita execução dos serviços contratados;

17.1.4. Acompanhar, fiscalizar e atestar a execução dos serviços;

17.1.5. Anotar em registro próprio todas as ocorrências relacionadas com a execução do contrato, determinando o que for necessário à regularização dos serviços, bem como anotando faltas da **CONTRATADA** ou falhas desta na execução do objeto;

17.1.6. Efetuar contatos, especificações de demandas, acompanhamento e pareceres técnicos referentes ao contrato;

17.1.7. Remeter advertências à **CONTRATADA**, por escrito, quando os serviços não estiverem sendo prestados de forma satisfatória.

17.2. OBRIGAÇÕES DA CONTRATADA

17.2.1. A **CONTRATADA** deverá realizar diagnósticos de problemas e prestar suporte remoto, via conexão de dados segura ou presencial;

17.2.2. Entregar o objeto contratual, na forma, prazo e local previstos. Caso o atendimento não seja feito dentro do prazo, a **CONTRATADA** ficará sujeita às sanções previstas em Contrato;

17.2.3. Cumprir o Acordo de Nível de Serviço (SLA) estabelecido referente aos serviços de suporte contratados.

17.2.4. Submeter à aprovação do **CONTRATANTE** toda e qualquer alteração ocorrida nas especificações, em face de imposições técnicas, de cunho administrativo ou legal;

17.2.5. Responsabilizar-se por todos os encargos sociais, trabalhistas, previdenciários, fiscais e comerciais e tributos de qualquer espécie que venham a ser devidos em decorrência da execução deste instrumento, bem como custos relativos ao deslocamento e à estada de seus profissionais, caso existam;

17.2.6. Responsabilizar-se pelos danos causados diretamente ao **CONTRATANTE** ou a terceiros, decorrentes de sua culpa ou dolo, ação ou omissão, quando da execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento realizado pelo **CONTRATANTE**;

17.2.7. Arcar com o pagamento de eventuais multas aplicadas por quaisquer autoridades federais, estaduais e municipais, em consequência de fato a ela imputável e relacionado com esta contratação;

17.2.8. Arcar com todos os prejuízos advindos de perdas e danos, incluindo despesas judiciais e honorários advocatícios resultantes de ações judiciais, a que o **CONTRATANTE** for compelido a responder em decorrência da contratação;

17.2.9. Manter seus funcionários, quando nas dependências do **CONTRATANTE**, sujeitos às normas internas deste (segurança e disciplina), todos utilizando uniforme e crachá de identificação, porém sem qualquer vínculo empregatício com o órgão;

17.2.10. Possibilitar a fiscalização do **CONTRATANTE**, no tocante à verificação das especificações exigidas, prestando todos os esclarecimentos solicitados e atendendo às reclamações procedentes, caso ocorram;

17.2.11. Comunicar ao **CONTRATANTE**, de imediato e por escrito, qualquer irregularidade verificada durante a execução do contrato, para a adoção das medidas necessárias à sua regularização;

17.2.12. Manter durante toda a execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

17.2.13. Indicar seu preposto e respectivo substituto, que serão responsáveis pelo recebimento das demandas encaminhadas (Art. 68 da Lei n.º 8.666/93).

17.2.14. A **CONTRATADA** deverá responsabilizar-se pela confidencialidade, integridade e disponibilidade dos dados e informações custodiados em decorrência dos serviços prestados, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do **CONTRATANTE** ou de terceiros, devendo orientar seus empregados nesse sentido;

17.2.15. Os conhecimentos, dados e informações de propriedade do **CONTRATANTE**, tanto tecnológicos como administrativos, tais como: produtos, sistemas, técnicas, estratégias, métodos de operação e todos e quaisquer outros, repassados por força do objeto do contrato, constituem informação privilegiada e possuem caráter de confidencialidade;

17.2.16. Estas informações poderão ser utilizadas, só e exclusivamente, no cumprimento das cláusulas e condições estabelecidas no contrato, sendo expressamente vedado à **CONTRATADA**: utilizá-las para fins não previstos no instrumento contratual; e repassá-las a terceiros e/ou empregados não vinculados diretamente à execução do objeto contratado;

17.2.17. Fornecer, sem ônus para o **CONTRATANTE**, as atualizações e eventuais correções do software (*updates*);

17.2.18. Seguir todas as Normas, Políticas e Procedimentos de Segurança estabelecidas pelo **CONTRATANTE** para execução da Contratação, tanto nas dependências do **CONTRATANTE** como externamente;

17.2.19. Devem ser realizados também procedimentos periódicos de transferência de conhecimento, com o intuito de evitar que se crie um atraso de continuidade significativo entre os conhecimentos produzidos na execução contratual e a atualização tecnológica da equipe técnica e dos gestores, no que lhes concerne.

17.2.20. Propiciar todos os meios e facilidades necessárias à fiscalização dos serviços pela **CONTRATANTE**, cujo representante terá poderes para sustar o serviço, total ou parcialmente, a qualquer tempo, sempre que considerar a medida necessária, e recusar materiais e serviços empregados que não atendam aos termos contratuais;

17.2.21. Atender as demais condições estabelecidas no contrato.

XVIII – DAS PENALIDADES

18.1. Os casos de inexecução do objeto deste **edital**, erro de execução, execução imperfeita, atraso injustificado e inadimplemento, sujeitará o proponente contratado às penalidades previstas no Art. 87 da Lei nº 8.666/93, das quais destacam-se:
a) advertência;
b) multa de 0,5% (cinco décimos por cento) do valor, por dia de atraso injustificado na execução do mesmo, limitados a 30 (trinta) dias corridos, após o qual será caracterizada a inexecução total;
c) multa compensatória no valor de 5% (cinco por cento) sobre o valor total contratado;
d) suspensão temporária de participação em licitações e impedimento de contratar com o Município, no prazo de até 02 (dois) anos;
e) declaração de inidoneidade para contratar com a Administração Pública, até que seja promovida a reabilitação, facultando ao contratado o pedido de reconsideração da autoridade competente, no prazo de 10 (dez) dias da abertura de vistas ao processo.

18.2. Após o devido processo legal, as penalidades serão aplicadas pela autoridade competente que deverá comunicar a subsecretaria todas as ocorrências para fins de cadastramento e demais providências.

18.2.1. Entende-se por autoridade competente a gestora da despesa executada.

18.3. Os valores das multas aplicadas previstas nos sub-itens acima poderão ser descontados dos pagamentos devidos pela Administração.

18.4. Da aplicação das penalidades definidas nas alíneas "a", "b", "c" e "d" do item **18.1**, caberá recurso no prazo de (cinco) dias úteis, contados da intimação.

18.4.1. Da aplicação da penalidade definida na alínea "e" do item **18.1**, caberá pedido de reconsideração no prazo de 10 (dez) dias úteis, contados da intimação.

18.5. O recurso ou pedido de reconsideração relativo às penalidades acima dispostas será dirigido à autoridade gestora da despesa, a qual decidirá o recurso. no prazo de 05 (cinco) dias úteis e o pedido de reconsideração, no prazo de 10 (dez) dias úteis.

18.6. A aplicação de penalidades previstas para os casos de inexecução do objeto, erro de execução, execução imperfeita, atraso injustificado, inadimplemento e demais condutas ilícitas será de competência da autoridade gestora da despesa, nos termo do § 3º, do art. 87, da Lei nº 8.666/93.

18.7. O Município poderá rescindir o contrato, independentemente de qualquer procedimento judicial, observada a legislação vigente, nos seguintes casos:

a) por infração a qualquer de suas cláusulas;
b) decretação de falência, concurso de credores, dissolução ou liquidação;
c) em caso de transferência, no todo ou em parte, das obrigações assumidas neste contrato, sem prévio e expresso aviso ao Município;
d) por comprovada deficiência no atendimento do objeto do contrato;
e) mais de 2 (duas) advertências

18.8. A autoridade gestora da despesa poderá, ainda, sem caráter de penalidade, declarar rescindido o contrato por conveniência administrativa ou interesse público, conforme disposto no artigo 79 da Lei nº 8.666/93 e suas alterações.

XIX – DO PREÇO E DO PAGAMENTO

19.1. O preço total e o preço unitário deverão ser expressos em reais, com duas casas decimais, equivalentes ao de mercado na data da sessão pública de disputa de preços.

19.2. Deverão estar incluídos no preço, todos os insumos que o compõem, tais como as despesas com impostos, taxas, frete, seguros e quaisquer outros que incidam direta ou indiretamente sobre a execução do objeto desta licitação, sem quaisquer ônus para a Administração, e quaisquer outros que incidam sobre a avença.

19.3. O pagamento será em até 30 (trinta) dias e efetuado pela Unidade Requisitante, creditado em favor da licitante vencedora, através de ordem bancária contra a entidade bancária indicada na proposta (conforme modelo descrito abaixo), em que deverá ser efetivado o crédito:
BANCO: ..... AGÊNCIA: ..... CONTA CORRENTE: ..... LOCALIDADE: .....

19.4. Para efeito de cada pagamento a nota fiscal/fatura deverá estar acompanhada da autorização de uso da nota fiscal eletrônica, em duas vias emitidas através do site www.nfe.fazenda.gov.br, digitando a chave de acesso descrita no DANFE.

19.4.1. No caso da não apresentação da documentação de que trata o item **19.4**. ou estando o objeto em desacordo com as especificações e demais exigências do edital, fica a Unidade Requisitante autorizada a efetuar o pagamento, em sua integralidade, somente quando forem processadas as alterações e retificações determinadas, sem prejuízo da aplicação, ao fornecedor, das penalidades previstas.

19.4.2. A Unidade Requisitante poderá descontar do pagamento importâncias que, a qualquer título, lhes sejam devidas pelo fornecedor, por força da contratação.

19.4.3. Quando ocorrer a situação prevista no item **19.4.2**, não correrá juros ou atualizações monetárias de natureza qualquer, sem prejuízo de outras penalidades previstas.

19.4.4. Os documentos de cobrança deverão ser corretamente emitidos e no caso de incorreções serão devolvidos, e o prazo para o pagamento contar-se-á da data de reapresentação da nota fiscal eletrônica/fatura.

19.5. As Notas Fiscais deverão ser emitidas em moeda corrente do país.

19.5.1. Juntamente com a nota fiscal, a contratada deverá apresentar o certificado de regularidade do FGTS e a Certidão Conjunta de Débitos Relativos a Tributos Federais e à Dívida Ativa da União.

19.6. Na eventualidade de aplicação de multas, estas deverão ser liquidadas simultaneamente com parcela vinculada ao evento cujo descumprimento der origem à aplicação da penalidade.

19.7. O CNPJ da contratada constante da nota fiscal e fatura deverá ser o mesmo da documentação apresentada no procedimento licitatório.

19.8. No ato de retirada da Nota de Empenho, o fornecedor deverá fornecer os dados bancários (banco, agência e nº da conta) para depósitos referentes aos pagamentos, conforme exigência do SIAFEM.

19.9. Nenhum pagamento será efetuado ao proponente vencedor enquanto pendente de liquidação quaisquer obrigações financeiras que lhe foram impostas, em virtude de penalidade ou inadimplência, sem que isso gere direito ao pleito de reajustamento de preços ou correção monetária.

19.10. Com relação ao recolhimento de tributos na fonte sobre a prestação dos serviços descritos neste documento, o DEIN da SEPLAG-JF, informa: com relação ao recolhimento de tributos na fonte sobre a prestação de serviço de informática.

- Serviço passivo de retenção de IRRF;
- Serviço não passivo de retenção de INSS;
- Serviço não passivo de retenção de ISSQN.

19.10.1. A retenção do Imposto de Renda na Fonte e da Contribuição Previdenciária será feita em conformidade com o disposto nas Instruções Normativas/Manuais disponibilizados no site da PJF na página do Controle Interno: link: http://pjf.mg.gov.br/subsecretarias/controle_interno/legislacao.php.

XX - DAS SANÇÕES ADMINISTRATIVAS

20.1. Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, o proponente/adjudicatário que:

20.1.1. não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;

20.1.2. não assinar a ata de registro de preços, quando cabível;

20.1.3. apresentar documentação falsa;

20.1.4. deixar de entregar os documentos exigidos no certame;

20.1.5. ensejar o retardamento da execução do objeto;

20.1.6. não mantiver a proposta;

20.1.7. cometer fraude fiscal;

20.1.8. comportar-se de modo inidôneo;

20.2. 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 proponentes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

20.3. O proponente/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

20.3.1. Advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação;

20.3.2. Multa de 5% (cinco por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;

20.3.3. Impedimento de licitar e de contratar com o Município, pelo prazo de até dois anos;

20.3.4. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

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

20.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993.

20.6. 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.

XXI – DA IMPUGNAÇÃO AO ATO CONVOCATÓRIO

21.1. Decairá do direito de impugnar ou solicitar esclarecimentos acerca dos termos do presente Edital o proponente que não apontar as falhas ou irregularidades supostamente existentes até o **3º (terceiro) dia útil** que anteceder a data de início da sessão de disputa do Pregão, **por meio eletrônico**, devendo o Pregoeiro decidir sobre a impugnação ou prestar os esclarecimentos no prazo de até dois dias úteis contados da data de recebimento desta. Sendo intempestiva, a comunicação do suposto vício não suspenderá o curso do certame.

21.1.1. A impugnação feita tempestivamente pela proponente não a impedirá de participar do processo licitatório, ao menos até o trânsito em julgado da decisão a ela pertinente. Acolhida a petição contra o ato convocatório, será designada nova data para a realização do certame, se for o caso, sendo corrigido o ato convocatório.

21.1.2. Decairá também do direito de impugnar, perante a Administração, os termos deste edital, aquela que, tendo-o aceito sem objeção, vier a apontar depois do início da sessão de disputa do Pregão, falhas ou irregularidades que o viciaram, hipótese que não será aceita como recurso.

XXII – DISPOSIÇÕES GERAIS

22.1. Serão utilizados para a realização deste certame recursos de tecnologia da informação, compostos por um conjunto de programas de computador que permitem confrontação sucessiva através do envio de lances dos proponentes com plena visibilidade para o pregoeiro e total transparência dos resultados para a sociedade, através da Rede Mundial de Computadores – INTERNET.

22.2. A realização do procedimento estará a cargo da **Comissão Permanente de Licitação - CPL**, **subsecretaria** responsável pelo planejamento, coordenação e gerenciamento do sistema de licitações e contratos no âmbito da Administração Pública Direta, Autárquica e Fundacional e da Administradora do Pregão Eletrônico, entidade contratada para, através da rede mundial de computadores, prover o sistema de compras eletrônicas.

22.3. Como requisito para participação no pregão, em campo próprio do sistema eletrônico, a proponente deverá manifestar o pleno conhecimento e atendimento às exigências previstas no Edital.

22.4. O fornecedor, ao utilizar sua senha de acesso ao sistema para dar um lance no evento, terá expressado sua decisão irrevogável de concluir a transação a que se refere o evento nos valores e condições do referido lance, e caso este lance seja o escolhido pelo comprador, será reputado perfeito e acabado o contrato de compra e venda do produto negociado.

22.5. Incumbirá ao proponente 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.

22.6. Nenhuma indenização será devida aos proponentes por apresentarem documentação e/ ou apresentarem proposta relativa ao presente PREGÃO.

22.7. É facultado ao Pregoeiro a realização de diligências no curso do procedimento licitatório, bem como, sanear falhas, fazer complementação de insuficiências ou ainda, correções de caráter formal.

22.7.1. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas e documentos de habilitação, 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.

22.7.2. Obriga-se a proponente a fornecer ao Pregoeiro os documentos originais correspondentes em qualquer época que lhe forem solicitados.

22.7.3. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhados por meio eletrônico, ou, em se tratando de amostra, na forma e prazo indicados pelo Pregoeiro, sob pena de não aceitação da proposta.

22.8. A presente licitação somente poderá vir a ser revogada por razões de interesse público decorrentes 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.

22.9. O resultado desta licitação será lavrado em Ata, a qual será assinada pelo Pregoeiro e Equipe de Apoio.

22.10. O proponente é responsável pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.

22.11. No interesse da Administração, sem que caiba às participantes qualquer recurso ou indenização, poderá a licitação ter:
a) adiada sua abertura;
b) alterado o Edital, com fixação de novo prazo para a realização da licitação.

22.12. Para dirimir quaisquer questões decorrentes do procedimento licitatório, elegem as partes o Foro da cidade de Juiz de Fora/MG, com renúncia expressa a qualquer outro por mais privilegiado que seja.

22.13. Esclarecimentos em relação a eventuais dúvidas de interpretação do presente Edital poderão ser obtidos junto a **SARH/CPL/PJF** pelo telefone: (32) 3690-8188/8187/8492, nos dias úteis no horário das 09 às 11 horas ou 15 às 17 horas, ou através do e-mail **pregaoeletronico@pjf.mg.gov.br.**

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

22.15. Os casos omissos relativos à aplicabilidade do presente Edital serão sanados pela **PJF/SARH/CPL**, obedecida a legislação vigente.

22.16. O acompanhamento dos resultados, recursos e atos pertinentes a este edital poderão ser consultados no endereço: ***https://www.portaldecompraspublicas.com.br***, que será atualizado a cada nova etapa do pregão.

22.17. Fazem parte deste Edital os seguintes anexos:

Anexo I – Termo de Referência e Valor Estimado;
Anexo II – Minuta de Contrato.
Anexo III - Modelo de Declaração de Microempresa (ME) ou de Empresa de Pequeno Porte (EPP).
Anexo IV - Modelo de Declaração de Habilitação e Pleno Conhecimento.
Anexo V - Modelo de Declaração de Empregador Pessoa Jurídica.
Anexo VI – Modelo de Declaração de Inexistência de fato impeditivo.

PREGÃO ELETRÔNICO nº 044/2020 - SEPLAG

ANEXO I - TERMO DE REFERÊNCIA E ORÇAMENTO ESTIMADO

1. INTRODUÇÃO

O presente documento tem o objetivo de definir as características técnicas para uma nova contratação com *upgrade* de versão das licenças de software antivírus corporativo, incluindo, ativação, configuração, gerenciamento centralizado, garantia de atualização contínua e suporte técnico.

2. JUSTIFICATIVA TÉCNICA

Com um crescente número de ataques cibernéticos cada vez mais especializados, a contratação de uma solução de antivírus é imprescindível à segurança de qualquer parque computacional, pois os sistemas interconectados são altamente propensos a infecções de pragas virtuais as quais propagam-se em números alarmantes. Não dispor de uma solução que acompanhe tal velocidade é estar suscetível aos seus malefícios. Assim, uma nova contratação com *upgrade* do ***software antivírus Kaspersky Advanced Security for Business*** faz-se necessária para garantir a integridade, confiabilidade e segurança das informações contra ações de programas maliciosos que ponham em risco a segurança, preservando as estações de trabalho, equipamentos servidores, *laptops* e dispositivos móveis de toda a Prefeitura de Juiz de Fora (PJF) contra vírus e códigos manipulados.

Nos últimos anos vivenciamos uma crescente de ataques cibernéticos, seja em órgãos públicos ou na iniciativa privada, o que nos traz a necessidade de uma ferramenta confiável, robusta e eficaz de proteção.

A solução em operação na Prefeitura de Juiz de Fora (PJF), mantida pelo fabricante *Kaspersky é* uma das mais conceituadas do mercado, reconhecida por especialistas da área como a tecnologia de software mais indicada para o uso corporativo, visto as facilidades para gerenciamento centralizado e suporte a diversas plataformas de servidores, estações de trabalho e dispositivos móveis.

Segundo o Gartner, empresa referência na área de consultoria que cria conhecimento por meio de pesquisas sobre tecnologias, em especial a publicação, em 23 de agosto de 2019, do relatório Quadrante Mágico[1] para Proteção de *Endpoint*, que graficamente posicionou a ***Kaspersky*** como visionária do mercado no segmento, consolidando, assim, o caminho seguido pela SEPLAG-JF/SSTI.

Desta forma, é relevante a aquisição da solução ***Kaspersky*** já utilizada na PJF, otimizando a administração de todo o parque tecnológico, além de continuar permitindo a escalabilidade da solução implantada.

Junte-se as questões referidas nos parágrafos anteriores, a solução em operação na PJF disponibiliza recursos como: emissão de relatórios sobre o grau de infecção, gerenciamento dos equipamentos com o mesmo software, centralização das atualizações a partir de um único servidor, console de gerenciamento de estações de trabalho, *interface* de fácil acesso e eficácia na remoção das infecções virtuais.

Um outro fator fundamental diz respeito a PJF já utilizar a tecnologia da marca ***Kaspersky*** há cerca de 2 (dois) anos e meio, com aproximadamente **2.500** (duas mil e quinhentas) licenças ativadas e em operação, grande parte instaladas manualmente nos computadores das unidades da PJF inseridos na rede corporativa. As instalações se deram em grande parte de forma manual pelos seguintes motivos:

- **Ausência de controlador de domínio (LDAP - *Lightweight Directory Access Protocol*), ferramenta imprescindível para viabilizar instalações remotas dos agentes;**
- **1/3 (um terço) da rede (60 links de dados, incluindo diversos Postos de Saúde – UBS - serviços críticos - operando com baixíssima capacidade de transmissão - 1 Mbps, com tecnologia latente (radiofrequência), o que inviabiliza qualquer mecanismo de instalação remota.**
- **Nosso parque tecnológico apresenta uma heterogeneidade em se tratando dos sistemas operacionais presentes nos computadores, que estão em vias de modernização, mas ainda são um entrave para que um processo de instalação remota seja viabilizado com a segurança e confiabilidade necessárias.**

Em virtude da aquisição de novos computadores via PNAFM (Programa Nacional de Apoio à Gestão Administrativa e Fiscal dos Municípios Brasileiros), bem como da atualização tecnológica do Data Center prevista para ocorrer esse ano e da Lei Geral de Proteção de Dados[2] (LGPD), vislumbramos a necessidade de se dar um *upgrade* na licença atualmente em uso na PJF, de ***Select*** para ***Advanced***, tendo em vista ser uma tec-

nologia de maior porte para as necessidades da PJF, porém, que atenda as configurações da marca ***kaspersky*** para que não haja incompatibilidade com o ambiente já existente. Além disso, a versão ***Advanced*** possui a funcionalidade de criptografia de dados, para atendimento aos requisitos da LGPD, prevista para vigorar a partir de agosto de 2020.

O intuito de adquirirmos a mesma solução atualmente em uso na PJF é a de preservar os investimentos já efetuados (R$ 144.108,00)[3] para uso dessa ferramenta, aproveitando o nível de maturidade adquirido pela equipe no uso da solução, evitando-se assim desperdício de tempo e recursos em fazer uma nova instalação/configuração em todo o parque tecnológico, obtendo assim custos menores em se tratando de continuidade da mesma solução.

Além das justificativas apresentadas acima, manter uma solução de *Endpoint* robusta e eficaz também se faz necessário em face do fim do suporte e atualização de segurança da empresa **Microsoft** para o sistema operacional **Windows 7**, que ainda está presente em algumas máquinas da PJF. Enquanto não realizamos a atualização de todos os computadores para o sistema operacional **Windows 10**, uma solução de segurança conceituada e reconhecida é essencial como camada de segurança nas estações de trabalho.

Em face do exposto, a indicação da marca tem como fundamentação legal o **Art. 15, inc. I da Lei 8.666 de 1993**, o qual estabelece que *"as compras, sempre que possível deverão: atender ao princípio da padronização, que imponha compatibilidade de especificações técnicas e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantias oferecidas"*. Nesse sentido, a aquisição de licenças para uso do ***software antivírus Kaspersky Advanced Security for Business*** tem como finalidade precípua evitar desperdício de tempo e recursos na instalação e configuração de uma nova solução que não fosse da ***kaspersky***.

Sendo assim, torna-se imprescindível manter a segurança dos computadores adquirindo solução de antivírus robusta e essencial para que continuemos a utilizar os computadores do parque tecnológico da PJF com segurança.

3. OBJETO

Constitui objeto deste Termo de Referência (TR) a *Contratação de pessoa jurídica para* ***fornecimento de Solução de Segurança da Informação, composta por software antivírus Kaspersky Advanced Security for Business com licenças de uso para 24 (vinte e quatro) meses e suporte da CONTRATADA,*** **incluindo, ativação, configuração, gerenciamento centralizado, garantia de atualização contínua e suporte técnico**.

4. DESCRIÇÃO DO OBJETO E QUANTIDADES

Item	Descrição	Período	Quantidade
01	Renovação de licença de servidor	24 meses	01
02	Renovação de licença de uso de software antivírus corporativo	24 meses	2.700
03	Contratação de serviço de suporte técnico	24 meses	01

5. DETALHAMENTO DOS SERVIÇOS

A empresa **CONTRATADA** deverá ser responsável pelo fornecimento das novas licenças e pela devida prestação do suporte técnico contratado.

O processo deve incluir ajustes no ambiente que forem identificados e considerados necessários.

6. CARACTERÍSTICAS GERAIS DO SOFTWARE

6.1. O Software Antivírus contratado deve abranger:

6.1.2. Compatibilidade:
6.1.2.1. Microsoft Windows Server 2008 (Todas edições);
6.1.2.2. Microsoft Windows Server 2008 x64 SP1 (Todas edições);
6.1.2.3. Microsoft Windows Server 2008 R2 (Todas edições);
6.1.2.4. Microsoft Windows Server 2012 (Todas edições);

6.1.2.5. Microsoft Windows Server 2012 R2 (Todas edições);
6.1.2.6. Microsoft Windows Server 2016 x64
6.1.2.7. Microsoft Windows Small Business Server 2008 (Todas edições);
6.1.2.8. Microsoft Windows Small Business Server 2011 (Todas edições);
6.1.2.9. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;
6.1.2.10. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;
6.1.2.11. Microsoft Windows 8 SP1 Professional / Enterprise x32/x64;
6.1.2.12. Microsoft Windows 8 Professional / Enterprise x64;
6.1.2.13. Microsoft Windows 8.1 Professional / Enterprise x32;
6.1.2.14. Microsoft Windows 8.1 Professional / Enterprise x64;
6.1.2.15. Microsoft Windows 10 (Todas edições x32);
6.1.2.16. Microsoft Windows 10 (Todas edições x64).

6.1.3. Suportar as seguintes plataformas virtuais:
6.1.3.1. Vmware: Workstation 12.x Pro, vSphere 5.5, vSphere 6;
6.1.3.2. Microsoft Hyper-V: 2008, 2008 R2, 2008 R2 SP1, 2012, 2012 R2;
6.1.3.3. KVM integrado com: RHEL 5.4 e 5.x acima, SLES 11 Spx;
6.1.3.4. Citrix XenServer 6.1, 6.2. e 6.5;
6.1.3.5. Microsoft VirtualPC 6.0.156.0;
6.1.3.6. Parallels Desktop 7 e superior;
6.1.3.7. Oracle VM VirtualBox 4.0.4-70112.

6.1.4. Possuir as seguintes características:
6.1.4.1. A console deve ser acessada via WEB (HTTPS) ou MMC;
6.1.4.2. Console deve ser baseada no modelo cliente/servidor;
6.1.4.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
6.1.4.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
6.1.4.5. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch Management e MDM;
6.1.4.6. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
6.1.4.7. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
6.1.4.8. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
6.1.4.9. Deve registrar em arquivo de Log para todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
6.1.4.10. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
6.1.4.11. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
6.1.4.12. Capacidade de instalar remotamente a solução de segurança em Smartphones e Tablets de sistema iOS, Android e Windows;
6.1.4.13. Capacidade de instalar remotamente qualquer “app” em Smartphones e Tablets de sistema iOS;
6.1.4.14. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
6.1.4.15. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por sub-rede com os seguintes parâmetros: KB/s e horário;
6.1.4.16. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
6.1.4.17. Capacidade de gerenciar Smartphones e Tablets (Windows Phone, Android e iOS) protegidos pela solução de segurança;
6.1.4.18. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto;
6.1.4.19. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

6.1.4.20. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;
6.1.4.21. A comunicação entre o cliente e o servidor de administração deve ser criptografada;
6.1.4.22. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
6.1.4.23. Deve permitir a realocação de máquinas novas na rede para um determinado 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.

6.1.4.24. Capacidade de importar a estrutura do Active Directory para o descobrimento de máquinas;
6.1.4.25. 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;
6.1.4.26. Capacidade de monitorar diferentes sub-redes de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
6.1.4.27. 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;
6.1.4.28. Capacidade de, assim que detectar máquinas novas no Active Directory, sub-redes 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;
6.1.4.29. 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 02 (dois) dias, etc.;
6.1.4.30. 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;
6.1.4.31. Deve fornecer as seguintes informações dos computadores:
6.1.4.31.1. Se o antivírus está instalado;
6.1.4.31.2. Se o antivírus está iniciado;
6.1.4.31.3. Se o antivírus está atualizado;
6.1.4.31.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
6.1.4.31.5. Minutos/horas desde a última atualização de vacinas;
6.1.4.31.6. Data e horário da última verificação executada na máquina;
6.1.4.31.7. Versão do antivírus instalado na máquina;
6.1.4.31.8. Se é necessário reiniciar o computador para aplicar as mudanças;
6.1.4.31.9. Data e horário de quando a máquina foi ligada;
6.1.4.31.10. Quantidade de vírus encontrados (contador) na máquina;
6.1.4.31.11. Nome do computador;
6.1.4.31.12. Domínio ou grupo de trabalho do computador;
6.1.4.31.13. Data e horário da última atualização de vacinas;
6.1.4.31.14. Sistema operacional com Service Pack;
6.1.4.31.15. Quantidade de processadores;
6.1.4.31.16. Quantidade de memória RAM;
6.1.4.31.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
6.1.4.31.18. Endereço IP;
6.1.4.31.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
6.1.4.31.20. Atualizações do Windows Update instaladas;
6.1.4.31.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
6.1.4.31.22. Vulnerabilidades de aplicativos instalados na máquina.
6.1.4.32. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que os usuários não consigam alterá-las;

6.1.4.33. Capacidade de reconectar as máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
6.1.4.33.1. Alteração de Gateway Padrão;
6.1.4.33.2. Alteração de sub-rede;
6.1.4.33.3. Alteração de domínio;
6.1.4.33.4. Alteração de servidor DHCP;
6.1.4.33.5. Alteração de servidor DNS;
6.1.4.33.6. Alteração de servidor WINS;
6.1.4.33.7. Resolução de Nome;
6.1.4.33.8. Disponibilidade de endereço de conexão SSL.
6.1.4.34. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
6.1.4.35. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
6.1.4.36. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
6.1.4.37. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
6.1.4.38. 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;
6.1.4.39. 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;
6.1.4.40. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF,HTML e XML;
6.1.4.41. Capacidade de gerar traps SNMP para monitoramento de eventos;
6.1.4.42. Capacidade de enviar e-mails para contas específicas em caso de algum evento;
6.1.4.43. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e sub-redes;
6.1.4.44. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
6.1.4.45. Deve possuir compatibilidade com Cisco Network Admission Control (NAC);
6.1.4.46. Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo);
6.1.4.47. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc.), inclusive de máquinas que estejam em sub-redes diferentes do servidor;
6.1.4.48. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
6.1.4.49. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
6.1.4.50. 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;
- Ação realizada.

6.1.4.51. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
6.1.4.52. Capacidade de diferenciar máquinas virtuais de máquinas físicas.
6.1.4.53. Capacidade de listar updates nas máquinas com o respectivo link para download
6.1.4.54. Deve criar um backup de todos arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;
6.1.4.55. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;
6.1.4.56. Capacidade de realizar inventário de hardware de todas as máquinas clientes;
6.1.4.57. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
6.1.4.58. Capacidade de diferenciar máquinas virtuais de máquinas físicas.
6.1.4.59. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);

6.1.4.60. Capacidade de listar updates nas máquinas com o respectivo link para download.
6.1.4.61. Listar em um único local, todos os computadores não gerenciados na rede;

6.2. Estações Windows:

6.2.1. Compatibilidade:
6.2.1.1. Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e posterior;
6.2.1.2. Microsoft Windows 8.1 Pro / Enterprise x86 / x64;
6.2.1.3. Microsoft Windows 8.1 Pro / Enterprise x86 / x64;
6.2.1.4. Microsoft Windows 10 Pro / Enterprise x86 / x64;
6.2.1.5. Microsoft Windows Server 2012 R2 Standard x64;
6.2.1.6. Microsoft Windows Server 2012 Foundation x64;
6.2.1.7. Microsoft Windows Server 2012 Standard x64;
6.2.1.8. Microsoft Small Business Server 2011 Standard x64;
6.2.1.9. Microsoft Windows Server 2008 R2 Standard/Enterprise x64 SP1;
6.2.1.10. Microsoft Windows Server 2008 Standard/Enterprise x86/x64 SP2;
6.2.1.11. Microsoft Windows Server 2016 x64.

6.2.2. Características:
6.2.2.1. Deve prover as seguintes proteções:
6.2.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
6.2.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
6.2.2.1.3. Antivírus de e-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
6.2.2.1.4. Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc.);
6.2.2.1.5. O endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
6.2.2.1.6. Firewall com IDS;
6.2.2.1.7. Autoproteção (contra-ataques aos serviços/processos do antivírus);
6.2.2.1.8. Controle de dispositivos externos;
6.2.2.1.9. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;
6.2.2.1.10. Controle de acesso a sites por horário;
6.2.2.1.11. Controle de acesso a sites por usuários;
6.2.2.1.12. Controle de execução de aplicativos;
6.2.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados.
6.2.2.2. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
6.2.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ame aças encontradas no período (alta, média ou baixa);
6.2.2.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
6.2.2.5. 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, (ex:"Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
6.2.2.6. 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;
6.2.2.7. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
6.2.2.8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
6.2.2.9. 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;
6.2.2.10. Capacidade de verificar somente arquivos novos e alterados;
6.2.2.11. Capacidade de verificar objetos usando heurística;

6.2.2.12. Capacidade de agendar uma pausa na verificação;
6.2.2.13. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
6.2.2.14. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
6.2.2.15. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
6.2.2.15.1. Perguntar o que fazer, ou:
6.2.2.15.1.1. Bloquear acesso ao objeto;
6.2.2.15.1.2. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador).
6.2.2.15.2. Caso positivo de desinfecção:
6.2.2.15.2.1. Restaurar o objeto para uso.
6.2.2.15.3. Caso negativo de desinfecção:
6.2.2.15.3.1. Mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador).
6.2.2.16. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
6.2.2.17. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);
6.2.2.18. Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;
6.2.2.19. Capacidade de verificar links inseridos em e-mails contra phishings;
6.2.2.20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Opera, dentre outros;
6.2.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística;
6.2.2.22. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
6.2.2.22.1. Perguntar o que fazer, ou;
6.2.2.22.2. Bloquear o e-mail;
6.2.2.22.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador).
6.2.2.22.4. Caso positivo de desinfecção:
6.2.2.22.4.1. Restaurar o e-mail para o usuário.
6.2.2.22.5. Caso negativo de desinfecção:
6.2.2.22.5.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração preestabelecida pelo administrador).
6.2.2.23. Caso o e-mail contenha código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
6.2.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
6.2.2.25. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
6.2.2.26. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas;
6.2.2.27. Deve ter suporte total ao protocolo IPv6;
6.2.2.28. Capacidade de alterar as portas monitoradas pelos módulos de Web e e-mail;
6.2.2.29. Na verificação de tráfego web, caso encontrado código malicioso o programa deve perguntar o que fazer, ou:
6.2.2.29.1. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
6.2.2.29.2. Permitir acesso ao objeto.
6.2.2.30. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
6.2.2.30.1. Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo real, ou:
6.2.2.30.2. Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação.
6.2.2.31. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
6.2.2.32. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as consequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;
6.2.2.33. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;

6.2.2.34. 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;
6.2.2.35. Deve possuir módulo de bloqueio de *Phishing*, com atualizações incluídas nas vacinas, obtidas pelo *Anti-Phishing Working Group* (http://www.antiphishing.org/);
6.2.2.36. Capacidade de distinguir diferentes sub-redes e conceder opção de ativar ou não o firewall para uma sub-rede específica;
6.2.2.37. Deve possuir módulo IDS (*Intrusion Detection System*) para proteção contra *port scans* e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada junto com as vacinas;
6.2.2.38. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
6.2.2.38.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
6.2.2.38.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo que terá acesso à rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
6.2.2.39. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
6.2.2.39.1. Discos de armazenamento locais;
6.2.2.39.2. Armazenamento removível;
6.2.2.39.3. Impressoras;
6.2.2.39.4. CD/DVD;
6.2.2.39.5. Drives de disquete;
6.2.2.39.6. Modems;
6.2.2.39.7. Dispositivos de fita;
6.2.2.39.8. Dispositivos multifuncionais;
6.2.2.39.9. Leitores de smart card;
6.2.2.39.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc.);
6.2.2.39.11. Wi-Fi;
6.2.2.39.12. Adaptadores de rede externos;
6.2.2.39.13. Dispositivos MP3 ou Smartphones;
6.2.2.39.14. Dispositivos Bluetooth;
6.2.2.39.15. Câmeras e Scanners.
6.2.2.40. 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;
6.2.2.41. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
6.2.2.42. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
6.2.2.43. Capacidade de configurar novos dispositivos por Class ID/Hardware;
6.2.2.44. Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc.), com possibilidade de configuração por usuário ou grupos de usuários e agendamento;
6.2.2.45. Capacidade de limitar a execução de aplicativos por hash MD5, 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.);
6.2.2.46. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
6.2.2.47. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;
6.2.2.48. 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;
6.2.2.49. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.
6.2.2.50. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:
6.2.2.50.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.
6.2.2.50.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.
6.2.2.51. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

6.2.2.52. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).
6.2.2.53. Capacidade de integração com o Windows Defender Security Center.
6.2.2.54. Capacidade de integração com a Antimalware Scan Interface (AMSI).
6.2.2.55. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).
6.2.2.56. Deve possuir módulo que monitora e bloqueia atividades potencialmente maliciosas, baseado no comportamento do usuário e Machine Learning.
6.2.2.56.1. O módulo deve ser capaz de agir nos seguintes estados:
6.2.2.56.1.1. Aprendizado: coleta informações sobre as atividades executadas pelo usuário.
6.2.2.56.1.2. Bloqueio: bloqueia as atividades potencialmente maliciosas que não sejam compatíveis com a rotina do usuário.
6.2.2.56.1.3. Notificação: notifica sobre as atividades potencialmente maliciosas que não sejam compatíveis com a rotina do usuário.

6.3. Estações Mac OS X

6.3.1. Compatibilidade:
6.3.1.1. Mac OS X 10.9 (Mavericks);
6.3.1.2. Mac OS X 10.10 (Yosemite);
6.3.1.3. Mac OS X 10.11 (El Capitan);
6.3.1.4. Mac OS 10.12 (Sierra);
6.3.1.5. Mac OS 10.13 (High Sierra);

6.3.2. Características:
6.3.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
6.3.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
6.3.2.3. A instalação e primeira execução do produto deve ser feita sem necessidade de reinicializarão do computador, de modo que o produto funcione com toda sua capacidade;
6.3.2.4. Deve possuir suportes a notificações utilizando o Growl;
6.3.2.5. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ame aças encontradas no período (alta, média ou baixa);
6.3.2.6. Capacidade de voltar para a base de dados de vacina anterior;
6.3.2.7. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
6.3.2.8. 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, (ex:"Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
6.3.2.9. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
6.3.2.10. 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;
6.3.2.11. Capacidade de verificar somente arquivos novos e alterados;
6.3.2.12. Capacidade de verificar objetos usando heurística;
6.3.2.13. Capacidade de agendar uma pausa na verificação;
6.3.2.14. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
6.3.2.14.1. Perguntar o que fazer, ou;
6.3.2.14.2. Bloquear acesso ao objeto;
6.3.2.14.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador).
6.3.2.14.4. Caso positivo de desinfecção:
6.3.2.14.4.1. Restaurar o objeto para uso.
6.3.2.14.5. Caso negativo de desinfecção:
6.3.2.14.5.1. Mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador).

6.3.2.15. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
6.3.2.16. Capacidade de verificar arquivos de formato de e-mail;
6.3.2.17. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;
6.3.2.18. Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

6.4. Estações de trabalho Linux:

6.4.1. Compatibilidade:

6.4.1.1. Plataforma 32-bits:
6.4.1.1.1. Red Hat Enterprise Linux 6.9;
6.4.1.1.2. Linux Mint 18.x;
6.4.1.1.3. Linux Mint 19.x;
6.4.1.1.4. CentOS-6.9;
6.4.1.1.5. CentOS-8;
6.4.1.1.6. Debian GNU/Linux 9.4
6.4.1.1.7. Debian GNU/Linux 10;
6.4.1.1.8. Ubuntu 16.04 LTS;
6.4.1.1.9. Ubuntu 18.04 LTS.

6.4.1.2. Plataforma 64-bits:
6.4.1.1.1. Red Hat Enterprise Linux 6.9;
6.4.1.1.2. Linux Mint 18.x;
6.4.1.1.3. Linux Mint 19.x;
6.4.1.1.4. CentOS-6.9;
6.4.1.1.5. CentOS-8;
6.4.1.1.6. Debian GNU/Linux 9.4
6.4.1.1.7. Debian GNU/Linux 10;
6.4.1.1.8. Ubuntu 16.04 LTS;
6.4.1.1.9. Ubuntu 18.04 LTS.

6.4.2. Características:

6.4.2.1. Deve prover as seguintes proteções:
6.4.2.1.1. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
6.4.2.1.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
6.4.2.2. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
6.4.2.2.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
6.4.2.2.2. 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;
6.4.2.2.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
6.4.2.2.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
6.4.2.3. Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
6.4.2.4. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

6.4.2.5. 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;
6.4.2.6. Capacidade de verificar objetos usando heurística;
6.4.2.7. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
6.4.2.8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
6.4.2.9. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).
6.4.2.10. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
6.4.2.10.1. Perguntar o que fazer, ou;
6.4.2.10.2. Bloquear acesso ao objeto;
6.4.2.10.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador);
6.4.8.10.4. Caso positivo de desinfecção:
6.4.8.10.5. Restaurar o objeto para uso.
6.4.8.10.6. Caso negativo de desinfecção:
6.4.8.10.7. Mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador).
6.4.2.11. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando.

6.5. Servidores Windows:

6.5.1. Compatibilidade:
6.5.1.1. Plataforma 32-bits:
6.5.1.1.1. Microsoft Windows Server 2008 Standard / Enterprise / Data Center (SP1 ou posterior);
6.5.1.1.2. Microsoft Windows Server 2008 Core Standard / Enterprise / Data Center (SP1 e posterior).

6.5.1.2. Plataforma 64-bits:
6.5.1.2.1. Microsoft Windows Server 2008 Standard / Enterprise / Data Center (SP1 ou posterior);
6.5.1.2.2. Microsoft Windows Server 2008 Core Standard / Enterprise / Data Center (SP1 ou posterior);
6.5.1.2.3. Microsoft Windows Server 2008 R2 Standard / Enterprise / Data Center (SP1 ou posterior);
6.5.1.2.4. Microsoft Windows Server 2008 R2 Core Standard / Enterprise / Data Center (SP1 ou posterior);
6.5.1.2.5. Microsoft Windows Storage Server 2008 R2;
6.5.1.2.6. Windows Storage Server 2016;
6.5.1.2.7. Microsoft Windows Hyper-V Server 2008 R2 (SP1 ou posterior);
6.5.1.2.8. Microsoft Windows Server 2012 Essentials / Standard / Foundation / Data Center;
6.5.1.2.9. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Data Center;
6.5.1.2.10. Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Data Center;
6.5.1.2.11. Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Data Center;
6.5.1.2.12. Microsoft Windows Storage Server 2012 (Todas edições);
6.5.1.2.13. Microsoft Windows Storage Server 2012 R2 (Todas edições);
6.5.1.2.14. Microsoft Windows Hyper-V Server 2012;
6.5.1.2.15. Microsoft Windows Hyper-V Server 2012 R2;
6.5.1.2.16. Windows Server 2016 Essentials/Standard/Datacenter/Core;
6.5.1.2.17. Windows Hyper-V Server 2016.

6.5.2. Características:
6.5.2.1. Deve prover as seguintes proteções:
6.5.2.2. Antivírus de Arquivos residente (anti-spyware, antitrojan, antimalware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
6.5.2.3. Auto-proteção contra-ataques aos serviços/processos do antivírus;
6.5.2.4. Firewall com IDS;
6.5.2.5. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
6.5.2.6. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

6.5.2.7. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
6.5.2.8. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
6.5.2.9. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
6.5.2.10. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
6.5.2.11. Leitura de configurações;
6.5.2.12. Modificação de configurações;
6.5.2.13. Gerenciamento de Backup e Quarentena;
6.5.2.14. Visualização de relatórios;
6.5.2.15. Gerenciamento de relatórios;
6.5.2.16. Gerenciamento de chaves de licença;
6.5.2.17. Gerenciamento de permissões (adicionar/excluir permissões acima);
6.5.2.18. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
6.5.2.18.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
6.5.2.18.2. 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 à rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
6.5.2.19. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;
6.5.2.20. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc.);
6.5.2.21. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (*Uninterruptible Power Supply – UPS*);
6.5.2.22. Em caso de erros, deve ter capacidade de criar *logs* e *traces* automaticamente, sem necessidade de outros softwares;
6.5.2.23. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
6.5.2.24. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
6.5.2.25. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
6.5.2.26. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
6.5.2.27. 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, (ex:"Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
6.5.2.28. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
6.5.2.29. 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;
6.5.2.30. Capacidade de verificar somente arquivos novos e alterados;
6.5.2.31. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos autodescompressores, .PST, arquivos compactados por compactadores binários, etc.);
6.5.2.32. Capacidade de verificar objetos usando heurística;
6.5.2.33. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
6.5.2.34. Capacidade de agendar uma pausa na verificação;
6.5.2.35. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
6.5.2.36. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
6.5.2.36.1. Perguntar o que fazer, ou;
6.5.2.36.2. Bloquear acesso ao objeto;
6.5.2.36.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador).
6.5.2.36.4. Caso positivo de desinfecção:
6.5.2.36.4.1. Restaurar o objeto para uso.
6.5.2.36.5. Caso negativo de desinfecção:

6.5.2.36.5.1. Mover para quarentena ou apagar (de acordo com configuração preestabelecida pelo administrador).
6.5.2.37. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
6.5.2.38. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
6.5.2.39. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
6.5.2.40. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

6.6. Servidores Linux:

6.6.1. Compatibilidade:

6.6.1.1. Plataforma 32-bits:
6.6.1.1.1. Red Hat Enterprise Linux Server 6.9;
6.6.1.1.2. CentOS-6.9 ou superior;
6.6.1.1.3. Ubuntu Server 14.04 LTS;
6.6.1.1.4. Ubuntu Server 16.04 LTS;
6.6.1.1.5. Ubuntu Server 18.04 LTS;
6.6.1.1.6. Debian GNU/Linux 7,8,9 e 10;
6.6.1.1.7. Oracle Linux 8.1;

6.6.1.2. Plataforma 64-bits:
6.6.1.2.1. Red Hat Enterprise Linux Server 6.x;
6.6.1.2.2. Red Hat Enterprise Linux Server 7.x;
6.6.1.2.3. CentOS-6.9;
6.6.1.2.4. CentOS-7.0;
6.6.1.2.5. CentOS-8.0;
6.6.1.2.6. Oracle Linux 7.3;
6.6.1.2.7. Oracle Linux 8.1;
6.6.1.2.8. OpenSUSE® 15.1;
6.6.1.2.9. Debian GNU/Linux 7,8,9 e 10;
6.6.1.2.10. Ubuntu Server 14.04 LTS;
6.6.1.2.11. Ubuntu Server 16.04 LTS;
6.6.1.2.12. Ubuntu Server 18.04 LTS;
6.6.1.2.13. SUSE Linux Enterprise Server 12 SP3.

6.6.2. Características:

6.6.2.1. Deve prover as seguintes proteções:
6.6.2.1.1. Antivírus de Arquivos residente (anti-spyware, antitrojan, antimalware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
6.6.2.1.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
6.6.2.2. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
6.6.2.2.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
6.6.2.2.2. 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;
6.6.2.2.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
6.6.2.2.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;
6.6.2.3. Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
6.6.2.4. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

6.6.2.5. 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;
6.6.2.6. Capacidade de verificar objetos usando heurística;
6.6.2.7. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
6.6.2.8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
6.6.2.9. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

7. Smartphones e tablets

7.1. Compatibilidade:
7.1.1. Apple iOS 9.0 e posteriores;
7.1.2. Android 5.0 e posteriores.

7.2. Características:

Deve prover as seguintes proteções:

7.2.1. Proteção em tempo real do sistema de arquivos do dispositivo interceptação e verificação de ameaças digitais.
7.2.2. Proteção contra adware e autodialers;
7.2.3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;
7.2.4. Arquivos abertos no smartphone;
7.2.5. Programas instalados usando a interface do smartphone:
7.2.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;
7.2.7. Deverá isolar em área de quarentena os arquivos infectados;
7.2.8. Deverá atualizar as bases de vacinas de modo agendado;
7.2.9. Deverá bloquear spams de SMS através de Black lists;
7.2.10. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado com mensagem de aviso ao utilizador do dispositivo;
7.2.11. Capacidade de desativar por política:
7.2.12. Wi-fi;
7.2.13. Câmera;
7.2.14. Bluetooth.
7.2.15. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;
7.2.16. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;
7.2.17. Deverá ter firewall pessoal (Android);
7.2.18. Capacidade de tirar fotos quando a senha for inserida incorretamente;
7.2.19. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile;
7.2.20. Device Manager 2008 SP1;
7.2.21. Capacidade de enviar comandos remotamente de:
7.2.22. Localizar;
7.2.23. Bloquear.
7.2.24. Capacidade de detectar Jailbreak em dispositivos iOS;
7.2.25. Capacidade de bloquear o acesso a site por categoria em dispositivos;
7.2.26. Capacidade de bloquear o acesso a sites phishing ou malicioso;
7.2.27. Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;
7.2.28. Capacidade de bloquear o dispositivo quando o cartão “SIM” for substituído;
7.2.29. Capacidade de configurar White e blacklist de aplicativos;
7.2.30. Capacidade de localizar o dispositivo quando necessário;
7.2.31. Permitir atualização das definições quando estiver em “roaming”;
7.2.32. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

7.2.33. Deve permitir verificar somente arquivos executáveis;
7.2.34. Deve ter a capacidade de desinfectar o arquivo se possível;
7.2.35. Capacidade de agendar uma verificação;
7.2.36. Capacidade de enviar URL de instalação por e-mail;
7.2.37. Capacidade de fazer a instalação através de um link QRCode;
7.2.38. Capacidade de executar as seguintes ações caso a desinfecção falhe:

- Deletar;
- Ignorar;
- Quarentenar;
- Perguntar ao usuário.

8. Gerenciamento de dispositivos móveis (MDM)

8.1. Compatibilidade:
8.1.1. Dispositivos com os sistemas operacionais:
8.1.1.1. Apple iOS 9 e posteriores;
8.1.1.2. Android 5 e posteriores;

8.2. Características:
8.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;
8.2.2. Capacidade de ajustar as configurações de:
8.2.2.1. Sincronização de e-mail;
8.2.2.2. Uso de aplicativos;
8.2.2.3. Senha do usuário;
8.2.2.4. Criptografia de dados;
8.2.2.5. Conexão de mídia removível.
8.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;
8.2.4. Capacidade de, remotamente, *resetar* a senha de dispositivos iOS;
8.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;
8.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS;
8.2.7. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;
8.2.8. Possibilidade de exigir senha para abrir aplicações instaladas em container;
8.2.9. Deve permitir que o usuário utilize autenticação do Active Directory para abrir aplicações em container;
8.2.10. Deve permitir que uma senha seja digitada a cada x(minutos) para continuar utilizando uma aplicação em container;
8.2.11. Deve permitir a criptografia de dados salvos pelas aplicações em container;
8.2.12. Permitir sincronização com perfil do “Touch Down”;
8.2.13. Capacidade de desinstalar remotamente o antivírus do dispositivo;
8.2.14. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;
8.2.15. Capacidade de sincronizar com Samsung Knox;
8.2.16. Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

9. Criptografia

9.1. Compatibilidade

9.1.1. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;
9.1.2. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;
9.1.3. Microsoft Windows 7 Professional SP1 ou superior x86/x64;
9.1.4. Microsoft Windows 8 Enterprise x86/x64;
9.1.5. Microsoft Windows 8 Pro x86/x64;
9.1.6. Microsoft Windows 8.1 Pro x86/x64;
9.1.7. Microsoft Windows 8.1 Enterprise x86/x64;
9.1.8. Microsoft Windows 10 Enterprise x86/x64;
9.1.9. Microsoft Windows 10 Pro x86/x64;

9.2. Características

9.2.1. 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;
9.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
9.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
9.2.4. Capacidade de utilizar *Single Sign-On* para a autenticação de pré-boot;
9.2.5. Permitir criar vários usuários de autenticação pré-boot;
9.2.6. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
9.2.7. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
9.2.7.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
9.2.7.2. Criptografar todos os arquivos individualmente;
9.2.7.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
9.2.7.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;
9.2.8. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;
9.2.9. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
9.2.10. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
9.2.11. Verifica compatibilidade de hardware antes de aplicar a criptografia;
9.2.12. Possibilita estabelecer parâmetros para a senha de criptografia;
9.2.13. Bloqueia o reuso de senhas;
9.2.14. Bloqueia a senha após um número de tentativas preestabelecidas;
9.2.15. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
9.2.16. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo
9.2.17. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;
9.2.18. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
9.2.19. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;
9.2.20. Permite criar um grupo de extensões de arquivos a serem criptografados;
9.2.21. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
9.2.22. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento;
9.2.23. Capacidade de deletar arquivos de forma segura após a criptografia;
9.2.24. Capacidade de criptografar somente o espaço em disco utilizado;
9.2.25. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
9.2.26. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
9.2.27. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;
9.2.28. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;
9.2.29. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
9.2.30. Capacidade de fazer “Hardware encryption”.

10. Gerenciamento de Sistemas

10.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores *bare-metal*;
10.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;
10.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
10.4. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;
10.5. Capacidade de gerenciar licenças de softwares de terceiros;
10.6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
10.7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, service tag, número de identificação e outros;
10.8. Possibilita fazer distribuição de software de forma manual e agendada;
10.9. Suporta modo de instalação silenciosa;
10.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
10.11. Possibilita fazer a distribuição através de agentes de atualização;
10.12. Utiliza tecnologia multicast para evitar tráfego na rede;
10.13. Possibilita criar um inventário centralizado de imagens;
10.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
10.15. Suporte a WakeOnLan para deploy de imagens;
10.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
10.17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
10.18. Capacidade de gerar relatórios de vulnerabilidades e patches;
10.19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
10.20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
10.21. Permite baixar atualizações para o computador sem efetuar a instalação;
10.22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
10.23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
10.24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
10.25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;
10.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
10.27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;
10.28. Capacidade de configurar o reinício do computador após a aplicação das atualizações e correções de vulnerabilidades;
10.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;
10.30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes.

11. SUPORTE TÉCNICO DURANTE TODA A VIGÊNCIA CONTRATUAL

11.1. As licenças de uso devem incluir suporte técnico consistindo em:

11.1.1. Suporte remoto, via conexão de dados segura, ou presencial, prestado pela equipe habilitada pelo fabricante do produto, com certificação na solução;

11.1.2. Os chamados devem ser classificados de duas maneiras: aqueles onde haja parada no ambiente consumada, iminente ou forçada a acontecer por alguma decisão técnica e, aqueles onde não haja parada do ambiente, devendo haver tratamento de urgência diferenciado para as duas situações;

11.1.3. O suporte **"normal"** deve ser prestado em horário comercial com prazo de início de atendimento de até 24 (vinte e quatro) horas da abertura do chamado;

11.1.4. O suporte **"urgente"** deve ser prestado em qualquer horário e dia da semana, com prazo de início de atendimento de até 04 (quatro) horas da abertura do chamado;

11.1.5. Deve ser fornecido conta de acesso ao site do fabricante, onde se possa fazer o download dos componentes da solução e suas atualizações, bem como abrir tickets de atendimento.

12. ORÇAMENTO ESTIMADO: CUSTO DA CONTRATAÇÃO

Para efeito de referência e planejamento estima-se o custo médio em:

ITEM	DESCRIÇÃO	PERÍODO	QTD.	VR. UNITÁRIO (R$)	VR. TOTAL (R$)
01	Renovação com *upgrade* de licença de software antivírus corporativo sendo uma das licenças para Servidor de Núcleo de Distribuição e Console de Gerenciamento do Parque Tecnológico	24 meses	2.701	89,94	242.927,94
02	Serviço de suporte técnico	24 meses	01	1.075,00	25.800,00
TOTAL					**268.727,94**

13. DA ENTREGA DO PRODUTO

As licenças do software antivírus corporativo deverão ser confirmadas e liberadas, no máximo de 15 (quinze) dias após a emissão da ordem de serviço emitida pela Subsecretaria de Tecnologia da Informação e enviadas à SEPLAG-JF/SSTI/DPTI/SSEG, situada à Av. Brasil, 2001 - 4º andar/Centro - 36.060-010 Juiz de Fora/MG, ou para o endereço eletrônico **seginfo@pjf.mg.gov.br**.

14. DOTAÇÃO ORÇAMENTÁRIA E TRIBUTAÇÃO

O valor proposto para as licenças do software antivírus corporativo, incluindo, ativação, configuração, gerenciamento centralizado, garantia de atualização contínua e suporte técnico, pelo período de no mínimo 24 (vinte e quatro) meses, partirá da fonte **0100600000** de natureza **nº 3.3.90.40.36** cuja dotação é **04.126.0001.1051.0000**.

14.1. TRIBUTAÇÃO

Com relação ao recolhimento de tributos na fonte sobre a prestação dos serviços descritos neste Termo de Referência, o DEIN da SEPLAG-JF, no e-mail que segue em anexo, informa: com relação ao recolhimento de tributos na fonte sobre a prestação de serviço de informática.

- Serviço passivo de retenção de IRRF;
- Serviço não passivo de retenção de INSS;
- Serviço não passivo de retenção de ISSQN.

15. OBRIGAÇÕES DA CONTRATANTE

15.1. Receber o objeto no prazo e condições estabelecidas no contrato;

15.2. Verificar minuciosamente, no prazo fixado, a conformidade do produto recebido com as especificações constantes no Termo de Referência e Contrato;

15.3. Propiciar a **CONTRATADA** as condições necessárias à perfeita execução dos serviços contratados;

15.4. Acompanhar, fiscalizar e atestar a execução dos serviços;

15.5. Anotar em registro próprio todas as ocorrências relacionadas com a execução do contrato, determinando o que for necessário à regularização dos serviços, bem como anotando faltas da **CONTRATADA** ou falhas desta na execução do objeto;

15.6. Efetuar contatos, especificações de demandas, acompanhamento e pareceres técnicos referentes ao contrato;

15.7. Remeter advertências à **CONTRATADA**, por escrito, quando os serviços não estiverem sendo prestados de forma satisfatória.

16. OBRIGAÇÕES DA CONTRATADA

16.1. A **CONTRATADA** deverá realizar diagnósticos de problemas e prestar suporte remoto, via conexão de dados segura ou presencial;

16.2. Entregar o objeto contratual, na forma, prazo e local previstos. Caso o atendimento não seja feito dentro do prazo, a **CONTRATADA** ficará sujeita às sanções previstas em Contrato;

16.3. Cumprir o Acordo de Nível de Serviço (SLA) estabelecido referente aos serviços de suporte contratados.

16.4. Submeter à aprovação do **CONTRATANTE** toda e qualquer alteração ocorrida nas especificações, em face de imposições técnicas, de cunho administrativo ou legal;

16.5. Responsabilizar-se por todos os encargos sociais, trabalhistas, previdenciários, fiscais e comerciais e tributos de qualquer espécie que venham a ser devidos em decorrência da execução deste instrumento, bem como custos relativos ao deslocamento e à estada de seus profissionais, caso existam;

16.6. Responsabilizar-se pelos danos causados diretamente ao **CONTRATANTE** ou a terceiros, decorrentes de sua culpa ou dolo, ação ou omissão, quando da execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento realizado pelo **CONTRATANTE**;

16.7. Arcar com o pagamento de eventuais multas aplicadas por quaisquer autoridades federais, estaduais e municipais, em consequência de fato a ela imputável e relacionado com esta contratação;

16.8. Arcar com todos os prejuízos advindos de perdas e danos, incluindo despesas judiciais e honorários advocatícios resultantes de ações judiciais, a que o **CONTRATANTE** for compelido a responder em decorrência da contratação;

16.9. Manter seus funcionários, quando nas dependências do **CONTRATANTE**, sujeitos às normas internas deste (segurança e disciplina), todos utilizando uniforme e crachá de identificação, porém sem qualquer vínculo empregatício com o órgão;

16.10. Possibilitar a fiscalização do **CONTRATANTE**, no tocante à verificação das especificações exigidas, prestando todos os esclarecimentos solicitados e atendendo às reclamações procedentes, caso ocorram;

16.11. Comunicar ao **CONTRATANTE**, de imediato e por escrito, qualquer irregularidade verificada durante a execução do contrato, para a adoção das medidas necessárias à sua regularização;

16.12. Manter durante toda a execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

16.13. Indicar seu preposto e respectivo substituto, que serão responsáveis pelo recebimento das demandas encaminhadas (Art. 68 da Lei n.º 8.666/93).

16.14. A **CONTRATADA** deverá responsabilizar-se pela confidencialidade, integridade e disponibilidade dos dados e informações custodiados em decorrência dos serviços prestados, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do **CONTRATANTE** ou de terceiros, devendo orientar seus empregados nesse sentido;

16.15. Os conhecimentos, dados e informações de propriedade do **CONTRATANTE**, tanto tecnológicos como administrativos, tais como: produtos, sistemas, técnicas, estratégias, métodos de operação e todos e quaisquer outros, repassados por força do objeto do contrato, constituem informação privilegiada e possuem caráter de confidencialidade;

16.16. Estas informações poderão ser utilizadas, só e exclusivamente, no cumprimento das cláusulas e condições estabelecidas no contrato, sendo expressamente vedado à **CONTRATADA**: utilizá-las para fins não previstos no instrumento contratual; e repassá-las a terceiros e/ou empregados não vinculados diretamente à execução do objeto contratado;

16.17. Fornecer, sem ônus para o **CONTRATANTE**, as atualizações e eventuais correções do software (*updates*);

16.18. Seguir todas as Normas, Políticas e Procedimentos de Segurança estabelecidas pelo **CONTRATANTE** para execução da Contratação, tanto nas dependências do **CONTRATANTE** como externamente;

16.19. Devem ser realizados também procedimentos periódicos de transferência de conhecimento, com o intuito de evitar que se crie um atraso de continuidade significativo entre os conhecimentos produzidos na execução contratual e a atualização tecnológica da equipe técnica e dos gestores, no que lhes concerne.

16.20. Propiciar todos os meios e facilidades necessárias à fiscalização dos serviços pela **CONTRATANTE**, cujo representante terá poderes para sustar o serviço, total ou parcialmente, a qualquer tempo, sempre que considerar a medida necessária, e recusar materiais e serviços empregados que não atendam aos termos contratuais;

16.21. Atender as demais condições estabelecidas no contrato.

17. MANUTENÇÃO DO SOFTWARE LICENCIADO

17.1. ACORDO DE NÍVEIS DE SERVIÇO

17.1.1. Entende-se como assistência técnica às correções de defeitos, ajustes e fornecimento de *releases* e versões (atualizações) do software;

17.1.2. São definidos como defeitos, os erros que provoquem funcionamento diferente daquele previsto na documentação do software;

17.1.3. São definidos como ajustes, alterações no software que melhore o seu desempenho nas aplicações da **CONTRATANTE;**

17.1.4. Entende-se por "*release"* pequenos ajustes no software. Neste caso, seu número de referência é incrementado, como por exemplo: de "11.1" para "11.2";

17.1.5. Entende-se por "versão" uma adição substancial dos recursos do software em questão; neste caso, seu número de referência é alterado de "11.1" para "12.0";

17.1.6. O fornecimento de nova "*release*" ou "versão" não implicará em custo adicional para a **CONTRATANTE**;

17.1.7. O serviço de suporte básico será realizado mediante solicitação da **CONTRATANTE**, em regime 8X5 (segunda à sexta em horário comercial).

17.1.8. Os problemas encontrados no software deverão ser descritos e notificados via uma das seguintes formas de contato: fac-símile, correio eletrônico (e-mail), skype e detalhados, se possível, com informações verbais pelo telefone;

17.1.9. Será fornecido à **CONTRATANTE** pela **CONTRATADA**, e sem custos adicionais, novo "release" do software na ocorrência de troca de versão do sistema operacional praticada no hardware onde está instalado o software. A **CONTRATADA** providenciará o envio do novo "release" no prazo máximo de 10 (dez) dias;

17.1.10. Toda despesa decorrente dos treinamentos (instrutores, elaboração do material didático, deslocamento, alimentação e hospedagem dos instrutores, etc.) será de exclusiva responsabilidade da **CONTRATADA**.

17.1.11. Somente o corpo técnico da **CONTRATADA** ou equipe habilitada pelo fabricante do produto com certificação na solução, poderá realizar os serviços a que se refere o contrato;

17.1.12. Os serviços contratados não incluem a correção de defeitos do software, decorrentes do uso indevido, negligência ou imperícia dos usuários ou problemas do sistema operacional ou do hardware onde o software esteja instalado e/ou decorrentes de qualquer modificação feita no software por qualquer um que não seja a própria **CONTRATADA** ou sem o seu consentimento;

17.1.13. Não faz parte da cobertura visitas de técnicos da **CONTRATADA** às instalações da **CONTRATANTE**, em virtude de problemas causados por imperícia ou desconhecimento, pelos usuários, das instruções ou normas básicas de operação e funcionamento do sistema, que, quando identificados pelo técnico escalado, serão cobradas integralmente da **CONTRATANTE**, ao valor de homem/hora de análise;

17.1.14. Quando, comprovadamente, as falhas detectadas no software coberto, sejam de responsabilidade da **CONTRATADA**, as correspondentes correções serão feitas sem ônus à **CONTRATANTE**.

18. PREÇO E CONDIÇÕES DE PAGAMENTO

Para pagamento, caberá à **CONTRATADA** emitir Nota Fiscal referente aos serviços objetivados no presente termo.

19. VIGÊNCIA

19.1. O contrato terá vigência de 24 (vinte e quatro) meses a partir da data de assinatura.

19.2. Ao final do período acima estipulado, poderá ser prorrogado por iguais e sucessivos períodos, através de Termo Aditivo, desde que não haja manifestação por escrito em contrário, por quaisquer das partes, no prazo de até 30 (trinta) dias antes de cada término de contrato/aditivo, ficando estabelecido que sua rescisão desobrigará as partes dos compromissos pactuados no aludido contrato.

19.3. Do reajuste do contrato:

19.3.1. O contrato poderá ter o seu valor reajustado, desde que seja observado o interregno mínimo de 01(um) ano, a contar da data da proposta, ou da data do orçamento a que a proposta se referir, conforme disposto no Decreto Municipal nº 8.542, de 09 de maio de 2005.

19.3.2. Para o reajuste do contrato será adotado como indicador o Índice de Preços ao Consumidor Amplo – IPCA, calculado pelo Instituto Brasileiro de Geografia e Estatística – IBGE, conforme disposto no Decreto Municipal nº 8.542, de 9 de maio de 2005.

19.3.3. O valor pactuado poderá ser revisto mediante solicitação da contratada, com vistas a restabelecer a equação econômico-financeira do contrato, na forma do inc. II, da alínea "d", do art. 65, da Lei nº. 8.666/93.

19.3.4. As eventuais solicitações deverão fazer-se acompanhar de comprovação de superveniência do fato imprevisível ou previsível, porém de consequências incalculáveis, bem como da demonstração analítica de seu impacto nos custos do Contrato.

20. PENALIDADES

20.1. Os casos de inexecução do objeto da licitação, erro de execução, execução imperfeita, atraso injustificado e inadimplemento, sujeitará o proponente contratado às penalidades previstas no Art. 87 da Lei nº 8.666/93, das quais destacam-se:
a) advertência;
b) multa de 0,5% (cinco décimos por cento) do valor, por dia de atraso injustificado na execução do mesmo, limitados a 30 (trinta) dias corridos, após o qual será caracterizada a inexecução total;
c) multa compensatória no valor de 5% (cinco por cento) sobre o valor total contratado;
d) suspensão temporária de participação em licitações e impedimento de contratar com o Município, no prazo de até 02 (dois) anos;
e) declaração de inidoneidade para contratar com a Administração Pública, até que seja promovida a reabilitação, facultando ao contratado o pedido de reconsideração da autoridade competente, no prazo de 10 (dez) dias da abertura de vistas ao processo.

20.2. Após o devido processo legal, as penalidades serão aplicadas pela autoridade competente que deverá comunicar a subsecretaria todas as ocorrências para fins de cadastramento e demais providências.

20.2.1. Entende-se por autoridade competente a gestora da despesa executada.

20.3. Os valores das multas aplicadas previstas nos sub-itens acima poderão ser descontados dos pagamentos devidos pela Administração.

20.4. Da aplicação das penalidades definidas nas alíneas "a", "b", "c" e "d" do item **20.1**, caberá recurso no prazo de (cinco) dias úteis, contados da intimação.

20.4.1. Da aplicação da penalidade definida na alínea "e" do item **20.1**, caberá pedido de reconsideração no prazo de 10 (dez) dias úteis, contados da intimação.

20.5. O recurso ou pedido de reconsideração relativo às penalidades acima dispostas será dirigido à autoridade gestora da despesa, a qual decidirá o recurso. no prazo de 05 (cinco) dias úteis e o pedido de reconsideração, no prazo de 10 (dez) dias úteis.

20.6. A aplicação de penalidades previstas para os casos de inexecução do objeto, erro de execução, execução imperfeita, atraso injustificado, inadimplemento e demais condutas ilícitas será de competência da autoridade gestora da despesa, nos termo do § 3º, do art. 87, da Lei nº 8.666/93.

20.7. O Município poderá rescindir o contrato, independentemente de qualquer procedimento judicial, observada a legislação vigente, nos seguintes casos:

a) por infração a qualquer de suas cláusulas;
b) decretação de falência, concurso de credores, dissolução ou liquidação;
c) em caso de transferência, no todo ou em parte, das obrigações assumidas neste contrato, sem prévio e expresso aviso ao Município;
d) por comprovada deficiência no atendimento do objeto do contrato;
e) mais de 2 (duas) advertências

20.8. A autoridade gestora da despesa poderá, ainda, sem caráter de penalidade, declarar rescindido o contrato por conveniência administrativa ou interesse público, conforme disposto no artigo 79 da Lei nº 8.666/93 e suas alterações.

21. RESPONSÁVEL PELO ACOMPANHAMENTO DO FUTURO CONTRATO

Em conformidade com Art. 67 da Lei nº 8.666/93, será responsável pelo acompanhamento do contrato o Supervisor de Segurança da Informação do Departamento de Planejamento de Tecnologia da Informação da Subsecretaria de Tecnologia da Informação.

22. QUALIFICAÇÃO TÉCNICA

22.1. A proponente deverá comprovar aptidão para desempenho de atividade pertinente e compatível com o objeto da licitação através da apresentação de pelo menos 1 (um) atestado de capacidade técnica, emitido por pessoa jurídica de direito publico ou privado, que comprove a aptidão para desempenho a contento de objeto semelhante.

22.2. A proponente deverá comprovar que é fornecedor autorizada da solução antivírus fornecida, por meio de declaração emitida pelo fabricante do software antivírus.

22.3. A proponente deverá comprovar que possui pelo menos 02 (dois) profissionais certificados na solução pelo FABRICANTE, para prestação dos serviços de configuração necessários.

22.3.1. A comprovação de vínculo do profissional com o licitante poderá ser feita mediante a apresentação de um dos seguintes documentos:

22.3.1.1. Carteira de trabalho e previdência social (CTPS) do responsável técnico;
22.3.1.2. Contrato social da licitante, do qual conste o responsável técnico como integrante da sociedade;
22.3.1.3. Contrato de prestação de serviços;
22.3.1.4. Declaração de contratação futura do responsável técnico detentor do atestado apresentado, desde que acompanhada da anuência deste.

PREGÃO ELETRÔNICO nº 044/2020 - SEPLAG

ANEXO II - MINUTA DE CONTRATO

CONTRATO QUE ENTRE SI FAZEM ..... E A _____.

(deverá ser preenchido conforme orientação da Assessoria Jurídica responsável)

O (a) ....., neste ato representado por seu(ua) ....., Sr(a) . ....., brasileiro(a), casado(a), inscrito(a) no CPF nº ....., portador da CI nº ..... doravante denominado ....., com a interveniência da ..... de **.....**, neste ato representada por seu(ua) .....(a) Sr(a). ....., brasileiro(a), inscrito(a) no CPF nº ....., portador da CI nº .....e Secretaria ....., neste ato representada por seu ..... Sr. ....., brasileiro, inscrito no CPF nº ....., portador da CI nº ....., doravante denominado(s) **INTERVENIENTE(S)** e a sociedade empresária _____ _____ estabelecida à rua _____ nº ____, CNPJ nº ....., pelo seu representante infra-assinado Sr. ....., CPF nº ....., RG nº ....., doravante denominada CONTRATADA, considerando o resultado do **PREGÃO ELETRÔNICO nº ...../.....**, conforme consta do **processo** administrativo próprio **nº ...../.....**, firmam o presente contrato, obedecidas as disposições da Lei nº 8.666/93, suas alterações posteriores e as condições seguintes:

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. É objeto deste instrumento o **fornecimento de Solução de Segurança da Informação, composta por software antivírus Kaspersky Advanced Security for Business com licenças de uso para 24 (vinte e quatro) meses e suporte da CONTRATADA, incluindo, ativação, configuração, gerenciamento centralizado, garantia de atualização contínua e suporte técnico,** conforme especificações do edital e anexos do **Pregão Eletrônico nº 044/2020**, os quais integram este termo independente de transcrição por ser de conhecimento das partes.

1.1.1. Descrição do Objeto e Quantidades

Item	Descrição	Período	Quantidade
01	Renovação de licença de servidor	24 meses	01
02	Renovação de licença de uso de software antivírus corporativo	24 meses	2.700
03	Contratação de serviço de suporte técnico	24 meses	01

1.2. A empresa **CONTRATADA** deverá ser responsável pelo fornecimento das novas licenças e pela devida prestação do suporte técnico contratado.

1.3. O processo deve incluir ajustes no ambiente que forem identificados e considerados necessários.

1.4. Integra este contrato como se nele estivesse transcrito os itens elencados abaixo do Termo de Referência - **Anexo I** do Edital, assim como todas as especificações neste contidas:

a) Item 6 - Características Gerais do Software;
b) Item 7 - Smartphones e tablets;
c) Item 8 - Gerenciamento de dispositivos móveis (MDM);
d) Item 9 - Criptografia, e;
e) Item 10 - Gerenciamento de Sistemas.

CLÁUSULA SEGUNDA - DO PREÇO E DA FORMA DE PAGAMENTO

2.1. O presente contrato tem o valor global previsto de R$ ..... (.....), conforme preço registrado e quantitativos da UG, que é de pleno conhecimento das partes, sendo os valores individuais os seguintes:

ITEM	DESCRIÇÃO	PERÍODO	QTD.	VR. UNITÁRIO (R$)	VR. TOTAL (R$)
01	Renovação com *upgrade* de licença de software antivírus corporativo sendo uma das licenças para Servidor de Núcleo de Distribuição e Console de Gerenciamento do Parque Tecnológico	24 meses	2.701		
02	Serviço de suporte técnico	24 meses	01		

2.2. Deverão estar incluídos no preço, todos os insumos que o compõem, tais como as despesas com impostos, taxas, frete, seguros e quaisquer outros que incidam direta ou indiretamente sobre a execução do objeto desta licitação, sem quaisquer ônus para a Administração, e quaisquer outros que incidam sobre a avença.

2.3. O pagamento será em até 30 (trinta) dias e efetuado pela Unidade Requisitante, creditado em favor da contratada, através de ordem bancária contra a entidade bancária indicada na proposta (conforme modelo descrito abaixo), em que deverá ser efetivado o crédito:
BANCO: ..... AGÊNCIA: ..... CONTA CORRENTE: ..... LOCALIDADE: .....

2.4. Para efeito de cada pagamento a nota fiscal/fatura deverá estar acompanhada da autorização de uso da nota fiscal eletrônica, em duas vias emitidas através do site www.nfe.fazenda.gov.br, digitando a chave de acesso descrita no DANFE.

2.4.1. No caso da não apresentação da documentação de que trata o item **2.4**. ou estando o objeto em desacordo com as especificações e demais exigências do edital, fica a Unidade Requisitante autorizada a efetuar o pagamento, em sua integralidade, somente quando forem processadas as alterações e retificações determinadas, sem prejuízo da aplicação, ao fornecedor, das penalidades previstas.

2.4.2. A Unidade Requisitante poderá descontar do pagamento importâncias que, a qualquer título, lhes sejam devidas pelo fornecedor, por força da contratação.

2.4.3. Quando ocorrer a situação prevista no item **2.4.2**, não correrá juros ou atualizações monetárias de natureza qualquer, sem prejuízo de outras penalidades previstas.

2.4.4. Os documentos de cobrança deverão ser corretamente emitidos e no caso de incorreções serão devolvidos, e o prazo para o pagamento contar-se-á da data de reapresentação da nota fiscal eletrônica/fatura.

2.5. As Notas Fiscais deverão ser emitidas em moeda corrente do país.

2.5.1. Juntamente com a nota fiscal, a contratada deverá apresentar o certificado de regularidade do FGTS e a Certidão Conjunta de Débitos Relativos a Tributos Federais e à Dívida Ativa da União.

2.6. Na eventualidade de aplicação de multas, estas deverão ser liquidadas simultaneamente com parcela vinculada ao evento cujo descumprimento der origem à aplicação da penalidade.

2.7. O CNPJ da contratada constante da nota fiscal e fatura deverá ser o mesmo da documentação apresentada no procedimento licitatório.

2.8. No ato de retirada da Nota de Empenho, o fornecedor deverá fornecer os dados bancários (banco, agência e nº da conta) para depósitos referentes aos pagamentos, conforme exigência do SIAFEM.

2.9. Nenhum pagamento será efetuado ao proponente vencedor enquanto pendente de liquidação quaisquer obrigações financeiras que lhe foram impostas, em virtude de penalidade ou inadimplência, sem que isso gere direito ao pleito de reajustamento de preços ou correção monetária.

2.10. Com relação ao recolhimento de tributos na fonte sobre a prestação dos serviços descritos neste documento, o DEIN da SEPLAG-JF, informa: com relação ao recolhimento de tributos na fonte sobre a prestação de serviço de informática.

- Serviço passivo de retenção de IRRF;
- Serviço não passivo de retenção de INSS;
- Serviço não passivo de retenção de ISSQN.

2.10.1. A retenção do Imposto de Renda na Fonte e da Contribuição Previdenciária será feita em conformidade com o disposto nas Instruções Normativas/Manuais disponibilizados no site da PJF na página do Controle Interno: link: http://pjf.mg.gov.br/subsecretarias/controle_interno/legislacao.php.

2.11. DOS RECURSOS ORÇAMENTÁRIOS

2.11.1. O valor proposto para as licenças do software antivírus corporativo, incluindo, ativação, configuração, gerenciamento centralizado, garantia de atualização contínua e suporte técnico, pelo período de no mínimo 24 (vinte e quatro) meses, partirá da fonte **0100600000** de natureza **nº 3.3.90.40.36** cuja dotação é **04.126.0001.1051.0000**.

CLÁUSULA TERCEIRA - DO CONTRATO

3.1. O contrato regular-se-á, no que concerne a sua alteração, inexecução ou rescisão, pelas disposições da Lei nº 8.666, de 21 de junho de 1.993 observadas suas alterações posteriores, pelas disposições do Edital e pelos preceitos do direito público.

3.2. O contrato poderá, com base nos preceitos de direito público, ser rescindido pela autoridade gestora da despesa a todo e qualquer tempo, independentemente de interpelação judicial ou extrajudicial, mediante simples aviso, observadas as disposições legais pertinentes.

3.3. Farão parte integrante do contrato as condições previstas no Edital e na proposta apresentada pelo adjudicatário.

3.4. O contrato terá vigência de 24 (vinte e quatro) meses a partir da data de assinatura.

3.5. Ao final do período acima estipulado, poderá ser prorrogado por iguais e sucessivos períodos, através de Termo Aditivo, desde que não haja manifestação por escrito em contrário, por quaisquer das partes, no prazo de até 30 (trinta) dias antes de cada término de contrato/aditivo, ficando estabelecido que sua rescisão desobrigará as partes dos compromissos pactuados no aludido contrato.

3.6. Do reajuste do contrato:

3.6.1. O contrato poderá ter o seu valor reajustado, desde que seja observado o interregno mínimo de 01(um) ano, a contar da data da proposta, ou da data do orçamento a que a proposta se referir, conforme disposto no Decreto Municipal nº 8.542, de 09 de maio de 2005.

3.6.2. Para o reajuste do contrato será adotado como indicador o Índice de Preços ao Consumidor Amplo – IPCA, calculado pelo Instituto Brasileiro de Geografia e Estatística – IBGE, conforme disposto no Decreto Municipal nº 8.542, de 9 de maio de 2005.

3.6.3. O valor pactuado poderá ser revisto mediante solicitação da contratada, com vistas a restabelecer a equação econômico-financeira do contrato, na forma do inc. II, da alínea "d", do art. 65, da Lei nº. 8.666/93.

3.6.4. As eventuais solicitações deverão fazer-se acompanhar de comprovação de superveniência do fato imprevisível ou previsível, porém de consequências incalculáveis, bem como da demonstração analítica de seu impacto nos custos do Contrato.

CLÁUSULA QUARTA - DA ENTREGA DO PRODUTO, SUPORTE TÉCNICO DURANTE TODA A VIGÊNCIA CONTRATUAL E MANUTENÇÃO DO SOFTWARE LICENCIADO

4.1. DA ENTREGA DO PRODUTO

4.1.1. As licenças do software antivírus corporativo deverão ser confirmadas e liberadas, no máximo de 15 (quinze) dias após a emissão da ordem de serviço emitida pela Subsecretaria de Tecnologia da Informação e enviadas à SEPLAG-JF/SSTI/DPTI/SSEG, situada à Av. Brasil, 2001 - 4º andar/Centro - 36.060-010 Juiz de Fora/MG, ou para o endereço eletrônico **seginfo@pjf.mg.gov.br.**

4.2. SUPORTE TÉCNICO DURANTE TODA A VIGÊNCIA CONTRATUAL

4.2.1. As licenças de uso devem incluir suporte técnico consistindo em:

4.2.1.1. Suporte remoto, via conexão de dados segura, ou presencial, prestado pela equipe habilitada pelo fabricante do produto, com certificação na solução;

4.2.1.2. Os chamados devem ser classificados de duas maneiras: aqueles onde haja parada no ambiente consumada, iminente ou forçada a acontecer por alguma decisão técnica e, aqueles onde não haja parada do ambiente, devendo haver tratamento de urgência diferenciado para as duas situações;

4.2.1.3. O suporte **"normal"** deve ser prestado em horário comercial com prazo de início de atendimento de até 24 (vinte e quatro) horas da abertura do chamado;

4.2.1.4. O suporte **"urgente"** deve ser prestado em qualquer horário e dia da semana, com prazo de início de atendimento de até 04 (quatro) horas da abertura do chamado;

4.2.1.5. Deve ser fornecido conta de acesso ao site do fabricante, onde se possa fazer o download dos componentes da solução e suas atualizações, bem como abrir tickets de atendimento.

4.3. MANUTENÇÃO DO SOFTWARE LICENCIADO

4.3.1. ACORDO DE NÍVEIS DE SERVIÇO

4.3.1.1. Entende-se como assistência técnica às correções de defeitos, ajustes e fornecimento de *releases* e versões (atualizações) do software.

4.3.1.2. São definidos como defeitos, os erros que provoquem funcionamento diferente daquele previsto na documentação do software.

4.3.1.3. São definidos como ajustes, alterações no software que melhore o seu desempenho nas aplicações da **CONTRATANTE.**

4.3.1.4. Entende-se por "*release"* pequenos ajustes no software. Neste caso, seu número de referência é incrementado, como por exemplo: de "11.1" para "11.2".

4.3.1.5. Entende-se por "versão" uma adição substancial dos recursos do software em questão; neste caso, seu número de referência é alterado de "11.1" para "12.0".

4.3.1.6. O fornecimento de nova "*release*" ou "versão" não implicará em custo adicional para a **CONTRATANTE**.

4.3.1.7. O serviço de suporte básico será realizado mediante solicitação da **CONTRATANTE**, em regime 8X5 (segunda à sexta em horário comercial).

4.3.1.8. Os problemas encontrados no software deverão ser descritos e notificados via uma das seguintes formas de contato: fac-símile, correio eletrônico (e-mail), skype e detalhados, se possível, com informações verbais pelo telefone.

4.3.1.9. Será fornecido à **CONTRATANTE** pela **CONTRATADA**, e sem custos adicionais, novo "release" do software na ocorrência de troca de versão do sistema operacional praticada no hardware onde está instalado o software. A **CONTRATADA** providenciará o envio do novo "release" no prazo máximo de 10 (dez) dias.

4.3.1.10. Toda despesa decorrente dos treinamentos (instrutores, elaboração do material didático, deslocamento, alimentação e hospedagem dos instrutores, etc.) será de exclusiva responsabilidade da **CONTRATADA**.

4.3.1.11. Somente o corpo técnico da **CONTRATADA** ou equipe habilitada pelo fabricante do produto com certificação na solução, poderá realizar os serviços a que se refere o contrato.

4.3.1.12. Os serviços contratados não incluem a correção de defeitos do software, decorrentes do uso indevido, negligência ou imperícia dos usuários ou problemas do sistema operacional ou do hardware onde o software esteja instalado e/ou decorrentes de qualquer modificação feita no software por qualquer um que não seja a própria **CONTRATADA** ou sem o seu consentimento.

4.3.1.13. Não faz parte da cobertura visitas de técnicos da **CONTRATADA** às instalações da **CONTRATANTE**, em virtude de problemas causados por imperícia ou desconhecimento, pelos usuários, das instruções ou normas básicas de operação e funcionamento do sistema, que, quando identificados pelo técnico escalado, serão cobradas integralmente da **CONTRATANTE**, ao valor de homem/hora de análise.

4.3.1.14. Quando, comprovadamente, as falhas detectadas no software coberto, sejam de responsabilidade da **CONTRATADA**, as correspondentes correções serão feitas sem ônus à **CONTRATANTE**.

CLÁUSULA QUINTA - DAS OBRIGAÇÕES

5.1. OBRIGAÇÕES DA CONTRATANTE

5.1.1. Receber o objeto no prazo e condições estabelecidas no contrato;

5.1.2. Verificar minuciosamente, no prazo fixado, a conformidade do produto recebido com as especificações constantes no Termo de Referência e Contrato;

5.1.3. Propiciar a **CONTRATADA** as condições necessárias à perfeita execução dos serviços contratados;

5.1.4. Acompanhar, fiscalizar e atestar a execução dos serviços;

5.1.5. Anotar em registro próprio todas as ocorrências relacionadas com a execução do contrato, determinando o que for necessário à regularização dos serviços, bem como anotando faltas da **CONTRATADA** ou falhas desta na execução do objeto;

5.1.6. Efetuar contatos, especificações de demandas, acompanhamento e pareceres técnicos referentes ao contrato;

5.1.7. Remeter advertências à **CONTRATADA**, por escrito, quando os serviços não estiverem sendo prestados de forma satisfatória.

5.2. OBRIGAÇÕES DA CONTRATADA

5.2.1. A **CONTRATADA** deverá realizar diagnósticos de problemas e prestar suporte remoto, via conexão de dados segura ou presencial;

5.2.2. Entregar o objeto contratual, na forma, prazo e local previstos. Caso o atendimento não seja feito dentro do prazo, a **CONTRATADA** ficará sujeita às sanções previstas em Contrato;

5.2.3. Cumprir o Acordo de Nível de Serviço (SLA) estabelecido referente aos serviços de suporte contratados.

5.2.4. Submeter à aprovação do **CONTRATANTE** toda e qualquer alteração ocorrida nas especificações, em face de imposições técnicas, de cunho administrativo ou legal;

5.2.5. Responsabilizar-se por todos os encargos sociais, trabalhistas, previdenciários, fiscais e comerciais e tributos de qualquer espécie que venham a ser devidos em decorrência da execução deste instrumento, bem como custos relativos ao deslocamento e à estada de seus profissionais, caso existam;

5.2.6. Responsabilizar-se pelos danos causados diretamente ao **CONTRATANTE** ou a terceiros, decorrentes de sua culpa ou dolo, ação ou omissão, quando da execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento realizado pelo **CONTRATANTE**;

5.2.7. Arcar com o pagamento de eventuais multas aplicadas por quaisquer autoridades federais, estaduais e municipais, em consequência de fato a ela imputável e relacionado com esta contratação;

5.2.8. Arcar com todos os prejuízos advindos de perdas e danos, incluindo despesas judiciais e honorários advocatícios resultantes de ações judiciais, a que o **CONTRATANTE** for compelido a responder em decorrência da contratação;

5.2.9. Manter seus funcionários, quando nas dependências do **CONTRATANTE**, sujeitos às normas internas deste (segurança e disciplina), todos utilizando uniforme e crachá de identificação, porém sem qualquer vínculo empregatício com o órgão;

5.2.10. Possibilitar a fiscalização do **CONTRATANTE**, no tocante à verificação das especificações exigidas, prestando todos os esclarecimentos solicitados e atendendo às reclamações procedentes, caso ocorram;

5.2.11. Comunicar ao **CONTRATANTE**, de imediato e por escrito, qualquer irregularidade verificada durante a execução do contrato, para a adoção das medidas necessárias à sua regularização;

5.2.12. Manter durante toda a execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

5.2.13. Indicar seu preposto e respectivo substituto, que serão responsáveis pelo recebimento das demandas encaminhadas (Art. 68 da Lei n.º 8.666/93).

5.2.14. A **CONTRATADA** deverá responsabilizar-se pela confidencialidade, integridade e disponibilidade dos dados e informações custodiados em decorrência dos serviços prestados, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do **CONTRATANTE** ou de terceiros, devendo orientar seus empregados nesse sentido;

5.2.15. Os conhecimentos, dados e informações de propriedade do **CONTRATANTE**, tanto tecnológicos como administrativos, tais como: produtos, sistemas, técnicas, estratégias, métodos de operação e todos e quaisquer outros, repassados por força do objeto do contrato, constituem informação privilegiada e possuem caráter de confidencialidade;

5.2.16. Estas informações poderão ser utilizadas, só e exclusivamente, no cumprimento das cláusulas e condições estabelecidas no contrato, sendo expressamente vedado à **CONTRATADA**: utilizá-las para fins não previstos no instrumento contratual; e repassá-las a terceiros e/ou empregados não vinculados diretamente à execução do objeto contratado;

5.2.17. Fornecer, sem ônus para o **CONTRATANTE**, as atualizações e eventuais correções do software (*updates*);

5.2.18. Seguir todas as Normas, Políticas e Procedimentos de Segurança estabelecidas pelo **CONTRATANTE** para execução da Contratação, tanto nas dependências do **CONTRATANTE** como externamente;

5.2.19. Devem ser realizados também procedimentos periódicos de transferência de conhecimento, com o intuito de evitar que se crie um atraso de continuidade significativo entre os conhecimentos produzidos na execução contratual e a atualização tecnológica da equipe técnica e dos gestores, no que lhes concerne.

5.2.20. Propiciar todos os meios e facilidades necessárias à fiscalização dos serviços pela **CONTRATANTE**, cujo representante terá poderes para sustar o serviço, total ou parcialmente, a qualquer tempo, sempre que considerar a medida necessária, e recusar materiais e serviços empregados que não atendam aos termos contratuais;

5.2.21. Atender as demais condições estabelecidas no contrato.

CLÁUSULA SEXTA – DAS PENALIDADES

6.1. Os casos de inexecução do objeto deste **contrato**, erro de execução, execução imperfeita, atraso injustificado e inadimplemento, sujeitará o proponente contratado às penalidades previstas no Art. 87 da Lei nº 8.666/93, das quais destacam-se:
a) advertência;
b) multa de 0,5% (cinco décimos por cento) do valor, por dia de atraso injustificado na execução do mesmo, limitados a 30 (trinta) dias corridos, após o qual será caracterizada a inexecução total;
c) multa compensatória no valor de 5% (cinco por cento) sobre o valor total contratado;
d) suspensão temporária de participação em licitações e impedimento de contratar com o Município, no prazo de até 02 (dois) anos;
e) declaração de inidoneidade para contratar com a Administração Pública, até que seja promovida a reabilitação, facultando ao contratado o pedido de reconsideração da autoridade competente, no prazo de 10 (dez) dias da abertura de vistas ao processo.

6.2. Após o devido processo legal, as penalidades serão aplicadas pela autoridade competente que deverá comunicar a subsecretaria todas as ocorrências para fins de cadastramento e demais providências.

6.2.1. Entende-se por autoridade competente a gestora da despesa executada.

6.3. Os valores das multas aplicadas previstas nos sub-itens acima poderão ser descontados dos pagamentos devidos pela Administração.

6.4. Da aplicação das penalidades definidas nas alíneas “a”, “b”, “c” e “d” do item **6.1**, caberá recurso no prazo de (cinco) dias úteis, contados da intimação.

6.4.1. Da aplicação da penalidade definida na alínea “e” do item **6.1**, caberá pedido de reconsideração no prazo de 10 (dez) dias úteis, contados da intimação.

6.5. O recurso ou pedido de reconsideração relativo às penalidades acima dispostas será dirigido à autoridade gestora da despesa, a qual decidirá o recurso. no prazo de 05 (cinco) dias úteis e o pedido de reconsideração, no prazo de 10 (dez) dias úteis.

6.6. A aplicação de penalidades previstas para os casos de inexecução do objeto, erro de execução, execução imperfeita, atraso injustificado, inadimplemento e demais condutas ilícitas será de competência da autoridade gestora da despesa, nos termo do § 3º, do art. 87, da Lei nº 8.666/93.

6.7. O Município poderá rescindir o contrato, independentemente de qualquer procedimento judicial, observada a legislação vigente, nos seguintes casos:

a) por infração a qualquer de suas cláusulas;
b) decretação de falência, concurso de credores, dissolução ou liquidação;
c) em caso de transferência, no todo ou em parte, das obrigações assumidas neste contrato, sem prévio e expresso aviso ao Município;
d) por comprovada deficiência no atendimento do objeto do contrato;
e) mais de 2 (duas) advertências

6.8. A autoridade gestora da despesa poderá, ainda, sem caráter de penalidade, declarar rescindido o contrato por conveniência administrativa ou interesse público, conforme disposto no artigo 79 da Lei nº 8.666/93 e suas alterações.

CLÁUSULA SÉTIMA - DA FISCALIZAÇÃO E ACOMPANHAMENTO

7.1. Observado o disposto no artigo 67 da Lei Federal nº 8.666/93, o acompanhamento, a fiscalização, o recebimento e a conferência do objeto será realizada pela Unidade Requisitante ou no caso de substituição, pelo que for indicado pelo gestor da Unidade Requisitante.

7.2. A Unidade Requisitante atestará, no documento fiscal correspondente, a execução dos serviços nas condições exigidas, constituindo tal atestação requisito para a liberação dos pagamentos ao contratado.

7.2.1. O recebimento definitivo do objeto deste instrumento, somente se efetivará com a atestação referida no item anterior.

7.3. Responsável pelo acompanhamento do contrato

7.3.1. Em conformidade com Art. 67 da Lei nº 8.666/93, será responsável pelo acompanhamento do contrato o Supervisor de Segurança da Informação do Departamento de Planejamento de Tecnologia da Informação da Subsecretaria de Tecnologia da Informação.

CLÁUSULA OITAVA
DA CESSÃO

8.1. Havendo incontestável e justificado interesse público e autorização prévia e expressa da Prefeitura, o Contrato poderá ser cedido ou transferido no todo ou parcialmente.

8.1.1. A cessão do contrato poderá ocorrer independentemente da fase em que se encontrar a execução do objeto contratado, desde que o pretenso cessionário tenha participado e tenha sido habilitado na licitação. Serão convocadas as empresas por ordem de classificação obtida na licitação.

8.2. A subcontratação poderá ocorrer após autorização prévia e expressa da Prefeitura, em parte do contrato, assumindo a contratada, completa responsabilidade pela atuação dos subcontratados, que não terão qualquer vínculo com a Prefeitura.

8.3. As comunicações entre as partes, relacionadas com o acompanhamento e controle do presente contrato, serão feitas sempre por escrito.

CLÁUSULA NONA
DAS COMUNICAÇÕES

9.1. As comunicações entre as partes contratantes, relacionadas com o acompanhamento e controle do presente contrato, serão feitas sempre por escrito.

CLÁUSULA DÉCIMA – DISPOSIÇÕES GERAIS E DO FORO

10.1. Para dirimir quaisquer questões decorrentes do presente contrato, elegem as partes o Foro da Comarca de Juiz de Fora, com renúncia expressa a qualquer outro por mais privilegiado que seja.

E por estarem assim acordados, assinam este contrato os representantes das partes e as testemunhas abaixo em duas vias de igual teor;

Prefeitura de Juiz de Fora, ... de ..... de 20.....

PREFEITO
GESTOR(ES) DA(S) UG(S)
EMPRESA
Representante Legal
Cargo

Testemunha 1	**Testemunha 2**
Ass.:_____	Ass.:_____
Nome:_____	Nome:_____
C.I.:_____	C.I.:_____
C.P.F.:_____	C.P.F.:_____

PREGÃO ELETRONICO nº 044/2020 - SEPLAG

ANEXO III

MODELO DE DECLARAÇÃO DE MICROEMPRESA (ME) OU DE EMPRESA DE PEQUENO PORTE (EPP)

A empresa ....., inscrita no CNPJ sob o nº ....., por intermédio de seu representante legal Sr. (a) ....., portador do Documento de Identidade nº ....., inscrito no CPF sob o nº ..... DECLARA, sob as penas da Lei, que cumpre os requisitos legais para qualificação como ..... **(incluir a condição da empresa: Microempresa (ME) ou Empresa de Pequeno Porte (EPP))**, art. 3º da Lei Complementar nº 123/2006 e 2006 e Lei Municipal nº 12.211/2011 e que não está sujeita a quaisquer dos impedimentos do § 4º deste artigo, estando apta a usufruir do tratamento favorecido estabelecido nos artigos 42 a 49 da citada lei.

( ) Declaramos possuir restrição fiscal no(s) documento(s) de habilitação e pretendemos utilizar o prazo previsto no art. 43, § 1º da Lei Complementar nº. 123/06, para regularização, estando ciente que, do contrário, decairá o direito à contratação, estando sujeita às sanções previstas no art. 81 da Lei Federal nº 8.666/93.

(Observação: em caso afirmativo, assinalar a ressalva acima)

.....
(local e data)

.....
Assinatura, qualificação e carimbo
(representante legal)

• Declaração a ser emitida em papel timbrado, de forma que identifique a proponente.

PREGÃO ELETRÔNICO nº 044/2020 - SEPLAG

ANEXO IV

MODELO DE DECLARAÇÃO DE HABILITAÇÃO E PLENO CONHECIMENTO

A empresa ....., inscrita no CNPJ sob nº ....., sediada na ....., cidade de ....., estado ....., telefone(s) ....., e-mail para contato ....., neste ato representada pelo(a) Sr(a) …..**,** portador da Carteira de Identidade nº ….. e do CPF nº …..., declara, sob as penas da Lei, que preenche plenamente os requisitos de habilitação estabelecidos no presente Edital do **Pregão Eletrônico nº 044/2020**, assim como tem pleno conhecimento do objeto licitado e anuência das exigências constantes do Edital e seus anexos.

.....
(local e data)

.....
Assinatura, qualificação e carimbo
(representante legal)

• Declaração a ser emitida em papel timbrado, de forma que identifique a proponente.

PREGÃO ELETRÔNICO nº 044/2020 - SEPLAG

ANEXO V

MODELO DE DECLARAÇÃO DE EMPREGADOR PESSOA JURÍDICA

…....., inscrito no CNPJ nº ....., por intermédio de seu representante legal o(a) Sr(a) ....., portador da Carteira de Identidade nº ..... e do CPF nº ....., DECLARA, **sob as penas da Lei, em cumprimento ao disposto no inciso XXXIII, do art. 7º da Constituição da República**, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos.

Ressalva: emprega menor, a partir de quatorze anos, na condição de aprendiz ( )

.....
(local e data)

.....
Assinatura, qualificação e carimbo
(representante legal)

• Declaração a ser emitida em papel timbrado, de forma que identifique a proponente.

PREGÃO ELETRÔNICO nº 044/2020 - SEPLAG

ANEXO VI - DECLARAÇÃO DE INEXISTÊNCIA DE FATO IMPEDITIVO

(Nome da empresa), sediada (endereço completo), inscrita no CNPJ/MF sob o nº …....., por intermédio do seu representante legal o Sr.(a) …....., portador da Carteira de Identidade nº …..... e do CPF nº …....., **DECLARA**, sob as penas da lei, que não incorre em qualquer das condições impeditivas, especificando:

1 - Que não foi declarada inidônea por ato do Poder Público;

2 - Que não está impedida de transacionar com a Administração Pública;

3 - Que não foi apenada com rescisão de contrato, quer por deficiência dos serviços prestados, quer por outro motivo igualmente grave, no transcorrer dos últimos 5 (cinco) anos;

4 - Que não incorre nas demais condições impeditivas previstas no art. 9º da Lei Federal nº 8.666/93 consolidada pela Lei Federal nº 8.883/94.

5 - E que, se responsabiliza pela veracidade e autenticidade dos documentos oferecidos, comprometendo-se a comunicar a PREFEITURA MUNICIPAL DE JUIZ DE FORA a ocorrência de quaisquer fatos supervenientes impeditivos da habilitação, ou que comprometam a idoneidade da proponente, nos termos do artigo 32, parágrafo 2º, e do artigo 97 da Lei 8.666/93, e suas alterações.

.....
(local e data)

.....
Assinatura, qualificação e carimbo
(representante legal)

• Declaração a ser emitida em papel timbrado, de forma que identifique a proponente.