<table>
<tr><td colspan="4">EDITAL</td></tr>
<tr><td colspan="2">PREGÃO ELETRÔNICO nº 107/2024</td><td colspan="2">Data de abertura: 27/09/2024 às 09:30 hs no endereço eletrônico www.portaldecompraspublicas.com.br</td></tr>
<tr><td>Processo Administrativo nº 7.307/2024</td><td>SRP?
()Sim (X)Não</td><td>Exclusiva ME/EPP?
()Sim (X)Não</td><td>Reserva de quota ME/EPP?
()Sim (X)Não</td></tr>
<tr><td colspan="2">Objeto: Contratação de pessoa jurídica para fornecimento de Solução de Segurança da Informação, composta por software antivírus Kaspersky NEXT EDR Optmum com licenças de uso para 24 (vinte e quatro) meses e suporte da CONTRATADA por Igual período.</td><td>Marca/Modelo
(X)Sim ()Não</td><td>Margem de preferência?
()Sim (X)Não</td></tr>
<tr><td colspan="2">Valor total estimado R$ 1.189.650,00 (um milhão, cento e oitenta e nove mil e seiscentos e cinquenta reais).
Prazo para envio da proposta/documentação:
No mínimo, 2 (duas) horas após a convocação do pregoeiro.</td><td>Vistoria?
() Obrigatória
() Facultativa
(X) Não se aplica</td><td>Amostra/Demonstração?
()Sim (X)Não</td></tr>
<tr><td colspan="2">Pedidos de esclarecimento até 24//09/2024 para o endereço eletrônico: www.portaldecompraspublicas.com.br</td><td colspan="2">Impugnações até 24//09/2024 para o endereço eletrônico: www.portaldecompraspublicas.com.br</td></tr>
<tr><td colspan="4">Acompanhe as sessões públicas dos Pregões da Prefeitura de Juiz de Fora – MG pelo endereço <u>www.portaldecompraspublicas</u>, selecionando as opções Pesquisa de Processos > Objeto > Processo > Órgão > Pregões. O edital e outros anexos estão disponíveis para download no Portal de Compras Públicas e também no endereço eletrônico <u>https://www.pjf.mg.gov.br/secretarias/cpl/editais/pregao_eletronico/outros_anos.php</u>.</td></tr>
</table>

EDITAL
PREGÃO ELETRÔNICO nº 107/2024 – PJF

O Município de Juiz de Fora - MG, por meio da PJF, torna público que fará realizar licitação, sob a modalidade de **PREGÃO ELETRÔNICO**, **modo de disputa ABERTO,** pelo critério de julgamento **MENOR PREÇO GLOBAL** para a **prestação de serviço de contratação de pessoa jurídica para fornecimento de Solução de Segurança da Informação, composta por software antivírus Kaspersky NEXT EDR Optmum com licenças de uso para 24 (vinte e quatro) meses e suporte da CONTRATADA por Igual período,** devidamente descritos, caracterizados e especificados no Termo de Referência, na forma da lei.

A presente licitação se rege por toda a legislação aplicável à espécie, especialmente pelas normas de caráter geral da **Lei Federal nº 14.133/2021**, pela **Lei Complementar Federal nº 123/2006**, com as alterações promovidas pela **Lei Complementar nº 147/2014**, **Lei Municipal nº 12.211/2011**, **Decreto Municipal nº 15.635/2022**, **Decreto Municipal nº 15.610/2022** e demais legislações aplicáveis, bem como pelos preceitos de Direito Público, pelas disposições deste Edital e de seus Anexos, normas que as licitantes declaram conhecer e a elas se sujeitarem incondicional e irrestritamente.

A sessão pública do Pregão Eletrônico ocorrerá no dia 27/09/2024 às 09:30 hs, horário de Brasília – DF, no endereço eletrônico www.portaldecompraspublicas.com.br

1. DO OBJETO

1.1. O objeto da presente licitação é para a **prestação de serviço de Contratação de pessoa jurídica para fornecimento de Solução de Segurança da Informação, composta por software antivírus Kaspersky NEXT EDR Optmum com licenças de uso para 24 (vinte e quatro) meses e suporte da CONTRATADA por Igual período,** conforme as especificações constantes do Termo de Referência, **Anexo I.**

1.2. Integra este Edital, como se nele estivesse transcrito o Termo de Referência **(Anexo I)**, assim como todas as especificações neste contidas.

2. DOS RECURSOS ORÇAMENTÁRIOS

2.1. Os recursos necessários à aquisição do objeto ora licitado correrão à conta da seguinte dotação orçamentária:

Secretaria da Saúde: 10.122.0003.1208.0000 / 339040 / 1.600.00.0000
Secretaria de Transformação Digital e Administrativa: PT 04126000111880000 ND 339040 Fonte 1500000000 UG 611100
JFPREV: PT 09.128.0001.2166.0000 FONTE 1802000000 UG 343100
Secretaria de Educação: 131100 / 12.122.0007.2004.0000 / 1.5.00.001001 / 3.3.90.40
Secretaria de Mobilidade urbana: UG: 141100 / 26.122.0007.2004.0000 / 1759000000

2.2. O valor total estimado para a licitação é de **R$ 1.189.650,00 (um milhão, cento e oitenta e nove mil e seiscentos e cinquenta reais).**

3. DO CRITÉRIO DE JULGAMENTO

3.1. O critério de julgamento da presente licitação é o **menor preço global.**

4. DAS CONDIÇÕES DE PARTICIPAÇÃO

4.1. Para a participação nesta licitação é necessário que o interessado esteja credenciado regulamente junto ao Portal de Compras Públicas e Portal Nacional de Compras.

4.2. A licitante responde integralmente por todos os atos praticados no pregão eletrônico por seus representantes devidamente credenciados, assim como pela utilização da senha de acesso ao sistema, ainda que indevidamente, inclusive por pessoa não credenciada como sua representante.

4.3. Cada representante credenciado poderá representar apenas uma licitante, em cada pregão eletrônico.

4.4. O envio da proposta vinculará a licitante ao cumprimento de todas as condições e obrigações inerentes ao certame.

4.5. Não serão admitidas nesta licitação as empresas suspensas do direito de licitar, no prazo e nas condições do impedimento, e as declaradas inidôneas pela Administração Direta ou Indireta, assim como as empresas

e/ou seu sócio majoritário que tenham sido apenados com proibição de contratar com a Administração Pública, nos termos do art. 12 da Lei Federal nº 8.429/1992 e alterações posteriores.

4.6. Será permitida a participação de sociedades cooperativas, desde que apresentem a documentação de habilitação descrita no subitem 10.6.7.

4.7. Será permitida a participação em consórcio, sujeita às seguintes regras:

a) as empresas consorciadas apresentarão instrumento público ou particular de compromisso de constituição de consórcio, subscrito por todas elas, indicando a empresa líder, que será responsável principal, perante a Unidade Requisitante, pelos atos praticados pelo Consórcio, sem prejuízo da responsabilidade solidária estabelecida na alínea "d". Por meio do referido instrumento a empresa líder terá poderes para requerer, transigir, receber e dar quitação.
b) apresentação conjunta, mas individualizada, da documentação relativa à habilitação jurídica, à qualificação técnica, à qualificação econômico–financeira, à regularidade fiscal e à regularidade trabalhista. As consorciadas poderão somar seus quantitativos técnicos e econômico–financeiros, para o fim de atingir os limites fixados neste Edital relativamente à qualificação técnica e econômico–financeira. Não será admitida, contudo, a soma de índices de liquidez e endividamento, para fins de qualificação econômico–financeira;
c) as empresas consorciadas não poderão participar da licitação isoladamente, nem por intermédio de mais de um consórcio;
d) as empresas consorciadas responderão solidariamente pelos atos praticados em consórcio, tanto na fase da licitação quanto na da execução do objeto;
e) O consórcio vencedor, quando for o caso, ficará obrigado a promover a sua constituição e registro antes da aquisição.

4.8. As operações societárias promovidas por sociedades empresariais isoladamente ou por aquelas participantes de consórcio ou as alterações de composição de consórcio deverão ser submetidas à análise da Unidade Requisitante para aferição da manutenção das condições de habilitação ou verificação de suas implicações com o objeto do Contrato, que poderá ser extinto em qualquer hipótese de prejuízo ou elevação de risco para o seu cumprimento.

4.8.1. A substituição e o ingresso de consorciado deverá ser expressa e previamente autorizada pela Unidade Requisitante e será condicionada à comprovação de que a empresa substituta/ingressante preenche os requisitos exigidos para habilitação jurídica e de regularidades fiscal, social e trabalhista, além da comprovação de que o consórcio mantém, no mínimo, os quantitativos originários para efeito de habilitação técnica e os mesmos valores para efeito de qualificação econômico–financeira apresentados à ocasião do certame.

4.9. Não será permitida a participação de licitantes cujos dirigentes, gerentes, sócios ou componentes do seu quadro técnico sejam servidores da Administração Direta ou Indireta do Município, ou que o tenham sido nos últimos 180 (cento e oitenta) dias anteriores à data desta licitação. Será vedada também a participação de licitantes que possuam em seus quadros funcionais profissional que tenha ocupado cargo integrante dos 1º e 2º escalões da Administração Direta ou Indireta do Município, nos últimos 12 (doze) meses, devendo apresentar declaração de atendimento a tal requisito.

4.10. Não serão aceitas na presente licitação as licitantes que tenham participado da elaboração do(s) projeto(s) relacionado(s) ao objeto desta licitação, bem como aquelas cujo quadro técnico seja integrado por profissional que tenha atuado como autor ou colaborador do Termo de Referência.

4.11. Não será permitida a participação de licitantes que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau.

4.12. Não poderão disputar licitação ou participar da execução de contrato, direta ou indiretamente, empresas controladoras, controladas ou coligadas, nos termos da Lei Federal nº 6.404/76, concorrendo entre si, conforme o inciso V do art. 14 da Lei Federal nº 14.133/2021.

4.13. Não poderão disputar licitação ou participar da execução de contrato, direta ou indiretamente, que se enquadrem nas demais disposições do art. 14 da Lei Federal nº. 14.133, de 1º de abril de 2021.

4.14. As empresas estrangeiras que não funcionem no País deverão apresentar documentos equivalentes, visando à habilitação, na forma de regulamento emitido pelo Poder Executivo federal.

4.14.1. A empresa estrangeira, que concorrer isoladamente ou como líder de consórcio, deve informar endereço de representante em território brasileiro, com poderes para receber intimação e citação, bem como endereço eletrônico para comunicações.

4.15. Não poderão participar da licitação as pessoas físicas e jurídicas que se encontrarem em débito com a Fazenda do Município de Juiz de Fora - MG, nos termos do art. 41 do Código Tributário Municipal (Lei nº 5.546/1978).

4.16. Como condição para participação, a licitante assinalará **"sim"** ou **"não"** em campo próprio do sistema eletrônico, relativo às seguintes **Declarações**:

4.16.1. Que declara que está ciente e concorda com as condições contidas no Edital e seus anexos, bem como de que cumpre plenamente os requisitos de habilitação definidos neste Edital. (Declaração de conhecimento do Edital)

4.16.2. Que declara cumprir as exigências de reserva de cargos para pessoa com deficiência e para reabilitado de Previdência Social. (Declaração de reserva de cargos)

4.16.3. Que sob pena de desclassificação, declara que as suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas. (Declaração de proposta econômica)

4.16.4. Que declara para fins do inciso XXXIII do art. 7º da Constituição Federal, que não emprega menores de dezoito anos em trabalho noturno, perigoso ou insalubre e de que qualquer trabalho a menores de dezesseis anos. (Declaração de Não-Emprego de menores)

4.16.5. Que declara não possui em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, nos termos do inciso III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal. (Declaração de Não-Emprego de trabalho degradante)

4.16.6. Que declara, conforme disposto no art. 93 da Lei nº 8.213/91, estar ciente do cumprimento da reserve de cargos prevista em lei para pessoa com deficiência ou para trabalho da Previdência Social e que, se aplicando ao número de funcionários da minha empresa, atendo às regras de acessibilidade prevista na legislação. (Declaração de Acessibilidade)

4.16.7. Que declara sob as penas da lei, que até a presente data inexistem fatos impeditivos para sua habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores. (Declaração de Inexistência de Fato Superveniente)

4.16.8. Que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123/2006, estando apta a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49 e que não celebrou contratos com a Administração Pública cujos valores extrapolam a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte;

4.16.8.1. Nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo "não" impedirá o prosseguimento no certame;

4.16.8.2. Nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo "não" apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123/2006, mesmo que microempresa, empresa de pequeno porte.

4.17. A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

4.18. O envio da proposta vinculará a licitante ao cumprimento de todas as condições e obrigações inerentes ao certame.

5. DO CREDENCIAMENTO

5.1. O Credenciamento é o nível básico do registro cadastral no Portal de Compras Públicas que permite a participação dos interessados na modalidade licitatória pregão em sua forma eletrônica.

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

5.1.2. A perda da senha ou a quebra do sigilo deverão ser comunicadas imediatamente ao provedor do sistema para imediato bloqueio do acesso.

5.2. O cadastro deverá ser feito pelo licitante no Portal de Compras Públicas, acessando o endereço eletrônico www.portaldecompraspublicas.com.br.

5.3. 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.

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

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

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

6. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

6.1. Os licitantes encaminharão, **exclusivamente por meio do sistema**, a proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para recebimento das propostas, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.

6.1.1. As propostas de preço serão ofertadas com base no **menor preço global** do objeto licitado.

6.2. O envio de proposta, assim como dos documentos de habilitação, quando solicitados, ocorrerá por meio de chave de acesso e senha.

6.2.1. O licitante melhor classificado deverá apresentar a documentação de habilitação em campo próprio no sistema, a partir da solicitação do Pregoeiro no sistema eletrônico. O Pregoeiro não poderá estabelecer prazo inferior a **2 (duas) horas** para a apresentação da documentação.

6.3. As licitantes poderão retirar ou substituir suas propostas inseridos no sistema, até a abertura da sessão pública da presente licitação, no dia e horário estabelecido.

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

6.3.2. Os documentos complementares à proposta, quando necessários à confirmação daqueles exigidos no edital e já apresentados, serão encaminhados pelo licitante melhor classificado após o encerramento do envio de lances, em formato digital.

6.3.3. O pregoeiro poderá, no julgamento das propostas, sanar erros ou falhas que não alterem a substância das propostas, mediante decisão fundamentada, registrada em ata e acessível aos licitantes, e lhe atribuirá validade e eficácia para fins de classificação.

6.4. No preço proposto serão computadas todas as despesas para a entrega do(s) bem(ns), incluindo a totalidade dos custos diretos e indiretos do objeto da presente licitação, constituindo obrigação da CONTRATADA o pagamento dos salários de todos os seus empregados e respectivos encargos sociais, trabalhistas, previdenciários e securitários, bem como todos os tributos, encargos fiscais e comerciais decorrentes da execução do contrato, inclusive seguros, multas, e outras despesas relacionadas ao objeto da licitação e quaisquer despesas extras e necessárias não especificadas neste Edital, mas julgadas essenciais ao cumprimento do objeto desta licitação.

6.5. O valor total da proposta, acrescido dos valores devidos a título de contribuição previdenciária, na forma do item anterior, será considerado apenas para efeito de comparação com o valor das propostas apresentadas pelas demais licitantes, no momento do seu julgamento.

6.5.1. O valor devido título de contraprestação pela execução dos serviços será obtido mediante a dedução do valor total da proposta do montante do valor devido a título de contribuição previdenciária, o qual deverá ser recolhido à entidade competente, na forma da legislação.

6.5.2. Os **custos indiretos**, relacionados com as despesas de manutenção, utilização, reposição, depreciação e impacto ambiental do objeto licitado, entre outros fatores vinculados ao seu ciclo de vida, poderão ser considerados para a definição do menor dispêndio, sempre que objetivamente mensuráveis, conforme disposto em regulamento.

6.6. Nenhuma reivindicação para pagamento adicional será considerada se decorrer de erro ou má interpretação do objeto licitado ou deste Edital. Considerar–se–á que os preços propostos são completos e suficientes para pagar todos os serviços.

6.7. A licitante deverá remeter a proposta de preços devidamente adequada aos preços ofertados na fase competitiva em arquivo único compactado, no curso da sessão pública, quando solicitada a fazê–lo pelo Pregoeiro.

6.8. As licitantes arcarão com todos os custos relativos à apresentação das suas propostas. A Unidade Requisitante em nenhuma hipótese, será responsável por tais custos, quaisquer que sejam os procedimentos seguidos na licitação ou os seus resultados.

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

6.10. A licitante que se enquadre como microempresa ou empresa de pequeno porte e que queira usufruir do tratamento privilegiado assegurado pela Lei Complementar Federal nº 123/2006, deverá manifestar, em campo próprio do sistema eletrônico, que cumpre os requisitos previstos no referido diploma legal, especialmente no seu art. 3º, sob as penas da lei, em especial do art. 299 do Código Penal.

6.10.1. A falta da declaração de enquadramento da licitante como microempresa ou empresa de pequeno porte não conduzirá ao seu afastamento da licitação, mas tão somente dos benefícios da Lei Complementar Federal nº 123/2006.

6.10.2. A declaração falsa de enquadramento da licitante como microempresa ou empresa de pequeno porte implicará a sua inabilitação quando a falsidade for constatada no curso do certame, sem prejuízo das penalidades cabíveis.

7. DO PREENCHIMENTO DA PROPOSTA

7.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico de processamento do certame, dos seguintes campos:

7.1.1. Valor total do item;

7.1.2. Marca, quando for o caso;

7.1.3. Descrição do objeto, contendo as informações similares à especificação do Termo de Referência;

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

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

7.4. 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.

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

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

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

7.8. O prazo de validade da proposta não será inferior a **90 (noventa) dias corridos**, a contar da data de sua apresentação.

7.9. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelos órgãos de controle e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

8. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

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

8.2. Os licitantes poderão retirar ou substituir a proposta, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

8.2.1. 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 em sentido contrário, levado a efeito na fase de aceitação.

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

8.4. No caso de diligência, será disponibilizado no sistema um 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 de sistema eletrônico de processamento do certame, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

8.6. O lance deverá ser ofertado pelo **valor total do grupo.**

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

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

8.9. 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 indicado pelo pregoeiro.

8.10. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema de processamento do certame, na hipótese de lance inconsistente ou inexequível.

8.11. O procedimento seguirá de acordo com o modo de disputa adotado.

8.12. Será adotado para o envio de lances no pregão eletrônico o **modo de disputa aberto**. Os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

8.12.1. 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.

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

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

8.12.4. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, podendo ser auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

8.12.5. Após o reinício previsto no item supra, os licitantes serão convocados para apresentar lances intermediários.

8.13. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances na seguinte forma:

8.13.1. Na ordem crescente, quando adotado o critério de julgamento por menor preço; ou

8.13.2. Na ordem decrescente, quando adotado o critério de julgamento por maior desconto.

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

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. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, quando encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno

porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

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

8.19.2. A melhor classificada nos termos do subitem 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.

8.19.3. 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.

8.19.4. 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.

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

8.20.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto na ordem do art. 60 da Lei nº 14.133, de 2021.

8.20.2. Para fins do item **8.20.1**, o Pregoeiro poderá abrir diligências para solicitar a documentação dos licitantes empatados, nos moldes do art. 60 da Lei nº 14.133, de 2021.

8.21. Definido o resultado do julgamento, a Administração poderá negociar condições mais vantajosas com o primeiro colocado

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

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

8.21.3. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

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

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

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

9. JULGAMENTO DAS PROPOSTAS E DIREITO DE PREFERÊNCIA

9.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação.

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

9.3. Constatada a existência de sanção, nos moldes legais, o licitante será reputado inabilitado, por falta de condição de participação.

9.4. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

9.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício.

9.6. Verificadas as condições de participação e de utilização do tratamento favorecido, o Pregoeiro/Agente de Contratação 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 artigo 29 a 35 da IN SEGES nº 73, de 30 de setembro de 2022.

9.7. Será desclassificada a proposta vencedora que:

9.7.1. Contiver vícios insanáveis;

9.7.2. Não obedecer às especificações técnicas contidas no Termo de Referência;

9.7.3. Apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

9.7.4. Não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

9.7.5. Apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

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

9.8.1. A inexequibilidade, na hipótese de que trata o item **9.8**, só será considerada após diligência, provocada pelo Pregoeiro ao setor técnico adequado, que comprove:

9.8.1.1.que o custo do licitante ultrapassa o valor da proposta; e

9.8.1.2. Inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

10. DA HABILITAÇÃO

10.1. O julgamento da habilitação se processará mediante o exame dos documentos a seguir relacionados, os quais dizem respeito à:
a) Documentação relativa à habilitação jurídica;
b) Documentação relativa à habilitação econômica–financeira;
c) Documentação relativa à habilitação fiscal;
d) Documentação relativa à habilitação social e trabalhista;
e) Documentação relativa à qualificação técnica.

10.1.1. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Agente de Contratação verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos documentos inseridos no Portal de Compras Públicas, e ainda nos seguintes cadastros:

10.1.1.1. Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e o Cadastro Nacional de Empresas Punidas (CNEP);

10.1.1.2. Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça (CNJ);

10.1.1.3. Lista de Inidôneos, mantida pelo Tribunal de Contas da União (TCU).

10.1.2. Para fins de habilitação, será observado o preenchimento “sim ou não”, em campo próprio do sistema eletrônico, das declarações constantes nos subitens do item 4.16 deste Edital.

10.2. Não serão aceitos como documentação hábil a suprir exigências deste Edital pedidos de inscrição, protocolos, cartas ou qualquer outro documento que visem a substituir os exigidos, exceto nos casos admitidos pela legislação.

10.3. Se os Certificados, Declarações, Registros e Certidões não tiverem prazo de validade declarado no próprio documento, da mesma forma que não conste previsão em legislação específica, os referidos documentos deverão ter sido emitidos há, no máximo, **90 (noventa) dias**, contados até a data da realização da licitação.

10.4. O pregoeiro poderá, no julgamento da habilitação, sanar erros e falhas que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível aos licitantes, e lhes atribuirá validade e eficácia para fins de habilitação.

10.5. Na hipótese de necessidade de suspensão da sessão pública para a realização das diligências, com vistas ao saneamento de que trata o item **10.4**, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, **24 (vinte e quatro) horas de antecedência**, e a ocorrência será registrada em ata.

10.6. Da Habilitação Jurídica:

10.6.1. Registro comercial, no caso de empresário individual;

10.6.2. Estatuto ou Contrato Social em vigor, devidamente registrado, com chancela digital na forma eletrônica ou tradicional, em se tratando de sociedades empresárias, acompanhado dos documentos de designação de seus administradores, caso designados em ato separado;

10.6.3. Inscrição do ato constitutivo, no caso de sociedade simples, acompanhada da prova da composição da diretoria em exercício.

10.6.3.1. A sociedade simples que não adotar um dos tipos societários regulados no Código Civil deverá mencionar no respectivo ato constitutivo as pessoas naturais incumbidas de sua administração, exceto se assumir a forma de sociedade cooperativa.

10.6.4. A prova da investidura dos administradores da sociedade limitada eventualmente designados em ato separado do Contrato Social, mediante termo de posse no livro de atas da Administração e averbação no registro competente.

10.6.5. Decreto de autorização, em se tratando de empresa 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.

10.6.6. Na hipótese de existir alteração nos documentos citados acima posteriormente à constituição da sociedade, os referidos documentos deverão ser apresentados de forma consolidada, contendo todas as cláusulas em vigor.

10.6.7. As sociedades cooperativas deverão fornecer os seguintes documentos, de forma atualizada e consolidada:

10.6.7.1. Ato constitutivo;

10.6.7.2. Estatuto acompanhado da ata da Assembleia que o aprovou;

10.6.7.3. Regimento interno acompanhado da ata da Assembleia que o aprovou;

10.6.7.4. Regimentos dos fundos instituídos pelos cooperados acompanhados das atas das Assembleias que os aprovaram;

10.6.7.5. Atas das Assembleias Gerais em que foram eleitos os dirigentes e conselheiros da cooperativa;

10.6.7.6. Registro de presença dos cooperados nas 03 (três) últimas Assembleias Gerais;

10.6.7.7. Ata da sessão em que os cooperados autorizam a cooperativa a contratar o objeto deste certame, acompanhada dos documentos comprobatórios da data de ingresso de cada qual na cooperativa.

10.7. Da Habilitação Econômica-Financeira:

10.7.1. Balanço patrimonial e Demonstração do Resultado do Exercício (demonstrações contábeis) dos 2 (dois) últimos exercícios sociais, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta.

10.7.2. A capacidade Financeira da Sociedade Empresária será avaliada mediante os seguintes indicadores, das demonstrações contábeis do último exercício social.

a) Índice de Liquidez Geral (ILG) igual ou maior que 1 (um).

$$ILG = \frac{\text{ATIVO CIRCULANTE + REALIZÁVEL A LONGO PRAZO}}{\text{PASSIVO CIRCULANTE + PASSIVO NÃO CIRCULANTE}}$$

b) Índice de Liquidez Corrente (ILC) igual ou maior que 1 (um).

$$ILC = \frac{\text{ATIVO CIRCULANTE}}{\text{PASSIVO CIRCULANTE}}$$

10.7.2.1. Para a capacidade econômico-financeira exigida, os participantes deverão atender obrigatoriamente, os seguintes requisitos:
ILC ..... maior ou igual a 1(um)
ILG ..... maior ou igual a 1(um)

10.7.3. Serão considerados aceitos como na forma da lei o Balanço Patrimonial (inclusive o de abertura) e Demonstração do Resultado do Exercício que apresentem valores dos 2 (dois) últimos exercício, conforme art. 176, § 1º da Lei 6.404/76 e inciso I do art. 69 da Lei 14.133/2021 e 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 pelo órgão responsável.

10.7.3.1. Quando se tratar de sociedade constituída a menos de um ano, essa deverá apresentar apenas o balanço de abertura, o qual deverá conter a identificação legível e assinatura do responsável contábil da empresa, devidamente registrado no Conselho Regional de Contabilidade – CRC, bem como ser devidamente autenticado na Junta Comercial da sede ou domicílio da licitante ou em outro órgão equivalente;

10.7.3.2. Quando se tratar de sociedade constituída há menos de dois anos, os documentos referidos limitar–se–ão ao último exercício.

10.7.4. O licitante que não alcançar os índices acima exigidos, deverá comprovar que possui patrimônio líquido mínimo igual ou superior a 10% (dez por cento) do valor estimado para a contratação. A comprovação será obrigatoriamente feita pelo balanço patrimonial (Demonstrações contábeis do último exercício social), já exigíveis e apresentados na forma da lei.

10.7.4.1. Será exigido do consórcio licitante um acréscimo de 10% sobre o valor exigido de licitante individual para fins de habilitação econômico–financeira, conforme o § 1º do art. 15 da Lei Federal nº 14.133/2021.

10.7.5. 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.

10.7.5.1. 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.

10.8. Da Habilitação Fiscal:

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

10.8.2. Prova de inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicílio ou sede da licitante, pertinente à atividade empresarial objeto desta licitação.

10.8.3. 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.

10.8.4. Prova de regularidade para com a Fazenda Estadual;

10.8.5. Prova de regularidade para com a Fazenda Municipal;

10.8.5.1. 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.

10.8.5.2 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.

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

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

10.8.8. 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;

10.8.8.1. 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.

10.8.8.2. A não regularização da documentação no prazo estipulado implicará a decadência do direito à contratação, sem prejuízo do disposto no art. 90, § 5º, da Lei Federal nº 14.133/2021.

10.9. Documentação relativa à habilitação social e trabalhista:

10.9.1. Certidão Negativa de Débitos Trabalhistas – CNDT ou Certidão Positiva de Débitos Trabalhistas com efeito negativo.

10.10. Da Qualificação Técnica:

10.10.1. 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 público ou privado, que comprove a aptidão para desempenho a contento de objeto semelhante.

10.10.2. Não será admitida a apresentação de atestado de capacidade técnica emitido por empresa ou empresas do mesmo grupo econômico em favor da licitante participante, no caso desta também pertencer ao grupo econômico.

10.10.3. Os atestados ou certidões recebidas estão sujeitos à verificação do Pregoeiro e da sua Equipe de Apoio quanto à veracidade dos respectivos conteúdos, inclusive para os efeitos previstos nos arts. 169, § 3º, II, da Lei Federal nº 14.133/2021, e 337–F do Código Penal.

10.10.4. Comprovação de aptidão para o fornecimento de bens similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado.

10.10.5. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

10.10.6. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

10.10.7. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

10.10.8. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

10.10.9. Apresentar no mínimo 01 (um) atestado de Capacidade Técnica, expedido por pessoa jurídica de direito público ou privado, comprovando a execução de serviços técnicos em fornecimento e implantação de ambiente similar.

10.10.10. No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente.

10.10.11. É facultado à CONTRATANTE solicitar o contrato social das empresas envolvidas para dirimir quaisquer dúvidas referentes ao exposto acima.

10.10.12. O(s) atestado(s) ou documento(s) poderá(ão) ser objeto de diligências a fim de esclarecer quaisquer dúvidas quanto ao seu conteúdo, tipificação dos serviços executados, inclusive com verificação dos respectivos expedientes que lhe deram origem, visitas ao local etc.

10.10.13. Em atendimento ao Art. 67 da Lei 14.133 de 2021 em consonância com a Lei 4.769/65, nos casos onde os serviços prestados pelas empresas licitantes se enquadrarem no Art. 2º alíneas a e b da Lei 4.769/65 e com o Art. 3º do regulamento aprovado pelo Decreto 61.934/67, os mesmos deverão ser seguidos

11. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

11.1. 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:

11.1.1. 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 ou seu representante legal.

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

11.2. 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.

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

11.3. Os preços devem ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso.

11.3.1. 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.

11.4. 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.

11.5. 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.

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

12. DO RECURSO

12.1. Divulgada a vencedora, o Pregoeiro informará aos licitantes, por meio de mensagem lançada no sistema, que poderão manifestar a intenção de interpor recurso, em campo próprio do sistema, no prazo concedido na sessão pública.

12.2. As licitantes que manifestarem o interesse em recorrer terão o prazo de 3 (três) dias úteis para apresentação das razões do recurso, sendo facultado às demais licitantes a oportunidade de apresentar contrarrazões no mesmo prazo, contado a partir do dia do término do prazo da recorrente, sendo–lhes assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses.

12.3. A apresentação das razões e das contrarrazões dos recursos deverá ser realizada, única e exclusivamente, em campo próprio do sistema eletrônico, observados os prazos estabelecidos no item anterior.

12.4. Os recursos serão dirigidos ao Pregoeiro, que poderá reconsiderar seu ato no prazo de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata, nos moldes do art. 165 da Lei Federal nº. 14.133, de 1º de abril de 2021.

12.4.1. Poderá ocorrer pedido de reconsideração, no prazo de 3 (três) dias úteis, contado da data de intimação, relativamente a ato do qual não caiba recurso hierárquico, nos moldes do inciso II, do art. 165 da Lei Federal nº. 14.133, de 1º de abril de 2021.

12.5. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente e o acolhimento do recurso importará a invalidação dos atos insuscetíveis de aproveitamento.

12.6. Decididos os recursos e constatada a regularidade dos atos praticados, a autoridade competente adjudicará o objeto da licitação à licitante vencedora e homologará o procedimento licitatório.

13. DA ADJUDICAÇÃO, HOMOLOGAÇÃO E CONTRATAÇÃO

13.1. Encerradas as fases de julgamento e habilitação, e exauridos os recursos administrativos, o processo licitatório será encaminhado à autoridade superior, que poderá adjudicar o objeto e homologar a licitação.

13.2. Integra o presente Edital, a minuta do Contrato cujas disposições disciplinarão as relações entre a Unidade Requisitante e a ADJUDICATÁRIA.

13.3. O fornecimento dos bens que tiverem seus preços registrados na Ata de Registro de Preços será solicitado pelo CONTRATANTE mediante convocação da ADJUDICATÁRIA, por meio de publicação no Diário Oficial do Município ou de comunicação formal, com antecedência mínima de 2 (dois) dias úteis, para assinatura do contrato ou para retirada de instrumento equivalente, ciente de que deverá comparecer no endereço informado, podendo, na impossibilidade de comparecimento do seu representante legal, enviar mandatário munido da respectiva procuração, por instrumento público ou particular, com firma reconhecida, e da via original do documento de identidade e do cartão do Cadastro de Pessoas Físicas – CPF do outorgado, conferindo–lhe poderes específicos para a assinatura de contrato administrativo ou para a retirada de instrumento equivalente.

13.3.1. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação da parte durante seu transcurso, devidamente justificada, e desde que o motivo apresentado seja aceito pela Unidade Requisitante.

13.3.2. Nas contratações de grande vulto, o licitante vencedor deverá comprovar a implantação de programa de integridade, no prazo de 6 (seis) meses, contado da celebração do contrato, na forma do § 4º do art. 25 da Lei Federal nº 14.133/2021.

13.4. Deixando a ADJUDICATÁRIA de assinar o Contrato ou a Ata de Registro de Preços (ARP) ou de retirar o instrumento equivalente no prazo assinalado, poderá o Pregoeiro, independentemente da aplicação das sanções administrativas à faltosa, examinar as ofertas subsequentes e a qualificação das licitantes por ordem de classificação, e assim, sucessivamente, observado o direito de preferência para as microempresas e empresas de pequeno porte, até a apuração de uma que atenda ao contido neste Edital, sendo a respectiva licitante declarada vencedora.

13.5. A ADJUDICATÁRIA deverá comprovar, no momento da assinatura do Contrato ou da ARP ou da retirada do instrumento equivalente, a manutenção das condições demonstradas para habilitação no Edital.

13.6. A CONTRATADA será responsável, na forma do Contrato ou da ARP, pela qualidade dos serviços que são objeto desta licitação, em conformidade com as especificações do termo de referência e/ou dos projetos,

com as normas da Associação Brasileira de Normas Técnicas – ABNT, e demais normas técnicas pertinentes, a ser atestada pelo responsável da fiscalização quanto à execução do contrato.

13.6.1.A ocorrência de desconformidade implicará na substituição dos materiais recusados, por outro, que será substituído, sem ônus para a Unidade Requisitante e sem prejuízo da aplicação das sanções cabíveis.

13.7. A CONTRATADA será também responsável, na forma do Contrato, por todos os ônus, encargos e obrigações comerciais, tributárias, previdenciárias e trabalhistas, e por todos os danos e prejuízos que, a qualquer título, causar a terceiros, especialmente, mas não limitado, aos concessionários de serviços públicos, em virtude da execução do objeto contratado, respondendo por si, seus empregados, prepostos e sucessores.

13.8. No momento da assinatura do Contrato ou da retirada do instrumento equivalente, a ADJUDICATÁRIA deverá apresentar, quando couber, relação nominal de seus empregados, com a devida documentação comprobatória, demonstrando cumprir o disposto nas políticas de inclusão estabelecidas na legislação em vigor.

13.9. O Contrato vigorará a partir da assinatura até 24 (vinte e quatro) meses.

13.10. O prazo de execução dos serviços poderá ser prorrogado ou alterado nos termos da Lei Federal nº 14.133/2021.

13.10.1. No caso de serviços e fornecimentos contínuos, o contrato poderá ser prorrogado na forma dos arts. 107 e 106, §2º, da Lei Federal nº 14.133/2021, e das demais normas aplicáveis.

14. DO CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

14.1. Observado o disposto no Art. 117 da Lei nº 14.133/2014, o acompanhamento, a fiscalização, o recebimento e a conferência do objeto, serão realizados por fiscal designado lotado na Unidade Requisitante e demais regramentos previstos no Termo de Referência, **que segue anexo e faz parte deste Edital. (Item 22 do Anexo I)**

15. DA ENTREGA E CRITÉRIO DE ACEITAÇÃO DO OBJETO

15.1. As regras sobre entrega e critério de aceitação do objeto constam no Termo de Referência, **que segue anexo e faz parte deste Edital. (Itens 4 e 5 do Anexo I)**

16. DAS OBRIGAÇÕES

16.1. Da Unidade Requisitante:

16.1.1. As regras sobre as obrigações da Unidade Requisitante constam no Termo de Referência, **que segue anexo e faz parte deste Edital. (Item 19.1 do Anexo I)**

16.2. Da licitante vencedora:

16.2.1. Respeitar todas as condições impostas pela legislação para a execução do serviço, além das exigências e padrões definidos no Termo de Referência.

16.2.2. As regras sobre as obrigações da licitante vencedora constam no Termo de Referência, **que segue anexo e faz parte deste Edital. (Itens 19.2 ao 19.6 do Anexo I)**

17. DAS SANÇÕES ADMINISTRATIVAS

17.1. A recusa da adjudicatária em assinar o termo de contrato ou em retirar o instrumento equivalente dentro do prazo estabelecido caracteriza o descumprimento total das obrigações assumidas, independentemente do disposto no subitem 13.4, sujeitando–a às penalidades previstas em lei e no Termo de Referência, **que segue anexo e faz parte deste Edital. (Item 23 do Anexo I)**

17.1.1. As regras sobre as sanções administrativas são aquelas impostas por lei e constam no Termo de Referência, **que segue anexo e faz parte deste Edital. (Item 23.4 do Anexo I)**

17.2. A personalidade jurídica poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos nesta Lei ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, a pessoa jurídica sucessora ou a empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o sancionado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

18. DO PAGAMENTO

18.1. Os pagamentos deverão ser efetuados após a regular liquidação da despesa, nos termos do art. 63 da Lei Federal nº 4.320/64, observado o disposto no art. 141 da Lei Federal nº 14.133/2021.

18.1.1. As regras sobre pagamento constam no Termo de Referência, **que segue anexo e faz parte deste Edital. (Item 21 do Anexo I)**

18.2. A contratada deverá apresentar juntamente com o documento de cobrança, os comprovantes de recolhimento do FGTS e INSS de todos os empregados atuantes no contrato, assim como Certidão Negativa de Débitos Trabalhistas – CNDT ou Certidão Positiva de Débitos Trabalhistas com efeito negativo válida, declaração de regularidade trabalhista.

18.3. Do reajuste:

18.3.1. Em casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

$$I = \frac{}{(TX/100)}$$

365
EM= I

x N x VP

Onde:
I = índice de atualização financeira;
TX = percentual da taxa de juros de mora anual;
EM = encargos moratórios
N = número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = valor da parcela em atraso.

18.3.2. Para a hipótese definida no item anterior, a Licitante Vencedora fica obrigada a emitir fatura suplementar, identificando de forma clara que se trata de valor pertinente à atualização financeira originária de pagamento de fatura em atraso por inadimplemento da Unidade Requisitante.

18.3.3. O ISSQN, se devido, será recolhido, na forma do Código Tributário Municipal vigente e da Lei 10.630 de 30.12.03, caso não haja comprovação do recolhimento junto ao Município sede da contratada.

18.3.4. 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.

19. DO PREÇO, DO REAJUSTAMENTO EM SENTIDO ESTRITO E DO REEQUILÍBRIO ECONÔMICO DO CONTRATO

19.1. Os preços contratados serão fixos e irreajustáveis, pelo período de 12 (doze) meses a partir da data da apresentação da Proposta Comercial.

19.2. O valor do contrato será fixo e irreajustável, porém poderá ser corrigido anualmente mediante requerimento da contratada, após o interregno mínimo de um ano, contado a partir da data da apresentação da proposta, pelo IPCA, tomando-se por base a data da apresentação da proposta.

19.3. A periodicidade do reajuste é anual, aplicado somente aos pagamentos de valores referentes a eventos físicos realizados a partir do 1° (primeiro) dia imediatamente subsequente ao término do 12º (décimo segundo) mês e, assim, sucessivamente, contado desde a data da apresentação da proposta e de acordo com a vigência do contrato.

19.4. Após a aplicação do reajuste nos termos deste documento, o novo valor da parcela ou saldo contratual terá vigência e passará a ser praticado, pelo próximo período de 01 (um) ano, sem reajuste adicional e, assim, sucessivamente, durante a existência jurídica do contrato.

19.4.1. Nos reajustes subsequentes ao primeiro, o intervalo mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

19.5. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

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

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

19.5.3. Na ausência de previsão legal quanto ao índice substituto, caberá à Administração indicar novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

19.6. O reajuste será realizado por apostilamento.

19.7. Para restabelecer o equilíbrio econômico-financeiro inicial do contrato em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução do contrato tal como pactuado, respeitada, em qualquer caso, a repartição objetiva de risco estabelecida no contrato.

19.7.1. Para fins do reequilíbrio econômico financeiro do contrato, as partes devem apresentar solicitação, anexando planilha detalhada dos custos do objeto, fazendo um comparativo com a composição dos custos para obtenção dos preços inicialmente contratados e planilha dos custos para fins do reequilíbrio econômico do contrato.

19.8. A extinção do contrato não configurará óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório.

19.8.1. O pedido de restabelecimento do equilíbrio econômico-financeiro deverá ser formulado durante a vigência do contrato e antes de eventual prorrogação nos termos do art. 107 da Lei 14.133/2021.

20. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

20.1. Até 03 (três) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa poderá impugnar este Edital e/ou apresentar pedido de esclarecimento.

20.2. A impugnação e/ou pedido de esclarecimento deverão ser feitos exclusivamente por forma eletrônica no sistema, no endereço eletrônico www.portaldecompraspublicas.com.br.

20.3. A resposta à impugnação ou ao pedido de esclarecimento será divulgada no Portal de Compras Públicas no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

20.4. Acolhida a impugnação, que implique em eventual modificação no edital, culminará na definição e publicação de nova data para a realização do certame, desde que a alteração não comprometa a formulação das propostas.

20.5. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame, salvo quando se amolda ao art. 55, parágrafo 1º, da Lei nº 14.133/2021.

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

20.6. As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a administração.

20.7. As respostas às impugnações e aos esclarecimentos solicitados, bem como outros avisos de ordem geral, serão cadastradas no endereço eletrônico **www.portaldecompraspublicas.com.br**, sendo de responsabilidade dos licitantes, seu acompanhamento.

20.8. A petição de impugnação apresentada por empresa deve ser firmada por aquele que tem poderes de representação com login e senha no sistema de operacionalização do certame.

21. DAS DISPOSIÇÕES GERAIS

21.1. Será divulgada ata da sessão pública no sistema eletrônico.

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

21.3. No julgamento das propostas e da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

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

21.5. No período de vigência da Ata de Registro de Preços, a Administração terá a faculdade de contratar ou não o fornecimento dos bens.

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

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

21.8. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do começo e incluir-se-á o do vencimento, observadas as disposições do art. 183 da Lei Federal nº 14.133/2021.

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

21.10. O licitante é o responsável pela fidelidade e legitimidade das informações prestadas e dos documentos apresentados em qualquer fase da licitação.

21.10.1. A falsidade de qualquer documento apresentado ou a inverdade das informações nele contidas implicará a imediata desclassificação do proponente que o tiver apresentado, ou, caso tenha sido o vencedor, a rescisão do contrato ou do documento equivalente, sem prejuízo das demais sanções cabíveis.

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

21.12. A Autoridade Competente, poderá revogar esta licitação por razões de interesse público decorrente de fato superveniente que constitua óbice manifesto e incontornável, ou anulá-lo por ilegalidade, de ofício ou por provocação de terceiros, salvo quando for viável a convalidação do ato ou do procedimento viciado, desde que observados os princípios da ampla defesa e contraditório.

21.12.1. A anulação da licitação induz à extinção do contrato.

21.12.2. A anulação da licitação por motivo de ilegalidade não gera obrigação de indenizar.

21.13. É facultado ao pregoeiro, em qualquer fase desta licitação, promover diligência destinada a esclarecer ou completar a instrução do processo.

21.14. Fica eleito o Foro do Município de Juiz de Fora - MG para dirimir quaisquer dúvidas oriundas do presente Edital, renunciando as partes desde já a qualquer outro, por mais especial ou privilegiado que seja.

21.15. Esclarecimentos em relação a eventuais dúvidas de interpretação do presente Edital poderão ser obtidos junto a Subsecretaria de Licitações e Compras pelo telefone: (32) 3690-8188/8187, nos dias úteis no horário das 09 às 11 horas ou 15 às 17 horas.

21.16. Os casos omissos relativos à aplicabilidade do presente Edital serão sanados pela Subsecretaria de Licitações e Compras, obedecida a legislação vigente.

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

21.18. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

Anexo I - Termo de Referência.
Anexo I.A – Estudo Técnico Preliminar
Anexo II – Minuta de Contrato.

Juiz de Fora-MG, data da assinatura eletrônica,

(GESTOR DA UNIDADE REQUISITANTE)

PREGÃO ELETRÔNICO nº 107/2024 – PJF

ANEXO I

TERMO DE REFERÊNCIA

1. ÓRGÃO SOLICITANTE

Secretaria de Transformação Digital e Administrativa - STDA

2. OBJETO

Contratação de pessoa jurídica para fornecimento de Solução de Segurança da Informação, composta por software antivírus Kaspersky NEXT EDR Optmum com licenças de uso para 24 (vinte e quatro) meses e suporte da CONTRATADA por Igual período.

O(s) serviço(s) objeto desta contratação são caracterizados como comuns, uma vez que os padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado.

O fornecedor será selecionado por meio da realização de procedimento de licitação, na modalidade pregão, sob a forma eletrônica, com critério de julgamento pelo menor preço global por grupo de itens e o modo de disputa será aberto.

O prazo de vigência da contratação é de 24 (vinte e quatro) meses contados da assinatura, prorrogável para até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

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.

O serviço é enquadrado como continuado tendo em vista que é imprescindível, pelas razões já detalhadas no Estudo Técnico Preliminar, que a Prefeitura de Juiz de Fora (doravante PJF) disponha de uma ferramenta robusta e reconhecida pelo mercado para, não apenas proteger o parque tecnológico de ameaças digitais, mas também possibilitar o controle do ambiente dentro da infraestrutura atual, atendendo as demandas internas a fim de garantir a segurança cibernética nos ativos de tecnológicos da PJF.

3. JUSTIFICATIVA DE NECESSIDADE DA CONTRATAÇÃO

Com um crescente número de ataques cibernéticos cada vez mais especializados, a contratação de uma solução de segurança de *endpoints* para estações de trabalhos, servidores, dispositivos móveis, dentre outros, é imprescindível à proteção cibernética de qualquer parque tecnológico, 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 a esses malefícios. Assim, uma nova contratação d*a versão* atualizada do ***software antivírus Kaspersky Advanced Security for Business*** que, após uma revisão de produtos da fabricante, passou a ser nomeada de ***Kaspersky NEXT EDR OPTIMUM*** e teve funcionalidades de detecção e resposta inseridas em seu escopo, dará continuidade a proteção já padronizada no parque tecnológico da PJF. A utilização de uma ferramenta conceituada no mercado e já em utilização nesta Prefeitura desde 2017, faz-se necessária para garantir a integridade, confiabilidade e segurança das informações contra ações de programas maliciosos que ponham em risco a segurança cibernética, preservando as estações de trabalho, equipamentos servidores, *laptops* e dispositivos móveis de toda a PJF contra as diversas ameaças digitais da atualidade.

Nos últimos anos vivenciamos uma onda crescente de ataques cibernéticos, seja em órgãos públicos ou na iniciativa privada, houve também a instituição de novas legislações que tangenciam a proteção de dados e tudo isso nos traz a necessidade de uma ferramenta confiável, robusta e eficaz de proteção.
A solução atualmente em operação na PJF, mantida pelo fabricante *Kaspersky é* uma das mais conceituadas do mercado, reconhecida por especialistas da área como uma das tecnologias de software mais indicadas para o uso corporativo, visto as facilidades para gerenciamento centralizado e suporte a diversas plataformas de servidores, estações de trabalho e dispositivos móveis.
A pretendida contratação é relevante, pois mantém a administração de todo o parque tecnológico otimizada, 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, console de gerenciamento em Nuvem própria (o que desonera a contratante no quesito infraestrutura) e ferramenta de acesso remoto com área de trabalho compartilhada (o que possibilita que outros setores da Subsecretaria de Governança Digital (SSGD) também utilizem a ferramenta em seus respectivos atendimentos, reduzindo assim os custos de solução adicional).
Um outro fator fundamental diz respeito a PJF já utilizar a tecnologia do fabricante ***Kaspersky*** há cerca de 7 (sete) anos, com aproximadamente **3.200** (três mil e duzentas) 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 (62 links de dados, incluindo diversas Unidades Básicas de Saúde – UBS - serviços críticos - operando com baixa capacidade de transmissão - 4 Mbps, o que dificulta 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 (estações de trabalho com sistema operacional Windows nas versões 7, 10 e 11; estações de trabalho com sistema operacional Linux).

Em virtude da aquisição de novos computadores para a modernização do parque e ampliação dos serviços online viabilizados pelos sistemas de gestão integrados (GRP) nesta Prefeitura e da Lei Geral de Proteção de Dados[1] (LGPD), vislumbramos a necessidade de seguir com a versão da

[1] www.planalto.gov.br, LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 29/01/2020

solução equivalente à que temos hoje (a atual foi descontinuada pelo fabricante), uma vez que possuirá ainda mais funcionalidades para o monitoramento da segurança da rede corporativa e para que não haja incompatibilidade com o ambiente já existente. Vale ressaltar também que a continuidade da solução preserva os investimentos realizados desde 2017, aproveitando o nível de maturidade já adquirido pela equipe no uso da solução, evitando-se assim desperdício de tempo e recursos em fazer uma nova instalação completa em todo o parque tecnológico, reduzindo o escopo da implantação para uma reconfiguração dos agentes nos *endpoints* e obtendo assim custos menores.

Além das justificativas apresentadas acima, manter uma solução de *endpoint* robusta e eficaz também se faz necessário em face da ausência de suporte e atualização de segurança da empresa **Microsoft** para o sistema operacional **Windows 7** do fim do suporte e atualização de segurança para o sistema operacional **Windows 10**, que ainda estão presentes em muitas máquinas da PJF. Enquanto não realizamos a atualização de todos os computadores para o sistema operacional **Windows 11**, 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. 41, inc. I da Lei 14.133 de 2021**, 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 Next EDR Optimum*** tem como finalidade precípua evitar desperdício de tempo (alta curva de aprendizado) e recursos na instalação completa de uma nova solução que não fosse da fabricante ***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.

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

Os serviços, licenças e console de gerenciamento a serem fornecidos pela CONTRATADA serão

realizados e entregues mediante ordem de serviço – OS e, sendo o caso, durante a sua prorrogação, nos moldes permitidos pelo art. 106, parágrafo 2º, da Lei nº 14.133/2021.
A categorização dos serviços segue abaixo:

- **Serviços de Prestação Instantânea**: Planejamento do projeto, instalação do sistema, migração de dados dos sistemas atualmente em uso, implantação, configuração e parametrização do sistema em seus ambientes de produção e homologação, treinamento e operação assistida (reconfiguração do ambiente pós implantação e alguns atendimentos do suporte operacional e técnico).

- **Serviços de Prestação Continuada:** Licença de uso, atualizações, reconfigurações e suporte operacional e técnico. Migração de regras e tarefas já criadas e aplicadas no âmbito da PJF.

4.1. SUPORTE OPERACIONAL E TÉCNICO DURANTE TODA A VIGÊNCIA CONTRATUAL

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

4.1.1.1. Suporte operacional e suporte técnico remoto, via conexão de dados segura, prestado pela equipe habilitada pelo fabricante do produto, com certificação na solução;

4.1.2. ACORDO DE NÍVEIS DE SERVIÇO

4.1.2.1. Entende-se como suporte a assistência técnica às correções de falhas, ajustes e fornecimento de *releases* e versões (atualizações) do software; apoio e mitigação de falhas críticas no ambiente em relação a proteção fornecida pelos endpoints.

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

4.1.2.3. São definidos como ajustes, alterações no software (atualização de versões) que melhorem o seu desempenho no ambiente da **CONTRATANTE;**

4.1.2.4. 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";

4.1.2.5. 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";

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

4.1.2.7. O serviço de suporte básico será realizado mediante solicitação da **CONTRATANTE**, em regime 24X7 a fim de salvaguardar a CONTRATANTE em situações consideradas

críticas (como ataque de *Ramsonwere* por exemplo).

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

4.1.2.9. 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 após o seu lançamento;

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

4.1.2.11. 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 este termo;

4.1.2.12. 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;

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

4.1.2.14. 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;

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

4.1.2.16. 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;

4.1.2.17. 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 chamados de atendimento

4.2. TREINAMENTO

4.2.1. Será necessário treinamento reduzido, focado nas novas funcionalidades, à equipe que

atuará com a solução. O treinamento deverá ser de no mínimo 8 (oito) horas de duração, podendo variar a critério da CONTRATADA em comum acordo com a CONTRATANTE a fim de garantir que o conteúdo apresentado supra as necessidades da CONTRATADA quanto à transferência de conhecimento das novidades funcionais do software em relação a versão atualmente em utilização na PJF.

4.2.2. Após a configuração do ambiente em nuvem da console a CONTRATADA será responsável pelo treinamento dos usuários designados pela CONTRATANTE.

4.2.3. Esta etapa deverá ser realizada remotamente, focando nas novas funcionalidades da console em nuvem e diferenças entre o novo ambiente e o ambiente on-premise (MMC) que existe hoje na PJF. em datas e horários definidos em comum acordo entre as partes.

4.2.4. A **CONTRATADA** deverá definir o conteúdo programático e o quantitativo do treinamento necessário à capacitação e transferência de conhecimento ao público-alvo, fixando a carga horária e o número de encontros, considerando as novas funcionalidades disponíveis na console de gerenciamento da solução.

5. CARACTERÍSTICAS DO SOFTWARE

5.1. Do módulo de proteção de endpoint

5.1.1. A solução proposta deverá proteger os sistemas operacionais abaixo:

5.1.1.1. Windows 7
5.1.1.2. Windows 8
5.1.1.3. Windows 8.1
5.1.1.4. Windows 10
5.1.1.5. Windows 11

5.1.2. Servidores:

5.1.2.1. Windows Small Business Server 2011
5.1.2.2. Windows MultiPoint Server 2011
5.1.2.3. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022
5.1.2.4. Servidores de terminal Microsoft

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

5.1.4. Sistemas operacionais Linux de 32 bits:

5.1.4.1. CentOS 6.7 e posterior
5.1.4.2. Debian GNU/Linux 11.0 e posterior
5.1.4.3. Debian GNU/Linux 12.0 e posterior
5.1.4.4. Red Hat Enterprise Linux 6.7 e posterior

5.1.5. Sistemas operacionais Linux de 64 bits:

5.1.5.1. Amazon Linux 2.
5.1.5.2. CentOS 6.7 e mais tarde
5.1.5.3. CentOS 7.2 e posterior.
5.1.5.4. CentOS Stream 8.
5.1.5.5. CentOS Stream 9.
5.1.5.6. Debian GNU/Linux 11.0 e posterior.

5.1.5.7. Debian GNU/Linux 12.0 e posterior.
5.1.5.8. Linux Mint 20.3 e superior.
5.1.5.9. Linux Mint 21.1 e posterior.
5.1.5.10. OpenSUSE Leap 15.0 e posterior.
5.1.5.11. Oracle Linux 7.3 e posterior.
5.1.5.12. Oracle Linux 8.0 e posterior.

5.1.5.13. Oracle Linux 9.0 e posterior.
5.1.5.14. Red Hat Enterprise Linux 6.7 e posterior
5.1.5.15. Red Hat Enterprise Linux 7.2 e posterior.
5.1.5.16. Red Hat Enterprise Linux 8.0 e posterior.
5.1.5.17. Red Hat Enterprise Linux 9.0 e posterior.
5.1.5.18. Rocky Linux 8.5 e posterior.
5.1.5.19. Rocky Linux 9.1.
5.1.5.20. SUSE Linux Enterprise Server 12.5 ou posterior.
5.1.5.21. SUSE Linux Enterprise Server 15 ou posterior.
5.1.5.22. Ubuntu 20.04 LTS.
5.1.5.23. Ubuntu 22.04 LTS.
5.1.6. Sistemas operacionais Arm de 64 bits:
5.1.6.1. CentOS Stream 9.
5.1.6.2. SUSE Linux Enterprise Server 15.
5.1.6.3. Ubuntu 22.04 LTS.
5.1.7. Sistemas operacionais MAC OS:
5.1.7.1. macOS 12 – 14
5.1.8. Ferramentas de virtualização MAC OS:
5.1.8.1. Parallels Desktop 16 para Mac Business Edition
5.1.8.2. VMware Fusion 11.5 Profissional
5.1.8.3. VMware Fusion 12 Profissional
5.1.9. A solução proposta deverá suportar as seguintes plataformas virtuais:
5.1.9.1. VMware Workstation 17.0.2 Pro
5.1.9.2. VMware ESXi 8.0 Update 2
5.1.9.3. Microsoft Hyper-V Server 2019
5.1.9.4. Citrix Virtual Apps e Desktop 7 2308
5.1.9.5. Citrix Provisioning 2308
5.1.9.6. Citrix Hypervisor 8.2 Update 1

5.2. Do módulo de gerenciamento avançado

5.2.1. A solução proposta deve suportar arquitetura cloud-native e on-premisse;
5.2.2. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:
5.2.2.1. Amazon Web Services
5.2.2.2. Microsoft Azure
5.2.3. A solução proposta deve incluir as seguintes opções de integração SIEM:
5.2.3.1. HP (Microfoco) ArcSight
5.2.3.2. IBM QRadar
5.2.3.3. Splunk
5.2.3.4. Kaspersky KUMA
5.2.4. A solução proposta deve fornecer a capacidade de integração com as soluções

Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

5.2.5. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;

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

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

5.2.8. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

5.2.9. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

5.2.10. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.

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

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

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

5.2.14. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em um único/múltiplos dispositivos com base nas seguintes regras de ativação:

5.2.14.1. Status do dispositivo

5.2.14.2. Tag

5.2.14.3. Diretório ativo

5.2.14.4. Proprietários de dispositivos

5.2.14.5. Hardware

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

5.2.15.1. E-mail

5.2.15.2. Registro de sistema

5.2.15.3. SMS

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

5.2.16.1. Atributos de rede

5.2.16.2. Nome

5.2.16.3. Domínio e/ou Sufixo de Domínio

5.2.16.4. Endereço de IP

5.2.16.5. Endereço IP para servidor de gerenciamento

5.2.16.6. Localização no Active Directory

5.2.16.7. Unidade organizacional

5.2.16.8. Grupo

5.2.16.9. Sistema operacional

5.2.16.10. Número do pacote de serviço

5.2.16.11. Arquitetura Virtual

5.2.16.12. Registro de aplicativos
5.2.16.13. Nome da Aplicação
5.2.16.14. Versão do aplicativo
5.2.16.15. Fabricante
5.2.16.16. Tipo e versão
5.2.16.17. Arquitetura

5.2.17. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.

5.2.18. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.

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

5.2.19.1. Dispositivos Desktop/Servidores
5.2.19.2. Dispositivos móveis
5.2.19.3. Dispositivos de rede
5.2.19.4. Dispositivos virtuais
5.2.19.5. Componentes OEM
5.2.19.6. Periféricos de computador
5.2.19.7. Dispositivos IoT conectados
5.2.19.8. Telefones VoIP
5.2.19.9. Repositórios de rede

5.2.20. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:

5.2.20.1. Nome da Aplicação
5.2.20.2. Caminho do aplicativo
5.2.20.3. Metadados do aplicativo
5.2.20.4. Aplicativo Certificado digital
5.2.20.5. Categorias de aplicativos predefinidas pelo fornecedor
5.2.20.6. SHA256 e MD5

5.2.21. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:

5.2.21.1. Bluetooth
5.2.21.2. Dispositivos móveis
5.2.21.3. Modems externos
5.2.21.4. CD/DVD
5.2.21.5. Câmeras e scanners
5.2.21.6. MTPs
5.2.21.7. E a transferência de dados para dispositivos móveis

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

5.2.23. A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.

5.2.24. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

5.2.24.1. Estruturas de domínios e grupos de trabalho do Windows

5.2.24.2. Estruturas de grupos do Active Directory

5.2.24.3. Conteúdo de um arquivo de texto criado manualmente pelo administrador

5.2.25. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.

5.2.26. A solução proposta deve permitir realizar as seguintes ações para endpoints:

5.2.26.1. Verificação manual;

5.2.26.2. Verificação no acesso;

5.2.26.3. Verificação por demanda;

5.2.26.4. Verificação de arquivos compactados

5.2.26.5. Verificação de arquivos individuais, pastas e unidades;

5.2.26.6. Bloqueio e verificação de scripts

5.2.26.7. Proteção contra alteração de registros;

5.2.26.8. Proteção contra estouro de buffer;

5.2.26.9. Verificação em segundo plano/inativa

5.2.26.10. Verificação de unidade removível na conexão com o sistema;

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

5.2.28. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.

5.2.29. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.

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

5.2.31. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.

5.2.32. A solução proposta deve suportar Windows Failover Cluster.

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

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

5.2.35. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.

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

5.2.37. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.

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

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

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

5.2.41. A solução proposta deve contar com filtragem de firewall por endereço local,

interface física e Time-To-Live (TTL) de pacotes.

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

5.2.43. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo especifico de prevenção de intrusão.

5.2.44. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.

5.2.45. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).

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

5.2.47. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.

5.2.48. A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.

5.2.49. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.

5.2.50. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.

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

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

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

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

5.2.55. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.

5.2.56. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal. .

5.2.57. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.

5.2.58. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante

um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.

5.2.59. A solução proposta deve permitir ao administrador personalizar relatórios.

5.2.60. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.

5.2.61. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.

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

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

5.2.64. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.

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

5.2.66. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;

5.2.67. O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.

5.2.68. A solução proposta deve suportar integração com solução APT.

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

5.2.70. A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:

5.2.71. Windows

5.2.72. Linux

5.2.73. A solução proposta deverá suportar os seguintes servidores de banco de dados:

5.2.73.1. Windows:

5.2.73.2. Microsoft SQL Server

5.2.73.3. Microsoft Banco de dados SQL do Azure

5.2.73.4. MySQL Standard e Enterprise

5.2.73.5. MariaDB

5.2.73.6. PostgreSQL

5.2.74. Linux:

5.2.74.1. MySQL

5.2.74.2. MariaDB

5.2.74.3. PostgreSQL

5.2.75. A solução proposta deverá suportar as seguintes plataformas virtuais:

5.2.75.1. Windows:

5.2.75.2. VMware vSphere 6.7 e 7.0

5.2.75.3. Estação de trabalho VMware 16 Pro

5.2.75.4. Servidor Microsoft Hyper-V 2012 de 64 bits

5.2.75.5. Servidor Microsoft Hyper-V 2012 R2 de 64 bits

5.2.75.6. Microsoft Servidor Hyper -V 2016 de 64 bits
5.2.75.7. Servidor Microsoft Hyper-V 2019 de 64 bits
5.2.75.8. Servidor Microsoft Hyper-V 2022 de 64 bits
5.2.75.9. Citrix XenServer 7.1 LTSR
5.2.75.10. Citrix XenServer 8.x
5.2.75.11. Oracle VM VirtualBox 6.x

5.2.76. Linux:
5.2.76.1. VMware vSphere 6.7, 7.0 e 8.0
5.2.76.2. VMware Desktop 16 Pro e 17 Pro
5.2.76.3. Servidor Microsoft Hyper-V 2012 de 64 bits
5.2.76.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
5.2.76.5. Microsoft Servidor Hyper -V 2016 de 64 bits
5.2.76.6. Servidor Microsoft Hyper-V 2019 de 64 bits
5.2.76.7. Servidor Microsoft Hyper-V 2022 de 64 bits
5.2.76.8. Citrix XenServer 7.1 e 8.x
5.2.76.9. Oracle VM VirtualBox 6.x e7.x

5.2.77. A solução proposta deve suportar criptografia em vários níveis:
5.2.77.1. Criptografia completa do disco – incluindo disco do sistema
5.2.77.2. Criptografia de arquivos e pastas
5.2.77.3. Criptografia de mídia removível
5.2.77.4. Gerenciamento de criptografia BitLocker e MacOS Filevault2

5.2.78. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:
5.2.78.1. A criptografia de arquivos em unidades de computador locais.
5.2.78.2. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões.
5.2.78.3. A criação de listas criptografadas de pastas em unidades de computador locais.

5.2.79. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:

5.2.80. Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis.

5.2.81. Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.

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

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

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

5.2.85. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a

arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados

para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado.

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

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

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

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

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

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

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

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

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

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

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

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

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

5.2.99. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:

5.2.99.1. Uso do Trusted Platform Module e configurações de senha.

5.2.99.2. Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível.

5.2.99.3. Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets).

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

5.2.101. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:

5.2.101.1. Instalação remota de software de terceiros

5.2.101.2. Relatórios sobre software e hardware existentes

5.2.101.3. Monitoramento para instalação de software não autorizado

5.2.101.4. Remoção de software não autorizado

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

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

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

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

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

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

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

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

5.2.110. A solução proposta deve permitir ao administrador aprovar atualizações.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.2.135. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:

5.2.135.1. Inicie a instalação ao reiniciar ou desligar o computador.

5.2.135.2. Instale o gerador necessário todos os pré-requisitos do sistema.

5.2.135.3. Permitir a instalação de novas versões de aplicativos durante as atualizações.

5.2.135.4. Baixe atualizações para o dispositivo sem instalá-las.

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

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

5.2.137. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:

5.2.137.1. CEF;

5.2.137.2. LEEF;

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

5.2.139. O relatório da solução proposta deve conter informações CVE.

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

5.3. Do módulo de gerenciamento simplificado

5.3.1. A solução proposta deve suportar arquitetura cloud;

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

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

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

5.3.5. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.

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

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

5.3.8. A solução proposta deve incluir informações do endpoint:

5.3.8.1. IP público de internet;

5.3.8.2. IP interno do dispositivo;

5.3.8.3. Versão do agente de proteção;

5.3.8.4. Ultima comunicação com a console, contendo data e hora;

5.3.8.5. Informações do sistema operacional;

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

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

5.3.11. A solução proposta deve incluir treinamento em segurança cibernética.

5.4. Requisitos gerais

5.4.1. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:

5.4.1.1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.

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

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

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

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

5.4.6. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

5.4.6.1. Proteção contra ameaças sem arquivos (Fileless);

5.4.6.2. Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

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

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

5.4.9. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.

5.4.10. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.

5.4.11. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.

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

5.4.13. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.

5.4.14. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:

5.4.14.1. Controles de aplicativos,

5.4.14.2. Controle web e dispositivos

5.4.14.3. HIPS e Firewall

5.4.14.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;

5.4.14.5. Gerenciamento de criptografia de arquivos e discos;

5.4.14.6. Controle adaptativo para detecção de anomalias;

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

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

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

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

5.4.18. A solução proposta deve incluir um módulo capaz, no mínimo, de:

5.4.18.1. Bloqueio de aplicativos com base em sua categorização.

5.4.18.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.

5.4.19. A adição de sub-redes e a modificação de permissões de atividade.

5.4.20. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.

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

5.4.22. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.

5.4.23. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:

5.4.23.1. Modo silencioso;

5.4.23.2. Discos rígidos e dispositivos removíveis;

5.4.23.3. De todos as contas de usuários do dispositivo.

5.4.23.4. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:

5.4.23.4.1. Exclusão imediata de dados;

5.4.23.4.2. Exclusão de dados adiada.

5.4.24. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:

5.4.24.1. Excluir usando os recursos do sistema operacional - os arquivos são excluídos;

5.4.24.2. Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.

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

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

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

5.4.28. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.

5.4.29. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.

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

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

5.4.32. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;

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

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

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

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

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

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

5.4.39. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.

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

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

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

5.4.43. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário

aos recursos da web com base nos sites e tipo de conteúdo.

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

5.4.45. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;

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

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

5.4.48. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.

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

5.4.50. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.

5.4.51. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.

5.4.52. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.

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

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

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

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

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

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

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

5.4.60. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.

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

5.4.62. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:

5.4.62.1. Filtro de anexos.

5.4.62.2. Verificação de mensagens de email ao receber, ler e enviar.

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

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

5.4.65. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.);

5.4.66. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.

5.4.67. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.

5.4.68. A solução proposta deve incluir suporte ao protocolo IPv6.

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

5.4.70. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:

5.4.71. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.

5.4.72. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.

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

5.4.74. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.

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

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

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

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

5.4.79. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.

5.4.80. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia , bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.

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

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

5.4.83. A solução proposta deve permitir a instalação de software com funcionalidades de anti- malware e detecção e resposta de incidente a partir de um único pacote de distribuição.

5.4.84. A solução proposta deve suportar endereços IPv6.

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

5.4.86. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.

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

5.4.88. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.

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

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

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

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

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

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

5.4.95. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.

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

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

5.4.98. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado.

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

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

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

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

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

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

5.4.105. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.

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

5.4.107. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.

5.4.108. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo

adicional.

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

5.4.110. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:

5.4.110.1. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.

5.4.110.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.

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

5.4.112. A solução proposta deve gerar relatórios de vulnerabilidades encontradas nos dispositivos com sensor de endpoint instalado.

5.5. Do modulo de gerenciamento de dispositivos móveis

5.5.1. O modulo deve ser integrado a console de gerenciamento;

5.5.2. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

5.5.2.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)

5.5.3. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

5.5.3.1. iOS 10–17 ou iPadOS 13–17

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

5.5.5. A solução proposta deve suportar dispositivos iOS supervisionados.

5.5.6. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.

5.5.7. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.

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

5.5.9. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).

5.5.10. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.

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

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

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

5.5.14. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:

5.5.14.1. Dados em contêineres

5.5.14.2. Contas de e-mail corporativo

5.5.14.3. Configurações para conexão à rede Wi-Fi corporativa e VPN
5.5.14.4. Nome do ponto de acesso (APN)
5.5.14.5. Perfil do Android for Work
5.5.14.6. Recipiente KNOX
5.5.14.7. Chave do gerenciador de licença KNOX

5.5.15. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:
5.5.15.1. Todos os perfis de configuração instalados
5.5.15.2. Todos os perfis de provisionamento
5.5.15.3. O perfil iOS MDM
5.5.15.4. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas

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

5.5.17. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:

5.5.18. Critérios de verificação do dispositivo;

5.5.19. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;

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

5.5.21. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:
5.5.21.1. Cartões de memória e outras unidades removíveis
5.5.21.2. Câmera do dispositivo
5.5.21.3. Conexões Wi-Fi
5.5.21.4. Conexões Bluetooth
5.5.21.5. Porta de conexão infravermelha
5.5.21.6. Ativação do ponto de acesso Wi-Fi
5.5.21.7. Conexão de área de trabalho remota
5.5.21.8. Sincronização de área de trabalho
5.5.21.9. Definir configurações da caixa de correio do Exchange
5.5.21.9.1. Configurar caixa de e-mail em dispositivos iOS MDM
5.5.21.9.2. Configure contêineres Samsung KNOX.
5.5.21.9.3. Definir as configurações do perfil do Android for Work
5.5.21.9.4. Configurar e-mail/calendário/contatos
5.5.21.9.5. Defina as configurações de restrição de conteúdo de mídia. **5.5.21.9.6.** Definir configurações de proxy no dispositivo móvel **5.5.21.9.7.** Configurar certificados e SCEP

5.5.22. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay .

5.5.23. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:

5.5.23.1. Google Play, Huawei App Gallery e Apple App Store

5.5.23.2. Portal de inscrição móvel KNOX

5.5.23.3. Pacotes de instalação pré-configurados independentes

5.5.24. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.

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

5.5.26. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:

5.5.26.1. VMware AirWatch 9.3 ou posterior

5.5.26.2. MobileIron 10.0 ou posterior

5.5.26.3. IBM MaaS360 10.68 ou posterior

5.5.26.4. Microsoft Intune 1908 ou posterior

5.5.26.5. SOTI MobiControl 14.1.4 (1693) ou posterior

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

5.5.28. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:

5.5.28.1. Google Play

5.5.28.2. Galeria de aplicativos Huawei

5.5.28.3. Loja de aplicativos da Apple

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

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

5.5.31. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.

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

5.5.33. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.

5.5.34. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.

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

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

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

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

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

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

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

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

5.6. Do módulo de EDR

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

5.6.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.

5.6.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;

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

5.6.5. Deve apresentar informações detalhadas contendo:

5.6.5.1. Usuário que executou a ação;

5.6.5.2. Informações acesso privilegiado;

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

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

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

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

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

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

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

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

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

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

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

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

5.6.18. A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para

monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC.

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

5.6.20. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:

5.6.21. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).

5.6.22. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.

5.6.23. Informações gerais sobre a detecção, incluindo modo de detecção.

5.6.24. Alterações no registro associadas à detecção.

5.6.25. Histórico da presença de arquivos no dispositivo.

5.6.26. Ações de resposta executadas pela aplicação.

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

5.6.28. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:

5.6.28.1. Processo

5.6.28.2. Conexões de rede

5.6.28.3. Alterações no registro

5.6.28.4. Detalhes do download de objeto

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

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

5.6.29. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:

5.6.29.1. Impedir a execução de objetos

5.6.29.2. Isolamento de host

5.6.29.3. Excluir objeto do host ou grupo de hosts

5.6.29.4. Encerrar um processo no dispositivo

5.6.29.5. Colocar um objeto em quarentena

5.6.29.6. Execute a verificação do sistema

5.6.29.7. Execução remota de programa/processo/comando

5.6.29.8. Iniciar a varredura IoC para um grupo de hosts.

5.7. Requisitos para documentação da solução.

5.7.1. A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:

5.7.1.1. Ajuda on-line para administradores

5.7.1.2. Ajuda on-line para melhores práticas de implementação

5.7.1.3. Ajuda on-line para proteção de servidores de administração

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

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

6. PLANEJAMENTO DO PROJETO

6.1. Configuração do Ambiente

6.1.1. A **CONTRATADA**, deverá disponibilizar o ambiente em nuvem própria pré-configurada para a utilização da CONTRATANTE já com as licenças aplicadas.

6.1.2. A configuração das regras, bem como remoção dos *endpoints* atuais e instalação dos novos com apontamento para a nova console será de responsabilidade da **CONTRATADA** com a devida transferência de conhecimento para a **CONTRATANTE**.

7. ESTIMATIVA DE PREÇO E DISPONIBILIDADE ORÇAMENTÁRIA E FINANCEIRA PARA DESPESAS

7.1.1. Estima-se que o montante em torno dos gastos em contratações será de R$1.189.650,00, haja vista a estimativa de gastos apontada na tabela abaixo.

ITEM	ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Licenças Kaspersky Next EDR Optimum por 24 Meses.	Licença	3.500	R$289,90	R$1.014.650, 00
2	Suporte operacional e suporte técnico especializado da contratada, por 24 meses Modalidade 24x7 remoto.	Mês	24	R$140.000,0 0	R$140.000,00
3	Implantação e configuração em nuvem própria (remoção dos atuais *endpoints* e instalação dos novos).	Serviço	1	R$23.000,00	R$23.000,00

4	Treinamento remoto do tipo hands-on no produto Kaspersky Next EDR Optimum para até 2 (duas) pessoas.	Turma	1	R$12.000,00	R$12.000,00

7.1.2. A despesa com o objeto em questão correrá à conta das seguintes dotações orçamentárias:

- Secretaria da Saúde: 10.122.0003.1208.0000 / 339040 / 1.600.00.0000
- Secretaria de Transformação Digital e Administrativa: PT 04126000111880000 ND 339040 Fonte 1500000000 UG 611100
- JFPREV: PT 09.128.0001.2166.0000 FONTE 1802000000 UG 343100
- Secretaria de Educação: 131100 / 12.122.0007.2004.0000 / 1.5.00.001001 / 3.3.90.40
- Secretaria de Mobilidade urbana: UG: 141100 / 26.122.0007.2004.0000 /1759000000

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

8.1. FORMA DE SELEÇÃO E CRITÉRIO DE JULGAMENTO DA PROPOSTA

8.1.1. O fornecedor será selecionado por meio da realização de procedimento, modalidade, forma, e critério, estabelecidos no item 2 deste termo.

8.1.2. As exigências de Habilitação jurídica, fiscal, social e trabalhista encontrar-se-ão dispostas em edital, sendo aquelas dispostas nos limites da Lei 14.133/2021.

8.2. QUALIFICAÇÃO TÉCNICA

8.2.1. Comprovação de aptidão para o fornecimento de bens similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado.

8.2.2. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

8.2.3. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

8.2.4. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

8.2.5. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

8.2.6. Apresentar no mínimo 01 (um) atestado de Capacidade Técnica, expedido por pessoa jurídica de direito público ou privado, comprovando a execução de serviços técnicos em fornecimento e implantação de ambiente similar.

8.2.7. No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente.

8.2.8. É facultado à CONTRATANTE solicitar o contrato social das empresas envolvidas para dirimir quaisquer dúvidas referentes ao exposto acima.

8.2.9. O(s) atestado(s) ou documento(s) poderá(ão) ser objeto de diligências a fim de esclarecer quaisquer dúvidas quanto ao seu conteúdo, tipificação dos serviços executados, inclusive com verificação dos respectivos expedientes que lhe deram origem, visitas ao local etc.

8.2.10. Em atendimento ao Art. 67 da Lei 14.133 de 2021 em consonância com a Lei 4.769/65, nos casos onde os serviços prestados pelas empresas licitantes se enquadrarem no Art. 2º alíneas a e b da Lei 4.769/65 e com o Art. 3º do regulamento aprovado pelo Decreto 61.934/67, os mesmos deverão ser seguidos.

8.3. ACEITE DO OBJETO

8.3.1. Havendo o aceite da proposta quanto ao valor, o interessado classificado provisoriamente em primeiro lugar deverá apresentar declaração emitida pelos provedores, assegurando ser capaz de prover os serviços objetos desta contratação durante toda a vigência do contrato – Por 24 (vite e quatro) meses.

8.3.2. No caso de não apresentação da declaração no item 10.1.1 a proposta será recusada.

9. REQUISITOS DA CONTRATAÇÃO

9.1. REQUISITOS OBRIGATÓRIOS DA CONTRATANTE

9.1.1. Receber o objeto no prazo e condições estabelecidas neste Termo de Referência;

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

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

9.1.4. 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;

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

9.1.6. Remeter advertências à **CONTRATADA**, por escrito, quando os serviços não estiverem

sendo prestados de forma satisfatória.

9.2. REQUISITOS OBRIGATÓRIOS DA CONTRATADA

9.2.1. Fornecer acesso à console de forma ininterrupta durante todo o tempo de duração do contrato, ficando proibida a expiração do sistema, ou qualquer tipo de redução de funcionalidade, em tempo inferior ao contratado.

9.2.2. A **CONTRATADA** deverá comprovar que é fornecedora autorizada da solução de segurança fornecida, por meio de declaração emitida pelo fabricante do software antivírus.

9.2.3. A **CONTRATADA** deverá apresentar pelo menos 01 (um) atestado de capacidade técnica fornecido por pessoa jurídica pública ou privada comprovando aptidão para o fornecimento e suporte em características, quantidades e prazos compatíveis com o objeto deste Termo de Referência.

9.2.4. A **CONTRATADA** deverá comprovar que possui pelo menos 01 (um) profissional certificado na solução pelo FABRICANTE, para prestação dos serviços de configuração necessários.

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

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

9.2.7. Cumprir o Acordo de Nível de Serviço (SLA) estabelecido neste Termo de Referência. Refente aos serviços de suporte contratados. Item 7.2 deste termo.

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

9.2.9. 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;

9.2.10. 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**;

9.2.11. 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;

9.2.12. 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 desta contratação;

9.2.13. 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;

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

9.2.15. 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;

9.2.16. Manter, durante toda a vigência do contrato, as condições de habilitação (comprovações de capacidade técnica e demais documentações apresentadas no ato da habilitação), consignadas neste Termo de Referência;

9.2.17. 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, observando as legislações vigentes que tangenciam a proteção de dados como a Lei Geral de Proteção de dados (LGPD – Lei N. 13.709/2018), por exemplo.

9.2.18. 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**;

9.2.19. 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;

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

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

9.2.22. 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.

9.2.23. 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;

9.2.24. Atender as demais condições estabelecidas no contrato.

9.3. REQUISITOS DE SEGURANÇA

9.3.1. Deverá ser possível ter um controle de acesso de forma parametrizada, possuindo a definição de perfis de utilização individuais ou de grupos, para que cada usuário ou grupo de usuários possa, ou não, ter acesso a determinados módulos, funções e objetos para a execução de tarefas administrativas ou operacionais conforme demanda.

9.3.2. Registrar um histórico de operações (trilhas de auditoria e registros de controle) no sistema que possa ser consultado contendo data, hora, usuário, função do sistema e dado manipulado, para todas as operações: adições, alterações, consultas, ativações, desativações e exclusões de dados no sistema, a fim de que todo o sistema possa ser auditado.

9.3.3. O sistema deverá estar em conformidade com a Nº 13.709/2018 LGPD (Lei geral de Proteção de Dados) e suas alterações, garantindo a existência de um caminho rápido para a solicitação de informações relacionadas ao tratamento dos dados pessoais caso seja necessário e se aplique.

9.3.4. A solução deve possuir mecanismos de segurança da informação, relacionados à integridade, privacidade e autenticidade dos dados.

9.3.5. A **CONTRATADA** deverá apresentar relatórios de testes de vulnerabilidades tipo **pentest White Box** do ambiente em nuvem após a assinatura do contrato e antecedendo a entrada do sistema em produção (de acordo com cronograma de implantação a ser estabelecido), e a cada 6 (seis) meses durante a vigência do contrato, relatando as falhas encontradas e as correções realizadas.

9.3.5.1. Os testes (pentest) deverão ser compostos por:

a) Scan de infraestrutura (análise de portas de serviços, versão dos webservers, versões do kernel servidores Linux), etc.

b) Scan de aplicação (SQL Error Message, Cross-Site Scripting, SQL Disclousure, Directory Browsing, Open Redirect).

9.3.6. O resultado dos testes com as vulnerabilidades encontradas e as correções aplicadas deverão ser entregues em formato digital aos gestores do contrato.

9.3.7. Para o acesso à console de gerenciamento deverá ser provido conexões com certificação segura e criptografadas no transporte das informações (**HTTPS**). O fornecimento de qualquer certificado necessário para a utilização da console fica sob responsabilidade da **CONTRATADA**.

9.4. REQUISITOS DE PROTEÇÃO DE DADOS

9.4.1. O ambiente de gestão em nuvem própria (console de gerenciamento) deverá se pautar pelos conceitos de privacy by design e privacy by default, nos moldes previstos nos artigos 46, §2º e 49 da Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/2018).

9.4.2. Devem ser observados os princípios da transparência na coleta de dados; adoção de ações preventivas de segurança de tratamento de dados pessoais; a privacidade por padrão, ou seja, projetar a configuração padrão do produto ou serviço ofertado objetivando sempre a privacidade dos dados; proteção durante todo o ciclo de vida do desenvolvimento do produto ou serviço, isto é, ter a proteção de dados pensada de ponta a ponta; foco no

usuário; funcionalidade completa e bem protegida; além de visibilidade e transparência, de modo a permitir que o titular dos dados tenha ciência do processo de coleta com a maior transparência possível.

9.4.3. A console de gerenciamento em nuvem deve oferecer ferramentas de anonimização dos dados pessoais tratados em caso de coleta para cadastro, acesso e auditoria.

9.4.4. A fabricante deverá prover alerta de vazamento de dados, bem como interface com o titular dos dados pessoais (usuário que tenha seus dados coletados) para atendimento dos artigos 9º e 18 da LGPD. A CONTRATADA deverá intermediar o processo.

9.5. REQUISITOS DE INFRAESTRUTURA

9.5.1. Os serviços deverão ser prestados em regime integral, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana sem interrupção, inclusive fora do horário comercial, em finais de semana e feriados. Todos os serviços de Infraestrutura para suportar a presente contratação correrão por conta da Contratada, seja ela hospedada em provedor de nuvem pública ou privada ou ainda, em DataCenter próprio. A PJF não hospedará em suas dependências equipamentos e sistemas da presente contratação

9.5.2. Os serviços deverão estar disponíveis em **99,7%** do tempo contratado, de modo que o somatório mensal das indisponibilidades do serviço seja de, no máximo, **02 (duas) horas.**

9.6. *REQUISITOS LEGAIS*

9.6.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, ao Decreto do Executivo de Juiz de Fora nº 15635/2022, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), Lei n° 10.520, de 17 de julho de 2001, Decreto 10.024, de 20 de setembro de 2019, e a outras legislações aplicáveis, devendo observar ainda posteriores alterações nas legislações supra e aplicáveis.

10. CONDIÇÕES DE EXECUÇÃO

10.1. A contratação será formalizada nos termos do art. 95 da Lei 14.133/2021.

10.2. Início da execução do objeto: até 24 horas da emissão da ordem de serviço emitida pela Subsecretaria de Tecnologia da Informação e enviadas à STDA/SSGD/DANP/SSEGC, situada à Av. Brasil, 2001 - 7º andar/Centro - 36.060-010 Juiz de Fora/MG, ou para o endereço eletrônico seginfo@pjf.mg.gov.br;

10.3. Local e horário da prestação dos serviços:

10.3.1. Os serviços serão prestados remotamente.

10.3.2. Os serviços serão prestados no seguinte horário: das 08:00hs às 18:00hs.

10.4. SUBCONTRATAÇÃO

10.4.1. Não é admitida a subcontratação do objeto contratual.

10.5. PROCEDIMENTOS DE TRANSIÇÃO E FINALIZAÇÃO DO CONTRATO

10.5.1. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

11. DO PAGAMENTO

11.1. 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, o qual ocorrerá posteriormente à data de apresentação da competente nota fiscal/fatura e, em anexo a esta, o atestado de fiscalização emitido por servidor lotado na Unidade Requisitante, responsável pela fiscalização da aquisição:

BANCO: _____
AGÊNCIA: _____
CONTA CORRENTE: _____
LOCALIDADE: _____

11.2. As notas fiscais deverão ser emitidas em moeda corrente do país.

11.3. Para efeito de cada pagamento, a nota fiscal/fatura deverá estar acompanhada da autorização de uso da nota fiscal eletrônica.

11.4. No caso da não apresentação da documentação de que trata o subitem anterior ou estando o objeto em desacordo com as especificações e demais exigências previstas, 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, à Licitante Vencedora, das penalidades previstas.

11.5. A Unidade Requisitante poderá descontar do pagamento importâncias que, a qualquer título, lhes sejam devidas pela Licitante Vencedora, por força da contratação.

11.6. Quando ocorrer a situação prevista no subitem anterior, não correrá juros ou atualizações monetárias de natureza qualquer, sem prejuízo de outras penalidades previstas.

11.7. 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.

11.8. Ocorrendo atraso de pagamento por culpa exclusiva da Unidade Requisitante, o pagamento será realizado acrescido de atualização financeira e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, e os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, através da seguinte fórmula:

I = (TX/100) 365
EM= I x N x VP

Onde:
I = índice de atualização financeira;
TX = percentual da taxa de juros de mora anual; EM = encargos moratórios
N = número de dias entre a data prevista para o pagamento e a do efetivo pagamento; VP = valor da parcela em atraso.

11.9. Para a hipótese definida no subitem anterior, a Licitante Vencedora fica obrigada a emitir fatura suplementar, identificando de forma clara que se trata de valor pertinente à atualização financeira originária de pagamento de fatura em atraso por inadimplemento.

12. MODELO DE GESTÃO DO CONTRATO

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

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

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

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

12.5. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

12.6. A Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a Contratada designará outro para o exercício da atividade.

12.7. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput).

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

12.9. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º)

12.10. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada uma Reunião de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

12.11. A reunião será realizada em até 5 (cinco) dias úteis da assinatura do Contrato, podendo ser

prorrogada a critério da Contratante.

12.12. A pauta desta reunião observará, pelo menos:

12.12.1. Presença do representante legal da contratada, que apresentará o seu preposto;

12.12.2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

12.12.3. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

12.12.4. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

12.12.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

12.13. Será responsável pelo acompanhamento do contrato o Supervisor de Segurança Cibernética do Departamento de Análise de Negócios e Projetos da Subsecretaria de Governança Digital.

13. PENALIDADES

13.1. Os casos de inexecução do objeto deste Termo de Referência, erro de execução, execução imperfeita, atraso injustificado e inadimplemento, sujeitará o contratado às penalidades previstas no Art. 156 da Lei nº 14.133 de 2021, das quais destacam-se:

a) advertência;

b) multa;

c) Suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo não superior a 3 (três) anos;

d) declaração de inidoneidade para licitar ou 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.

13.2. Na aplicação das sanções serão considerados:

I - a natureza e a gravidade da infração cometida;

II - as peculiaridades do caso concreto;

III - as circunstâncias agravantes ou atenuantes;

IV - os danos que dela provierem para a Administração Pública;

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

13.3. A aplicação de qualquer penalidade será precedida de processo administrativo próprio, nos termos da Lei 14.133/2021.

13.4. DAS SANÇÕES ADMINISTRATIVAS

13.4.1. Comete infração administrativa nos termos da Lei 14.133, de 2021, a CONTRATADA que:

I - dar causa à inexecução parcial do contrato;
II - dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;
III - dar causa à inexecução total do contrato;
IV - deixar de entregar a documentação exigida para o certame;
V - não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
VI - não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
VII - ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;
VIII - apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;
IX - fraudar a licitação ou praticar ato fraudulento na execução do contrato;
X - comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
XI - praticar atos ilícitos com vistas a frustrar os objetivos da licitação;
XII - praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

13.4.2. Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

A) Advertência, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;

B) Multa de:

I – 0,1% (um décimo por cento) até 0,2% (dois décimos por cento) por dia sobre o valor adjudicado em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

II– 0,1% (um décimo por cento) até 10% (dez por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem acima, ou de inexecução parcial da obrigação assumida;

III – 0,1% (um décimo por cento) até 15% (quinze por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida;

IV – 0,2% a 3,2% por dia sobre o valor do contrato, conforme detalhamento constante das **tabelas 1 e 2**, abaixo;

V- 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois

por cento). O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato;

Tabela 1

GRAU	CORRESPONDÊNCIA
1	0,2% ao dia sobre o valor do contrato
2	0,4% ao dia sobre o valor do contrato
3	0,8% ao dia sobre o valor do contrato
4	1,6% ao dia sobre o valor do contrato
5	3,2% ao dia sobre o valor do contrato

Tabela 2

INFRAÇÃO		
ITEM	**DESCRIÇÃO**	**GRAU**
1	No caso de indisponibilidade crítica que ultrapasse 72 horas de ausência de acesso ao console de gerenciamento impactando significativamente nas atividades correlatas à utilização do console de gerenciamento.	05
2	No caso de indisponibilidade crítica que ultrapasse 48 horas de ausência de acesso ao console de gerenciamento impactando significativamente nas atividades correlatas à utilização do console de gerenciamento.	04
3	No caso de indisponibilidade crítica que ultrapasse 24 horas de ausência de acesso ao console de gerenciamento impactando significativamente nas atividades correlatas à utilização do console de gerenciamento.	03
4	A estabilidade nos módulos gerenciais é fundamental para garantir a eficiência da gestão da proteção aplicada aos computadores do parque tecnológico desta Prefeitura.	02
5	O cumprimento dos acordos de nível de serviço (SLA) estabelecidos no contrato é essencial para assegurar o bom funcionamento da solução de segurança. Em situações em que a empresa não cumprir os prazos estipulados, será considerado infração;	01

C) Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública Municipal opera e atua concretamente, pelo prazo de até três anos;

D) Declaração de inidoneidade para licitar ou contratar com a Administração Pública Municipal, 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.

13.4.3. As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

13.4.4. A Sanção de impedimento de licitar e contratar também é aplicável em quaisquer das hipóteses previstas como infração administrativa neste Termo de Referência.

13.4.5. As sanções previstas nos subitens **"A", "C" e "D"** poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

13.4.6. Também ficam sujeitas às penalidades do art. 156, III e IV da Lei nº 14.133, de 2021, as empresas ou profissionais que:

A) tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

B) tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

C) demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

13.4.7. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 14.133, de 2021, e subsidiariamente o DECRETO N.º
11.105 - de 13 de fevereiro de 2012.

13.4.8. Após o devido processo legal, as penalidades serão aplicadas pela autoridade competente que deverá comunicar à Subsecretaria de Licitações e Compras - SSLICOM todas as ocorrências para fins de cadastramento e demais providências.

13.4.9. Entende-se por autoridade competente a (s) secretaria (s) responsável (is) por cada módulo ou sistema.

13.4.10. Os valores das multas aplicadas previstas no item **12.2.2, alínea "b", incisos I a V,**
poderão ser descontados dos pagamentos devidos pela Administração.

13.4.11. Da aplicação das penalidades definidas no **item 12.1,** alíneas "a", "b", "c" e "d", caberá recurso no prazo de 5 (cinco) dias úteis, contados da intimação.

13.4.12. Da aplicação da penalidade definida na alínea "d" do item **12.1**, caberá pedido de reconsideração no prazo de 10 (dez) dias úteis, contados da intimação.

13.4.13. 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.

PREGÃO ELETRÔNICO nº 107/2024 – PJF

ANEXO I.A

ESTUDO TÉCNICO PRELIMINAR

I - DIAGNÓSTICO DA SITUAÇÃO ATUAL

Em 2017 a Prefeitura de Juiz de Fora aderiu a uma Ata de Registro de Preço, conseguindo assim contratar uma solução de segurança robusta e reconhecida no mercado por ser destaque na área, substituindo a solução antivírus em vigência na época, que era inferior em funcionalidades e detecção de ameaças.

Em 2020 foi realizada uma nova licitação, buscando a contração da mesma ferramenta com um upgrade de versão a fim de aumentar a proteção dos ativos da Prefeitura de Juiz de Fora (doravante PJF) e eliminar a necessidade de contratar outra ferramenta para realizar os acessos remotos com finalidade de suporte realizados pela supervisão de atendimento, buscando maior economicidade para esta Prefeitura. A solução foi contratada pelo período de dois anos com a possibilidade de renovação por igual período, o que ocorreu em 2022 e se mantém até o presente.

Agora em 2024 buscamos a manutenção da segurança e do controle dos ativos informáticos da PJF, pois a ferramenta possibilita o mínimo de gerência sobre os computadores de nosso parque tecnológico, visto que ainda não dispomos de uma solução de gerenciamento mais robusta como o Microsoft Active Directory (AD) para aplicar políticas remotamente e gerenciar os ativos em nossa rede corporativa.

Com um crescente número de ataques cibernéticos cada vez mais especializados, a contratação de uma solução de segurança antivírus com detecção e resposta a incidentes de *endpoint* 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 do solução ***software Kaspersky Next EDR Optimum*** que é uma atualização de produto realizada pela fabricante no ano de 2024 em relação ao ***Kaspersky Endpoint Security Advanced*** faz-se necessária para garantir a integridade, confiabilidade e segurança das informações contra ações de programas maliciosos que ponham em risco a segurança cibernética, preservando as estações de trabalho, equipamentos servidores, *laptops* e dispositivos móveis de toda a PJF.
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 a Software Reviews, empresa referência na área de consultoria que cria conhecimento por meio de pesquisas sobre tecnologias, em especial a publicação de agosto de 2023, do relatório Emotional Footprint Endpoint Protection, nomeou a ***Kaspersky*** como líder no relatório do Quadrante de Dados de Porteção de Endpoints (https://www.softwarereviews.com/categories/endpoint-protection?entitlement=gold_medal_Kaspersky_Endpoint_Security_for_Business_data_quadrant_awards_2023_endpoint_protection&utm_campaign=award-data-quadrant-awards-endpoint-protection-2023-08-22&utm_medium=). Ainda, podemos citar sites de revisão das principais ferramentas de segurança do mercado como o av-test.org que apresenta e valida a qualidade da ferramenta (https://www.av-test.org/en/antivirus/business-windows-client/windows-11/april-2024/kaspersky-lab-endpoint-security-12.4-242212/).

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, gerenciamento em nuvem própria sem onerar custos de infraestrutura para esta Prefeitura, conhecimento operacional da equipe que já utiliza a versão anterior da ferramenta desde 2017, sendo necessário apenas um treinamento mínimo do tipo Hands On para o desenvolvimento e aprendizado das novas funcionalidades e não um treinamento completo e minucioso da solução, pois a equipe já apresenta um nível de maturidade adquirido na utilização da solução, obtendo assim custos menores no contexto global da contratação.

Em virtude da aquisição de novos computadores pela Secretária de Saúde com verba originária de recurso parlamentar destinado à informatização do setor e implementação de um novo sistema de gestão integrado informatizado e para garantirmos a segurança cibernética da PJF, seguindo em conformidade com a Lei Geral de Proteção de Dados (LGPD), vislumbramos a necessidade da contratação continuada de uma ferramenta robusta e eficaz, que trará além das funcionalidades atualmente implantadas na PJF, a função de detecção e resposta à incidentes que foi inserida na reformulação dos produtos Kaspersky ocorrida em abril de 2024 e compatível com a versão pretendida no processo licitatório a ser iniciado.

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 muitas máquinas da PJF, o futuro fim de suporte ao sistema Windows 10 (amplamente utilizado na PJF) que ocorrerá em 14 de outubro de 2025 (https://learn.microsoft.com/pt-br/lifecycle/products/windows-10-home-and- pro). Enquanto não realizamos a atualização de todos os computadores para o sistema operacional **Windows 11**, 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. 41, inc. I da Lei 14.133 de 2021, 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 Kaspersky Next EDR Optimum* tem como finalidade precípua evitar desperdício de tempo e recursos na instalação e configuração completas 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.

Destaco aqui que a versão pretendida Kaspersky Next EDR Optimum é a evolução direta do produto que possuímos hoje, Kaspersky Advanced Security for Business e ainda acrescenta a funcionalidade de detecção e resposta (EDR). Sendo assim, caso fosse uma renovação dontratual apenas, nos seriam entregues licenças de uso da nova solução fornecida pela Kaspersky.

Com a adoção dos serviços advindos da contratação pretendida , a Prefeitura de Juiz de Fora terá acesso a tecnologias mais novas, obtendo o aumento da capacidade de proteção de dados em seu parque tecnológico com adição de uma nova funcionalidade atrelada a ferramenta que é a deteção e resposta a ameaças cibernéticas.

1. **Alinhamento entre a contratação e o planejamento da Administração (art. 5º, X)**

A despesa relacionada à SOLUÇÃO DE SEGURANÇA ANTIVÍRUS, KASPERSKY, para toda a Prefeitura de Juiz de Fora, foi antecipadamente contemplada na Lei Orçamentária Anual (LOA), havendo recursos financeiros alocados para este propósito. Esta alocação está em total conformidade com o Plano Plurianual (PPA), a Lei de Diretrizes Orçamentárias (LDO) e a LOA, evidenciando a aderência do investimento às diretrizes e metas estabelecidas pelos órgãos responsáveis pela gestão financeira e orçamentária. Desta forma, a provisão de recursos para a SOLUÇÃO DE SEGURANÇA ANTIVÍRUS, KASPERSKY, para toda a Prefeitura de Juiz de Fora, está respaldada pela estrutura orçamentária vigente e está em conformidade com as políticas e prioridades definidas no PPA, na LDO e na LOA. Esta abordagem assegura a viabilidade financeira da iniciativa e reflete o compromisso com a gestão responsável dos recursos públicos.

Ao término do exercício de 2023 foi realizada uma readequação orçamentária que ocasionou a redução de recursos destinados à contratação aqui pretendida, porém já foram provisionados recursos que sustentarão financeiramente o certame oriundo da presente demanda. As dotações orçamentárias constarão nos autos do processo em despacho contíguo a este documento.

2. **Descrição dos requisitos da potencial contratação (art. 5º, II)**

- Para atender as necessidades da PJF no tangente a segurança cibernética, estamos buscando manter o padrão da solução atualmente implantada, pois a mesma consegue atender a várias demandas do setor de tecnologia além de ser um antivírus conceituado e eficaz. Seguem as principais funcionalidades atualmente utilizadas por nós e almejadas nessa nova contratação:
- Proteção de *Endpoints*, contando com proteção contra *malware*, prevenção de invasões baseada em *host* e controle adaptativo de anomalias.
- Proteção contra *Ransomware*.
- Firewall e proteção contra ameaças à rede.
- Monitoramento e descoberta na nuvem.
- Segurança na Nuvem.
- Controles de dispositivos e da web.
- Gerenciamento de vulnerabilidades, de correções e de criptografia.
- Funcionalidades básicas de EDR com análise da causa raiz (visualização de ataque). Funcionalidade que não possuímos hoje e estará presente na nova versão.
- Funcionalidades essenciais de EDR com resposta automatizada (aplicar automaticamente ações de resposta aos *endpoints* na descoberta de ameaças). Funcionalidade que não possuímos hoje e estará presente na nova versão.

O objeto da contratação deverá ser composto conforme quadro a seguir:

DESCRIÇÃO	**QUANTIDADE**
Licenças Kaspersky Next EDR Optimum por 24 Meses.	3.500
Suporte técnico especializado da contratada, por 24 meses Modalidade 24x7 remoto.	1
Implantação e configuração em nuvem própria (remoção dos atuais *endpoints* e instalação dos novos).	1
Treinamento remoto hands-on no produto NEXT EDR OPTIMUM para 2 (duas) pessoas.	1

Foram verificadas possibilidades de substituição da solução de segurança atualmente em utilização na PJF e constatamos que uma solução de mesmo nível aumentaria o ônus desta Prefeitura, consumindo recursos e tempo de estudo e aprendizado. Para mantermos a segurança cibernética de aproximadamente 3.500 computadores, necessitamos utilizar uma ferramenta robusta e bem-conceituada no mercado, o que reforça o cuidado com a proteção dos dados tratados nesta Prefeitura.

Foram realizadas apresentações das soluções de Endpoint ESET e Bitdefender para que pudéssemos avaliar todas as suas funcionalidades e o que entregam em comparação com o que possuímos hoje e, assim, a solução que mais se aproximou do Kaspersky (Solução atual) foi o Eset.

II – ANÁLISE DE SOLUÇÕES

1. Levantamento de Mercado (art. 5º, IV)

Para a presente contratação não há opção de software livre que atendam as necessidades da PJF e,

conforme já justificado no diagnóstico da situação atual e posteriormente no termo de referência, não dispomos de outras ferramentas que possibilitem uma maior gerência dos computadores presentes em nosso parque informático, que apresenta características bem heterogêneas. Assim, optamos pela padronização/manutenção da solução já presente em nosso parque informático com a atualização de versão entregue pelo fabricante e demais justificativas já apresentadas anteriormente neste documento.

Foram Buscadas alternativas para a contratação junto aos principais *players* de mercado e listamos abaixo as três soluções estudadas.

- Bitdefender: solução de endpoint mais restrita das três avaliadas e não apresenta todas as funcionalidades que já possuímos. https://antivirusparaempresas.net/business-security

- ESET: solução de endpoint que se equipara em **quase** todas as funcionalidades utilizadas atualmente, porém perderíamos o acesso com área de trabalho compartilhada, hoje utilizado pela supervisão de atendimento, necessitando assim da implementação de outra ferramenta. https://www.eset.com/br/antivirus-corporativo/bundles/elite-protection/

- Kaspersky: atualmente em utilização na PJF, atendendo todas as necessidades do setor de tecnologia no tangente a segurança cibernética e ainda agregando funcionalidades como o acesso com área de trabalho compartilhada, execução de scripts pré-definidos, inventário do nosso parque informático e emissão de diverssos relatórios para gestão e controle dos ativos tecnológicos presentes na rede corporativa. http://www.kaspersky.com.br/next-edr-optimum

Devido a sua inferioridade ao compararmos a solução Bitdefender com as demais, serão apresentados apenas os valores das soluções que se equivalem, ESET e Kaspersky. Ambas propostas seguem anexadas no mesmo despacho deste estudo (ETP).

2. Estimativa do valor da contratação (art. 5º, V)

Os orçamentos preliminares dão conta que a média de valor do objeto licitado é da ordem de grandeza de R$1.200.000,00 (Um milhão e duzentos mil reais) pelo período de 24 meses. Optou-se por esse período em virtude do ônus contratual, financeiro e processual para que dentro da lei vigente 14.133/2021 o mesmo possa ser renovado bienalmente até o prazo máximo de 10 anos, conforme art.108, V.

2.1 Análise das Propostas

De forma a facilitar a comparação entre as diferentes propostas até aqui apresentadas, foi criada uma tabela com os valores totais, somando os valores de implantação (planejamento, migração, implantação, treinamento e suporte) e licença de uso para **24 meses**. Sendo assim, segue tabela com os valores dos orçamentos, das contratações e a média.

DESCRIÇÃO DO SERVIÇO	***Implantação e Licença de Uso para um Sistema Integrado de Gestão Previdenciária***

ESET ELITE PROTECTION (3.300 LICENÇAS), SUPORTE DA CONTRATADA POR IGUAL PERÍODO DAS LICENÇAS, IMPLANTAÇÃO E CONFIGURAÇÃO EM NUVEM PRÓPRIA COM REMOÇÃO DOS ATUAIS ENDPOINTS E INSTALAÇÃO DOS NOVOS E TREINAMENTO REMOTO HANDS-ON PARA ATÉ 2 PESSOAS.	*Empresa Microhard - R$ 1.119.746,00 Proposta anexa ao processo.*
KASPERSKY NEXT EDR OPTIMUM (3.500 LICENÇAS), SUPORTE 27X7 REMOTO POR IGUAL PERÍODO DAS LICENÇAS, IMPLANTAÇÃO E CONFIGURAÇÃO EM NUVEM PRÓPRIA COM REMOÇÃO DOS ATUAIS ENDPOINTS E INSTALAÇÃO DOS NOVOS E TREINAMENTO REMOTO HANDS-ON NO PRODUTO KASPERSKY NEXT EDR OPTIMUM PARA ATÉ 2 PESSOAS.	*Empresa Nework Secure - R$ 1.119.650,00 Proposta anexa ao processo.*
KASPERSKY NEXT EDR OPTIMUM (3.500 LICENÇAS), SUPORTE 27X7 REMOTO POR IGUAL PERÍODO DAS LICENÇAS, IMPLANTAÇÃO E CONFIGURAÇÃO EM NUVEM PRÓPRIA COM REMOÇÃO DOS ATUAIS ENDPOINTS E INSTALAÇÃO DOS NOVOS E TREINAMENTO REMOTO HANDS-ON NO PRODUTO KASPERSKY NEXT EDR OPTIMUM PARA ATÉ 2 PESSOAS.	*Empresa Big Company: R$1.572.750,00 Proposta anexa ao processo.*
KASPERSKY NEXT EDR OPTIMUM (3.500 LICENÇAS), SUPORTE 27X7 REMOTO POR IGUAL PERÍODO DAS LICENÇAS, IMPLANTAÇÃO E CONFIGURAÇÃO EM NUVEM PRÓPRIA COM REMOÇÃO DOS ATUAIS ENDPOINTS E INSTALAÇÃO DOS NOVOS E TREINAMENTO REMOTO HANDS-ON NO PRODUTO KASPERSKY NEXT EDR OPTIMUM PARA ATÉ 2 PESSOAS.	*Empresa Vtech Tecnologia da Informação: R$1.726.500,00* *Proposta anexa ao processo.*
MÉDIA	***R$ 1.384.661,50***

Analisando a tabela acima, nota-se que os valores obtidos através de orçamentos com fornecedores apresentaram valores de preço de mercado para o objeto em análise, que nesse caso seria o valor total de ***R$ 1.384.661,50****.*

3. Escolha da solução (consequência dos incisos VIII e XI do art. 5º)

De modo a sistematizar as informações das soluções pesquisadas e subsidiar a avaliação para o atendimento da demanda em análise, foi criada uma tabela para demonstrar em análise comparativa, vantagens (pontos fortes) e desvantagens (riscos, limitações, problemas) referentes à adoção de cada modalidade de solução.

Soluções	***Vantagens (pontos fortes)***	***Desvantagens (riscos, limitações, problemas)***
Kaspersky Next EDR Optimum	• *Baixo custo financeiro.* • *Fácil personalização.* • *Implantação rápida.*	• *Manutenção e atualização de responsabilidade da organização.* • *Exige equipe de desenvolvimento qualificada.* • *Exige manutenção de infraestrutura própria ou contratada.* • *Exige equipe de suporte própria.*
ESET	• *Baixo custo financeiro.* • *Fácil personalização.*	• *Manutenção e atualização de responsabilidade da organização.* • *Implantação lenta.* • *Exige uma grande equipe de desenvolvimento qualificada.* • *Exige manutenção de infraestrutura própria ou contratada.* • *Exige equipe de suporte própria.*

A solução a ser contratada tem o objetivo auxiliar nas carências existentes atualmente na STDA/SSGD/SSEGC, além de aprimorar a proteção já aplicada aos computadores da PJF.

Vale citar ainda as seguintes necessidades:

- *Capacidade insuficiente de pessoal para gerir um parque de mais de três mil computadores.*

- *Ausência de um controlador de domínio. (A solução fornece algumas ferramentas que nos permitem* execução de *scripts* e inventariar o parque tecnológico da PJF.
- A solução pode ser utilizada pela supervisão de manutenção para a realização de acessos

pontuais com área de trabalho compartilhada para que o solicitante acompanhe os procedimentos que estão sendo executados. (Isso elimina a necessidade de

contratação/implantação de uma segunda ferramenta)

Ante o exposto, o cenário apresentado neste documento, juntamente com as informações acima justifica a contratação do software Kaspersky, visando a padronização e a manutenção da segurança nos ativos tecnológicos desta Prefeitura. Conforme previsto na Lei 14.133, Art 41, Inciso I alíneas B e D.

III – DETALHAMENTO DA SOLUÇÃO ESCOLHIDA

A CONTRATADA, juntamente com a sua solução, deverá realizar os seguintes serviços:

Planejamento do Projeto

Instalação e/ou Configuração: conforme já justificado anteriormente nos paragráfos iniciais do presente documento, a solução pretendida já se encontra implantada e em funcionamento em nosso parque tecnológico (aproximadamente três mil e cem computadores) e como teremos um redirecionamento de servidor para nuvem própria da fabricante em questão, será necessário executar a reinstalação dos agentes instalados nos computadores para direcionarem a comunicação para o novo servidor (novo endereço). A CONTRATADA realizará essa configuração com transferência de conhecimento para a equipe técnica da PJF a fim de que sejam possíveis noas implementações de forma mais independente, pois com a implantação de sistemas de Planejamento de Recursos Governamentais – (GRP do Inglês Govvernment Resource Planning) teremos um aumento no número de computadores em nosso parque já vislumbrado na contratação pretendida.

- Disponibilização de console em Nuvem própria com garantia de disponibilidade e atesto de conformidade com a Lei Geral de Proteção de Dados13.709/2018 (LGPD) e suas

posteriores atualizações, bem como demais legislações brasileiras vigentes que devem ser observadas a fim de garantir a segurança dos possíveis dados pessoais por ela tratados.

- Remoção dos endpoints atuais.
- Instalação dos endpoints novos com direcionamento para o novo servidor em Nuvem do fabricante e criação de pontos de distribuição.
- Exportação/importação das políticas atualmente ativas em nosso ambiente.
- Exportação/importação das tarefas já criadas e utilizadas em nosso parque tecnológico.
- Emissão de relatório final de implantação/reconfiguração.

Treinamento: a contratação pretendida contempla treinamento reduzido focado apenas nas novas

funcionalidades, pois a equipe já possui conhecimento acumulado na utilização da maioria das funções, o que trouxe economia na contratação mantendo a solução em uso e padronizada na instituição desde 2017. O treinamento será do tipo hands-on (prático) de forma online.

Manutenção e suporte: a contratada deverá fornecer suporte técnico durante toda a vigência contratual conforme objeto pretendido no regime de 24x7 de forma remota e os chamados devem ser tratados de acordo com o acordo de nível de serviço (SLA-*Service Level Agreement)* estipulado no Termo de Referência complementar a este documento e ao edital.

Atendimento às especificações técnicas: O sistema deverá obrigatoriamente conter todas as funcionalidades descritas nos requisitos da contratação descritos no termo de referência.

1. Justificativas para o parcelamento ou não da contratação

A solução não será parcelada, pois além das implicações técnicas haveria ônus financeiro para a Prefeitura de Juiz de Fora. Podemos destacar os seguintes pontos em caso de parcelamento da solução:

- Implicaria um custo financeiro maior, pois seriam necessárias implantações e treinamentos distintos com ônus adicionais.
- Afetaria o gerenciamento da segurança dos sistemas por parte da supervisão responsável, influenciando o esforço alocado pela SSEGC para os trabalhos de prevenção, acompanhamento e controle.
- Implicaria o estabelecimento de brechas de segurança, por onde possíveis ameaças poderiam se concretizar nos *endpoints* não contemplados com a solução parcialmente contratada.
- Poderia, eventualmente, gerar questões de compatibilidade e integração entre soluções diferentes e/ou em momentos diferentes, o que compromete o esforço da SSEGC e o desempenho da segurança cibernética na PJF.

Assim, a forma mais segura de implementação é uma solução de segurança única com gerenciamento centralizado para aumentar a proteção digital desta Prefeitura.

2. Contratações correlatas e/ou interdependentes (art. 5. IX)

Não haverá contratações correlatas ou interdependentes.

3. Resultados pretendidos (art. 5º, XI)

Espera-se manter a segurança cibernética dos ativos tecnológicos da Prefeitura de Juiz de Fora, monitorando e gerindo os seus respectivos computadores, executando tarefas remotamente e ainda possibilitando o acesso com área de trabalho compartilhada tal como existe hoje e é utilizado concomitantemente pelas supervisões de suporte, redes e segurança.

No que tange a equipe da supervisão de segurança cibernética, a adoção da solução requerida no presente documento propicia a gestão de um parque tenológico heterogêneo (variadas versões de sistemas operacionais e modelos de computadores distintos) e numeroso como o da PJF.

4. Providências a serem adotadas (art. 5º, XII)

Por se tratar da padronização de uma solução já implantada em mais de 3.100 (três mil e cem) computadores, garantindo os objetivos almejados nessa contratação, apenas as ações como: ajustes de configuração dos endpoints com redirecionamento para o novo servidor em Nuvem do próprio fabricante e um treinamento reduzido e direcionado às novas funcionalidades serão necessários. O gerenciamento será 100% online e não trará ônus adicional para a PJF no tangente à infraestrutura.

5. Possíveis impactos ambientais (art. 5º, XIII)

No que diz respeito aos impactos ambientais, os integradores de serviços, com um dos quais se deseja celebrar um futuro contrato são prestadores de serviços que não geram impactos ambientais, portanto não há restrições ou providências a serem tomadas nesse sentido.

IV – POSICIONAMENTO CONCLUSIVO

art. 5º, XIV

Com base nas informações aqui apresentadas, a **contratação de uma solução de segurança robusta, renomada e já em utilização há sete anos na Prefeitura de Juiz de Fora** foi considerada, neste momento, a melhor opção.

É inegável considerar que por adotar uma solução já implantada em nossos ativos tecnológicos, evitamos intercorrências no projeto que poderiam levar a ausência de proteção adequada nos computadores da PJF.

REFERÊNCIAS

Para a elaboração do presente documento foram utilizadas as seguintes referências:

- Site da empresa Kaspersky. Disponível em: http://www.kaspersky.com.br/next-edr-optimum. Acesso em 19/06/2024.
- Site da empresa Bitdefender. Disponível em: https://antivirusparaempresas.net/business-security. Acesso em 19/06/2024.
- Site da empresa ESET. Disponível em: https://www.eset.com/br/antivirus-corporativo/bundles/elite-protection/. Acesso em 19/06/2024.
- Console de gerenciamento atual da solução implantada. Acessado recorrentemente ao longo dos estudos iniciais, quantificação de licenças para distribuição de ônus para as demais secretarias.
- Apresentação da solução com gerenciamento em Nuvem da Kaspersky. Realizada em 29/02/2024 pela fabricante com intermédio da empresa Network Secure.

- Apresentação da solução com gerenciamento em nuvem da ESET. Realizada em 22/01/2024 pelo fabricante com o intermédio da empresa Microhard.

- Prova de Conceito (PoC) da solução da Kaspersky intermediada pela atual contratada para conhecermos as novas funcionalidades. Realizada por 30 dias em:03/04/2024 até 03/05/2024.

- Site da organização AVTEST. Disponível em: https://www.av-test.org/en/antivirus/business- windows-client/. Acesso em 27/06/2024.

PREGÃO ELETRÔNICO nº 107/2024 – PJF

ANEXO II

MINUTA DE CONTRATO

(Preenchida conforme orientação da Assessoria Jurídica Local)

Termo de Contrato celebrado entre o MUNICÍPIO DE JUIZ DE FORA, por meio da(o) _____ ou a (o) _____ [*entidade da Administração Indireta*], como CONTRATANTE, e a _____, como CONTRATADA, para aquisição de bens na forma abaixo.

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 107/2024**, conforme consta do Processo Administrativo próprio **nº 7.307/2024**, firmam o presente contrato:

CLÁUSULA PRIMEIRA – LEGISLAÇÃO APLICÁVEL

1.1. Este Contrato se rege por toda a legislação aplicável à espécie, que desde já se entende como referida no presente termo, especialmente pelas normas de caráter geral da **Lei Federal nº 14.133/2021**, pela **Lei Complementar Federal nº 123/2006**, com as alterações promovidas pela **Lei Complementar nº 147/2014**, **Lei Municipal nº 12.211/2011**, **Decreto Municipal nº 15.635/2022**, **Decreto Municipal nº 15.610/2022** e **demais legislações aplicáveis**, bem como pelos preceitos de Direito Público, pelas regras constantes do Edital e de seus Anexos, pela Proposta da CONTRATADA e pelas disposições deste Contrato. A CONTRATADA declara conhecer todas essas normas e concorda em se sujeitar às suas estipulações, sistema de penalidades e demais regras delas constantes, ainda que não expressamente transcritas neste instrumento, incondicional e irrestritamente.

CLÁUSULA SEGUNDA - DO OBJETO

2.1. É objeto deste instrumento **contratação de pessoa jurídica para fornecimento de Solução de Segurança da Informação, composta por software antivírus Kaspersky NEXT EDR Optmum com licenças de uso para 24 (vinte e quatro) meses e suporte da CONTRATADA por Igual período**, devidamente descritos, caracterizados e especificados no Termo de Referência (Anexo I do Edital de Pregão Eletrônico nº 107/2024), na forma abaixo descrita:

CLÁUSULA TERCEIRA - DO PREÇO, DA DOTAÇÃO E DA FORMA DE PAGAMENTO

3.1. O presente contrato tem o valor global previsto de **R$ 1.189.650,00 (um milhão, cento e oitenta e nove mil e seiscentos e cinquenta reais),** conforme preço registrado e quantitativos da UG, que é de pleno conhecimento das partes, sendo os valores unitários os seguintes:

ITEM	DESCRIÇÃO	QUANT.	PREÇO UNITÁRIO
			R$
PREÇO TOTAL:			R$

3.2. Os pagamentos deverão ser efetuados após a regular liquidação da despesa, nos termos do **art. 63 da Lei Federal nº 4.320/64**, observado o disposto no **art. 141 da Lei Federal nº 14.133/2021**. O prazo para pagamento em até 30 (trinta) dias posteriores à data de apresentação da competente nota fiscal/fatura, junto ao setor da Unidade Requisitante responsável e, em anexo a esta, o Atestado de Fiscalização emitido por servidor lotado na Divisão de Recursos Financeiros, responsável pela fiscalização do Contrato, em conta corrente aberta em banco a ser indicado com os seguintes dados:

BANCO:_____ AGÊNCIA:_____ CONTA-CORRENTE:_____ LOCALIDADE:_____

3.3.O pagamento à CONTRATADA será realizado em razão do efetivo fornecimento realizado e aceito, sem que a Unidade Requisitante esteja obrigada a pagar o valor total do contrato caso todo o quantitativo do objeto previsto na cláusula segunda não tenha sido regularmente entregue e aceito.

3.4. A contratada deverá apresentar juntamente com o documento de cobrança, os comprovantes de recolhimento do FGTS e INSS de todos os empregados atuantes no contrato, assim como Certidão Negativa de Débitos Trabalhistas – CNDT ou Certidão Positiva de Débitos Trabalhistas com efeito negativo válida, declaração de regularidade trabalhista.

3.5. No caso de erro nos documentos de faturamento ou cobrança, estes serão devolvidos à contratada para retificação ou substituição, passando o prazo de pagamento a fluir, então, a partir da reapresentação válida desses documentos.

3.6. O valor dos pagamentos eventualmente efetuados com atraso, desde que não decorra de fato ou ato imputável à contratada, sofrerá a incidência de juros e correção monetária, de acordo com a variação da Taxa Selic aplicável à mora da Administração Pública, *pro rata die* entre o 31º (trigésimo primeiro) dia da data do protocolo do documento de cobrança no setor competente do órgão ou entidade licitante e a data do efetivo pagamento, limitados a 12% ao ano.

3.7. O valor dos pagamentos eventualmente antecipados será descontado à taxa de 1% (um por cento) ao mês, calculada *pro rata die*, entre o dia do pagamento e o 30º (trigésimo) dia da data do protocolo do documento de cobrança no setor competente do órgão ou entidade licitante.

3.8. Do reajuste:

3.8.1. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

$$I = \frac{TX}{100}$$
$$\frac{}{365}$$
$$EM = I \times N \times VP$$

Onde:
I = índice de atualização financeira;
TX = percentual da taxa de juros de mora anual;
EM = encargos moratórios
N = número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = valor da parcela em atraso.

3.8.1.1- Mediante requerimento do Contratado, o presente Contrato poderá ter seu valor reajustado, a cada período de 12 (doze) meses, pelo IPCA, formalizando-se o reajuste, a critério do Município, por termo aditivo ou por simples apostila, nos termos do art. 136, I, da Lei nº 14.133/21.

3.8.2. Para a hipótese definida no item 3.8.1.1., a Licitante Vencedora fica obrigada a emitir fatura suplementar, identificando de forma clara que se trata de valor pertinente à atualização financeira originária de pagamento de fatura em atraso por inadimplemento da Unidade Requisitante.

3.8.3. A teor do art. 92, V, da Lei nº 14.133/21, fará jus à Contratada, na periodicidade anual, e de acordo com o IPCA, ao reajustamento do preço contratado.

3.9. O ISSQN, se devido, será recolhido, na forma do Código Tributário Municipal vigente e da Lei 10.630 de 30.12.03, caso não haja comprovação do recolhimento junto ao Município sede da contratada.

3.10. 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.

3.11. Dos Recursos Orçamentários:

3.11.1. As despesas decorrentes da presente licitação correrão por conta da dotação nº:

Secretaria da Saúde: 10.122.0003.1208.0000 / 339040 / 1.600.00.0000
Secretaria de Transformação Digital e Administrativa: PT 04126000111880000 ND 339040 Fonte 1500000000 UG 611100
JFPREV: PT 09.128.0001.2166.0000 FONTE 1802000000 UG 343100
Secretaria de Educação: 131100 / 12.122.0007.2004.0000 / 1.5.00.001001 / 3.3.90.40
Secretaria de Mobilidade urbana: UG: 141100 / 26.122.0007.2004.0000 / 1759000000

CLÁUSULA QUARTA - DO CONTRATO

4.1. O contrato regular-se-á, no que concerne a sua alteração, inexecução ou rescisão, pelas disposições da Lei nº 14.133/2021, de 01 de abril de 2021 observadas suas alterações posteriores, pelas disposições do Edital e pelos preceitos do direito público.

4.2. 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.

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

4.4. A contratação terá eficácia a partir da data da publicação do instrumento correspondente no Portal Nacional de Contratações Públicas e vigorará por **24 (vinte e quatro)** meses contados desta.

4.4.1. O prazo de vigência do contrato poderá ser prorrogado para até 10 (dez) anos, ou alterado nos termos dos arts. 105 a 114 da Lei Federal nº 14.133/2021.

4.5. Da subcontratação:

4.5.1. Não é admitida a subcontratação do objeto contratual.

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

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

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

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

4.6.5. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

4.6.6. A Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a Contratada designará outro para o exercício da atividade.

4.6.7. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput).

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

4.6.9. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º)

4.6.10. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada uma Reunião de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

4.6.11. A reunião será realizada em até 5 (cinco) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

4.6.12. A pauta desta reunião observará, pelo menos:

4.6.12.1. Presença do representante legal da contratada, que apresentará o seu preposto;
4.6.12.2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;
4.6.12.3. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;
4.6.12.4. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;
4.6.12.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

4.6.13. Será responsável pelo acompanhamento do contrato o Supervisor de Segurança Cibernética do Departamento de Análise de Negócios e Projetos da Subsecretaria de Governança Digital.

CLÁUSULA QUINTA - DO PRAZO E RECEBIMENTO DOS SERVIÇOS

5.2. O prazo de execução será de 24 (vinte e quatro) horas, a partir do recebimento da ordem de serviço/autorização emitida pela Unidade Requisitante.

5.2.1. Os serviços deverão ser prestados remotamente, nesta cidade de Juiz de Fora/MG, das 08:00hs às 18:00hs.

5.2.2. A sociedade empresária deverá constar na Nota Fiscal a data e hora em que a entrega dos serviços executados foi feita, além da identificação de quem procedeu o recebimento dos mesmos.

5.3. A entrega dos serviços deste instrumento será feita ao servidor designado para tal fim, a quem caberá conferi-lo e lavrar Termo de Recebimento Provisório, para efeito de posterior verificação da conformidade dos mesmos com as exigências das especificações.

5.4. Caso o objeto não esteja de acordo com as especificações exigidas, o servidor não o aceitará e lavrará termo circunstanciado do fato, que deverá ser encaminhado à autoridade superior, sob pena de responsabilidade.

5.5. O servidor deverá processar a conferência do que foi entregue, lavrando o termo de recebimento definitivo ou notificando a contratada para refazer o objeto entregue em desacordo com as especificações (recebimento provisório).

5.6. O recebimento provisório ou definitivo não exclui a responsabilidade da contratada pela perfeita execução do serviço, ficando a mesma obrigada a substituir, no todo ou em parte, o objeto do contrato, se a qualquer tempo se verificarem vícios, defeitos ou incorreções.

5.7. Os serviços, licenças e console de gerenciamento a serem fornecidos pela CONTRATADA serão realizados e entregues mediante ordem de serviço – OS e, sendo o caso, durante a sua prorrogação, nos moldes permitidos pelo art. 106, parágrafo 2º, da Lei nº 14.133/2021. A categorização dos serviços segue abaixo:

5.7.1. Serviços de Prestação Instantânea: Planejamento do projeto, instalação do sistema, migração de dados dos sistemas atualmente em uso, implantação, configuração e parametrização do sistema em seus ambientes de produção e homologação, treinamento e operação assistida (reconfiguração do ambiente pós implantação e

alguns atendimentos do suporte operacional e técnico).

5.7.2. Serviços de Prestação Continuada: Licença de uso, atualizações, reconfigurações e suporte operacional e técnico. Migração de regras e tarefas já criadas e aplicadas no âmbito da PJF.

5.8. SUPORTE OPERACIONAL E TÉCNICO DURANTE TODA A VIGÊNCIA CONTRATUAL

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

5.8.1.1. Suporte operacional e suporte técnico remoto, via conexão de dados segura, prestado pela equipe habilitada pelo fabricante do produto, com certificação na solução;

5.8.2. ACORDO DE NÍVEIS DE SERVIÇO

5.8.2.1. Entende-se como suporte a assistência técnica às correções de falhas, ajustes e fornecimento de releases e versões (atualizações) do software; apoio e mitigação de falhas críticas no ambiente em relação a proteção fornecida pelos endpoints.

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

5.8.2.3. São definidos como ajustes, alterações no software (atualização de versões) que melhorem o seu desempenho no ambiente da CONTRATANTE;

5.8.2.4. 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";

5.8.2.5. 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";

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

5.8.2.7. O serviço de suporte básico será realizado mediante solicitação da CONTRATANTE, em regime 24X7 a fim de salvaguardar a CONTRATANTE em situações consideradas críticas (como ataque de Ramsonware por exemplo).

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

5.8.2.9. 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 após o seu lançamento;

5.8.2.10. Toda despesa, caso exista, decorrente dos treinamentos (instrutores, elaboração do material

didático, deslocamento, alimentação e hospedagem dos instrutores, etc.) será de exclusiva responsabilidade da CONTRATADA.

5.8.2.11. 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 este termo;

5.8.2.12. 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;

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

5.8.2.14. 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;

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

5.8.2.16. 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;

5.8.2.17. 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 chamados de atendimento

5.9. TREINAMENTO

5.9.1. Será necessário treinamento reduzido, focado nas novas funcionalidades, à equipe que atuará com a solução. O treinamento deverá ser de no mínimo 8 (oito) horas de duração, podendo variar a critério da CONTRATADA em comum acordo com a CONTRATANTE a fim de garantir que o conteúdo apresentado supra as necessidades da CONTRATADA quanto à transferência de conhecimento das novidades funcionais do software em relação a versão atualmente em utilização na PJF.

5.9.2. Após a configuração do ambiente em nuvem da console a CONTRATADA será responsável pelo treinamento dos usuários designados pela CONTRATANTE.

5.9.3. Esta etapa deverá ser realizada remotamente, focando nas novas funcionalidades da console em nuvem e diferenças entre o novo ambiente e o ambiente on-premise (MMC) que existe hoje na PJF. em datas e horários definidos em comum acordo entre as partes.

5.9.4. A CONTRATADA deverá definir o conteúdo programático e o quantitativo do treinamento necessário à capacitação e transferência de conhecimento ao público-alvo, fixando a carga horária e o número de encontros, considerando as novas funcionalidades disponíveis na console de gerenciamento da solução.

5.10. CARACTERÍSTICAS DO SOFTWARE

5.10.1. Do módulo de proteção de endpoint

5.10.1.1. A solução proposta deverá proteger os sistemas operacionais abaixo:

5.10.1.1.1. Windows 7
5.10.1.1.2. Windows 8
5.10.1.1.3. Windows 8.1
5.10.1.1.4. Windows 10
5.10.1.1.5. Windows 11

5.10.1.2. Servidores:

5.10.1.2.1. Windows Small Business Server 2011
5.10.1.2.2. Windows MultiPoint Server 2011
5.10.1.2.3. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022
5.10.1.2.4. Servidores de terminal Microsoft

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

5.10.1.4. Sistemas operacionais Linux de 32 bits:

5.10.1.4.1. CentOS 6.7 e posterior
5.10.1.4.2. Debian GNU/Linux 11.0 e posterior
5.10.1.4.3. Debian GNU/Linux 12.0 e posterior
5.10.1.4.4. Red Hat Enterprise Linux 6.7 e posterior

5.10.1.5. Sistemas operacionais Linux de 64 bits:

5.10.1.5.1. Amazon Linux 2.
5.10.1.5.2. CentOS 6.7 e mais tarde
5.10.1.5.3. CentOS 7.2 e posterior.
5.10.1.5.4. CentOS Stream 8.
5.10.1.5.5. CentOS Stream 9.
5.10.1.5.6. Debian GNU/Linux 11.0 e posterior.
5.10.1.5.7. Debian GNU/Linux 12.0 e posterior.
5.10.1.5.8. Linux Mint 20.3 e superior.
5.10.1.5.9. Linux Mint 21.1 e posterior.
5.10.1.5.10. OpenSUSE Leap 15.0 e posterior.
5.10.1.5.11. Oracle Linux 7.3 e posterior.
5.10.1.5.12. Oracle Linux 8.0 e posterior.
5.10.1.5.13. Oracle Linux 9.0 e posterior.
5.10.1.5.14. Red Hat Enterprise Linux 6.7 e posterior
5.10.1.5.15. Red Hat Enterprise Linux 7.2 e posterior.
5.10.1.5.16. Red Hat Enterprise Linux 8.0 e posterior.
5.10.1.5.17. Red Hat Enterprise Linux 9.0 e posterior.
5.10.1.5.18. Rocky Linux 8.5 e posterior.
5.101.5.19. Rocky Linux 9.1.
5.10.1.5.20. SUSE Linux Enterprise Server 12.5 ou posterior.

5.10.1.5.21. SUSE Linux Enterprise Server 15 ou posterior.
5.10.1.5.22. Ubuntu 20.04 LTS.
5.10.1.5.23. Ubuntu 22.04 LTS.

5.10.1.6. Sistemas operacionais Arm de 64 bits:

5.10.1.6.1. CentOS Stream 9.
5.10.1.6.2. SUSE Linux Enterprise Server 15.
5.10.1.6.3. Ubuntu 22.04 LTS.

5.10.1.7. Sistemas operacionais MAC OS:

5.10.1.7.1. macOS 12 – 14

5.10.1.8. Ferramentas de virtualização MAC OS:

5.10.1.8.1. Parallels Desktop 16 para Mac Business Edition
5.10.1.8.2. VMware Fusion 11.5 Profissional
5.10.1.8.3. VMware Fusion 12 Profissional

5.10.1.9. A solução proposta deverá suportar as seguintes plataformas virtuais:

5.10.1.9.1. VMware Workstation 17.0.2 Pro
5.10.1.9.2. VMware ESXi 8.0 Update 2
5.10.1.9.3. Microsoft Hyper-V Server 2019
5.10.1.9.4. Citrix Virtual Apps e Desktop 7 2308
5.10.1.9.5. Citrix Provisioning 2308
5.10.1.9.6. Citrix Hypervisor 8.2 Update 1

5.10.2. Do módulo de gerenciamento avançado

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

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

5.10.2.2.1. Amazon Web Services
5.10.2.2.2. Microsoft Azure

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

5.10.2.3.1. HP (Microfoco) ArcSight
5.10.2.3.2. IBM QRadar
5.10.2.3.3. Splunk
5.10.2.3.4. Kaspersky KUMA

5.10.2.4. A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

5.10.2.5. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;

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

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

5.10.2.8. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

5.10.2.9. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

5.10.2.10. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.

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

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

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

5.10.2.14. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em um único/múltiplos dispositivos com base nas seguintes regras de ativação:

5.10.2.14.1. Status do dispositivo
5.10.2.14.2. Tag
5.10.2.14.3. Diretório ativo
5.10.2.14.4. Proprietários de dispositivos
5.10.2.14.5. Hardware

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

5.10.2.15.1. E-mail
5.10.2.15.2. Registro de sistema
5.10.2.15.3. SMS

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

5.10.2.16.1. Atributos de rede
5.10.2.16.2. Nome
5.10.2.16.3. Domínio e/ou Sufixo de Domínio
5.10.2.16.4. Endereço de IP

5.10.2.16.5. Endereço IP para servidor de gerenciamento
5.10.2.16.6. Localização no Active Directory
5.10.2.16.7. Unidade organizacional
5.10.2.16.8. Grupo
5.10.2.16.9. Sistema operacional
5.10.2.16.10. Número do pacote de serviço
5.10.2.16.11. Arquitetura Virtual
5.10.2.16.12. Registro de aplicativos
5.10.2.16.13. Nome da Aplicação
5.10.2.16.14. Versão do aplicativo
5.10.2.16.15. Fabricante
5.10.2.16.16. Tipo e versão
5.10.2.16.17. Arquitetura

5.10.2.17. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.

5.10.2.18. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.

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

5.10.2.19.1. Dispositivos Desktop/Servidores
5.10.2.19.2. Dispositivos móveis
5.10.2.19.3. Dispositivos de rede
5.10.2.19.4. Dispositivos virtuais
5.10.2.19.5. Componentes OEM
5.10.2.19.6. Periféricos de computador
5.10.2.19.7. Dispositivos IoT conectados
5.10.2.19.8. Telefones VoIP
5.10.2.19.9. Repositórios de rede

5.10.2.20. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:

5.10.2.20.1. Nome da Aplicação
5.10.2.20.2. Caminho do aplicativo
5.10.2.20.3. Metadados do aplicativo
5.10.2.20.4. Aplicativo Certificado digital
5.10.2.20.5. Categorias de aplicativos predefinidas pelo fornecedor
5.10.2.20.6. SHA256 e MD5

5.10.2.21. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:

5.10.2.21.1. Bluetooth
5.10.2.21.2. Dispositivos móveis
5.10.2.21.3. Modems externos
5.10.2.21.4. CD/DVD

5.10.2.21.5. Câmeras e scanners
5.10.2.21.6. MTPs
5.10.2.21.7. E a transferência de dados para dispositivos móveis

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

5.10.2.23. A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.

5.10.2.24. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

5.10.2.24.1. Estruturas de domínios e grupos de trabalho do Windows
5.10.2.24.2. Estruturas de grupos do Active Directory
5.10.2.24.3. Conteúdo de um arquivo de texto criado manualmente pelo administrador

5.10.2.25. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.

5.10.2.26. A solução proposta deve permitir realizar as seguintes ações para endpoints:

5.10.2.26.1. Verificação manual;
5.10.2.26.2. Verificação no acesso;
5.10.2.26.3. Verificação por demanda;
5.10.2.26.4. Verificação de arquivos compactados
5.10.2.26.5. Verificação de arquivos individuais, pastas e unidades;
5.10.2.26.6. Bloqueio e verificação de scripts
5.10.2.26.7. Proteção contra alteração de registros;
5.10.2.26.8. Proteção contra estouro de buffer;
5.10.2.26.9. Verificação em segundo plano/inativa
5.10.2.26.10. Verificação de unidade removível na conexão com o sistema;

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

5.10.2.28. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.

5.10.2.29. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.

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

5.10.2.31. A solução proposta deve prever a criação de uma cópia de segurança do sistema de

administração com o auxílio de ferramentas integradas do sistema de administração.

5.10.2.32. A solução proposta deve suportar Windows Failover Cluster.

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

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

5.10.2.35. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.

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

5.10.2.37. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.

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

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

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

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

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

5.10.2.43. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo especifico de prevenção de intrusão.

5.10.2.44. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.

5.10.2.45. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).

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

5.10.2.47. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de

transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.

5.10.2.48. A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.

5.10.2.49. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.

5.10.2.50. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.

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

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

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

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

5.10.2.55. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.

5.10.2.56. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal.

5.10.2.57. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.

5.10.2.58. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.

5.10.2.59. A solução proposta deve permitir ao administrador personalizar relatórios.

5.10.2.60. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.

5.10.2.61. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.

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

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

5.10.2.64. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.

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

5.10.2.66. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;

5.10.2.67. O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.

5.10.2.68. A solução proposta deve suportar integração com solução APT.

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

5.10.2.70. A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:

5.10.2.71. Windows

5.10.2.72. Linux

5.10.2.73. A solução proposta deverá suportar os seguintes servidores de banco de dados:

5.10.2.73.1. Windows:
5.10.2.73.2. Microsoft SQL Server
5.10.2.73.3. Microsoft Banco de dados SQL do Azure
5.10.2.73.4. MySQL Standard e Enterprise
5.10.2.73.5. MariaDB
5.10.2.73.6. PostgreSQL

5.10.2.74. Linux:

5.10.2.74.1. MySQL
5.10.2.74.2. MariaDB

5.10.2.74.3. PostgreSQL

5.10.2.75. A solução proposta deverá suportar as seguintes plataformas virtuais:

5.10.2.75.1. Windows:
5.10.2.75.2. VMware vSphere 6.7 e 7.0
5.10.2.75.3. Estação de trabalho VMware 16 Pro
5.10.2.75.4. Servidor Microsoft Hyper-V 2012 de 64 bits
5.10.2.75.5. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
5.10.2.75.6. Microsoft Servidor Hyper -V 2016 de 64 bits
5.10.2.75.7. Servidor Microsoft Hyper-V 2019 de 64 bits
5.10.2.75.8. Servidor Microsoft Hyper-V 2022 de 64 bits
5.10.2.75.9. Citrix XenServer 7.1 LTSR
5.10.2.75.10. Citrix XenServer 8.x
5.10.2.75.11. Oracle VM VirtualBox 6.x

5.10.2.76. Linux:

5.10.2.76.1. VMware vSphere 6.7, 7.0 e 8.0
5.10.2.76.2. VMware Desktop 16 Pro e 17 Pro
5.10.2.76.3. Servidor Microsoft Hyper-V 2012 de 64 bits
5.10.2.76.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
5.10.2.76.5. Microsoft Servidor Hyper -V 2016 de 64 bits
5.10.2.76.6. Servidor Microsoft Hyper-V 2019 de 64 bits
5.102.76.7. Servidor Microsoft Hyper-V 2022 de 64 bits
5.10.2.76.8. Citrix XenServer 7.1 e 8.x
5.10.2.76.9. Oracle VM VirtualBox 6.x e7.x

5.10.2.77. A solução proposta deve suportar criptografia em vários níveis:
5.10.2.77.1. Criptografia completa do disco – incluindo disco do sistema
5.10.2.77.2. Criptografia de arquivos e pastas
5.10.2.77.3. Criptografia de mídia removível
5.10.2.77.4. Gerenciamento de criptografia BitLocker e MacOS Filevault2

5.10.2.78. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:
5.10.2.78.1. A criptografia de arquivos em unidades de computador locais.
5.10.2.78.2. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões.
5.10.2.78.3. A criação de listas criptografadas de pastas em unidades de computador locais.

5.10.2.79. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:

5.10.2.80. Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis.

5.10.2.81. Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.

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

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

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

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

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

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

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

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

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

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

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

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

5.10.2.94. A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por

palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos.

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

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

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

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

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

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

5.10.2.101. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:
5.10.2.101.1. Instalação remota de software de terceiros
5.10.2.101.2. Relatórios sobre software e hardware existentes
5.10.2.101.3. Monitoramento para instalação de software não autorizado
5.10.2.101.4. Remoção de software não autorizado

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

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

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

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

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

5.10.2.107. A solução proposta deve ter a capacidade de aplicar patches específicos com base na

criticidade ou gravidade.

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

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

5.10.2.110. A solução proposta deve permitir ao administrador aprovar atualizações.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.10.2.135. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:
5.10.2.135.1. Inicie a instalação ao reiniciar ou desligar o computador.
5.10.2.135.2. Instale o gerador necessário todos os pré-requisitos do sistema.
5.10.2.135.3. Permitir a instalação de novas versões de aplicativos durante as atualizações.
5.10.2.135.4. Baixe atualizações para o dispositivo sem instalá-las.
5.10.2.135.5. A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas.

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

5.10.2.137. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:

5.10.2.137.1. CEF;
5.10.2.137.2. LEEF;

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

5.10.2.139. O relatório da solução proposta deve conter informações CVE.

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

5.10.3. Do módulo de gerenciamento simplificado

5.10.3.1. A solução proposta deve suportar arquitetura cloud;

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

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

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

5.10.3.5. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.

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

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

5.10.3.8. A solução proposta deve incluir informações do endpoint:
5.10.3.8.1. IP público de internet;
5.10.3.8.2. IP interno do dispositivo;
5.10.3.8.3. Versão do agente de proteção;
5.10.3.8.4. Última comunicação com a console, contendo data e hora;
5.10.3.8.5. Informações do sistema operacional;

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

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

5.10.3.11. A solução proposta deve incluir treinamento em segurança cibernética.

5.10.4. Requisitos gerais

5.10.4.1. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:
5.10.4.1.1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware,

Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.

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

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

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

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

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

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

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

5.10.4.9. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.

5.10.4.10. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.

5.10.4.11. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.

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

5.10.4.13. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.

5.10.4.14. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:
5.10.4.14.1. Controles de aplicativos,
5.10.4.14.2. Controle web e dispositivos
5.10.4.14.3. HIPS e Firewall
5.10.4.14.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;
5.10.4.14.5. Gerenciamento de criptografia de arquivos e discos;
5.10.4.14.6. Controle adaptativo para detecção de anomalias;

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

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

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

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

5.10.4.18. A solução proposta deve incluir um módulo capaz, no mínimo, de:
5.10.4.18.1. Bloqueio de aplicativos com base em sua categorização.
5.10.4.18.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.

5.10.4.19. A adição de sub-redes e a modificação de permissões de atividade.

5.10.4.20. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.

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

5.10.4.22. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.

5.10.4.23. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:
5.10.4.23.1. Modo silencioso;
5.10.4.23.2. Discos rígidos e dispositivos removíveis;
5.10.4.23.3. De todos as contas de usuários do dispositivo.
5.10.4.23.4. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:
5.10.4.23.4.1. Exclusão imediata de dados;
5.10.4.23.4.2. Exclusão de dados adiada.

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

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

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

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

5.10.4.28. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.

5.10.4.29. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.

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

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

5.10.4.32. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;

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

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

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

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

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

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

5.10.4.39. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.

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

5.10.4.41. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB

ou permitir o acesso apenas aos dispositivos permitidos.

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

5.104.43. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.

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

5.10.4.45. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;

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

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

5.10.4.48. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.

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

5.10.4.50. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.

5.10.4.51. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.

5.10.4.52. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.

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

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

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

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

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

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

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

5.10.4.60. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.

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

5.10.4.62. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:
5.10.4.62.1. Filtro de anexos.
5.10.4.62.2. Verificação de mensagens de email ao receber, ler e enviar.

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

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

5.10.4.65. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.);

5.10.4.66. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.

5.10.4.67. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.

5.10.4.68. A solução proposta deve incluir suporte ao protocolo IPv6.

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

5.10.4.70. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:

5.10.4.71. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.

5.10.4.72. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.

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

5.10.4.74. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.

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

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

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

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

5.10.4.79. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.

5.10.4.80. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia , bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.

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

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

5.10.4.83. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.

5.10.4.84. A solução proposta deve suportar endereços IPv6.

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

5.10.4.86. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.

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

5.10.4.88. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.

5.10.4.89. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de

dados anti-malware mais recentes.

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

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

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

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

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

5.10.4.95. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.

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

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

5.10.4.98. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado.

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

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

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

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

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

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

5.10.4.105. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.

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

5.10.4.107. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.

5.10.4.108. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.

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

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

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

5.10.4.112. A solução proposta deve gerar relatórios de vulnerabilidades encontradas nos dispositivos com sensor de endpoint instalado.

5.10.5. Do modulo de gerenciamento de dispositivos móveis

5.10.5.1. O modulo deve ser integrado a console de gerenciamento;

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

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

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

5.10.5.5. A solução proposta deve suportar dispositivos iOS supervisionados.

5.10.5.6. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.

5.10.5.7. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.

5.10.5.8. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a

uma lista de permissões.

5.10.5.9. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).

5.10.5.10. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.

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

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

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

5.10.5.14. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:
5.10.5.14.1. Dados em contêineres
5.10.5.14.2. Contas de e-mail corporativo
5.10.5.14.3. Configurações para conexão à rede Wi-Fi corporativa e VPN
5.10.5.14.4. Nome do ponto de acesso (APN)
5.10.5.14.5. Perfil do Android for Work
5.10.5.14.6. Recipiente KNOX
5.10.5.14.7. Chave do gerenciador de licença KNOX

5.10.5.15. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:
5.10.5.15.1. Todos os perfis de configuração instalados
5.10.5.15.2. Todos os perfis de provisionamento
5.10.5.15.3. O perfil iOS MDM
5.10.5.15.4. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas

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

5.10.5.17. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:

5.10.5.18. Critérios de verificação do dispositivo;

5.10.5.19. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;

5.10.5.20. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre

hacks de dispositivos, por exemplo, root, Jailbreak e etc.

5.10.5.21. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:
5.10.5.21.1. Cartões de memória e outras unidades removíveis
5.10.5.21.2. Câmera do dispositivo
5.10.5.21.3. Conexões Wi-Fi
5.10.5.21.4. Conexões Bluetooth
5.10.5.21.5. Porta de conexão infravermelha
5.10.5.21.6. Ativação do ponto de acesso Wi-Fi
5.10.5.21.7. Conexão de área de trabalho remota
5.10.5.21.8. Sincronização de área de trabalho

5.10.5.21.9. Definir configurações da caixa de correio do Exchange
5.10.5.21.9.1. Configurar caixa de e-mail em dispositivos iOS MDM
5.10.5.21.9.2. Configure contêineres Samsung KNOX.
5.10.5.21.9.3. Definir as configurações do perfil do Android for Work
5.10.5.21.9.4. Configurar e-mail/calendário/contatos
5.10.5.21.9.5. Defina as configurações de restrição de conteúdo de mídia.
5.10.5.21.9.6. Definir configurações de proxy no dispositivo móvel
5.10.5.21.9.7. Configurar certificados e SCEP

5.10.5.22. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay

5.10.5.23. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:
5.10.5.23.1. Google Play, Huawei App Gallery e Apple App Store
5.10.5.23.2. Portal de inscrição móvel KNOX
5.10.5.23.3. Pacotes de instalação pré-configurados independentes

5.10.5.24. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.

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

5.10.5.26. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:

5.10.5.26.1. VMware AirWatch 9.3 ou posterior
5.10.5.26.2. MobileIron 10.0 ou posterior
5.10.5.26.3. IBM MaaS360 10.68 ou posterior
5.10.5.26.4. Microsoft Intune 1908 ou posterior
5.10.5.26.5. SOTI MobiControl 14.1.4 (1693) ou posterior

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

5.10.5.28. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:
5.10.5.28.1. Google Play
5.10.5.28.2. Galeria de aplicativos Huawei
5.10.5.28.3. Loja de aplicativos da Apple

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

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

5.10.5.31. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.

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

5.10.5.33. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.

5.10.5.34. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.

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

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

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

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

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

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

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

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

5.10.6. Do módulo de EDR

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

5.10.6.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.

5.10.6.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;

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

5.10.6.5. Deve apresentar informações detalhadas contendo:
5.10.6.5.1. Usuário que executou a ação;
5.10.6.5.2. Informações acesso privilegiado;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.10.6.20. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:

5.10.6.21. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).

5.10.6.22. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.

5.10.6.23. Informações gerais sobre a detecção, incluindo modo de detecção.

5.10.6.24. Alterações no registro associadas à detecção.

5.10.6.25. Histórico da presença de arquivos no dispositivo.

5.10.6.26. Ações de resposta executadas pela aplicação.

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

5.10.6.28. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:
5.10.6.28.1. Processo
5.10.6.28.2. Conexões de rede
5.10.6.28.3. Alterações no registro
5.10.6.28.4. Detalhes do download de objeto
5.10.6.28.5. A solução proposta deve fornecer orientação de resposta (resposta guiada).
5.10.6.28.6. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente

5.10.6.29. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:
5.106.29.1. Impedir a execução de objetos
5.10.6.29.2. Isolamento de host
5.10.6.29.3. Excluir objeto do host ou grupo de hosts
5.10.6.29.4. Encerrar um processo no dispositivo
5.10.6.29.5. Colocar um objeto em quarentena
5.10.6.29.6. Execute a verificação do sistema
5.10.6.29.7. Execução remota de programa/processo/comando
5.10.6.29.8. Iniciar a varredura IoC para um grupo de hosts.

5.10.7. Requisitos para documentação da solução.

5.10.7.1. A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:
5.10.7.1.1. Ajuda on-line para administradores
5.10.7.1.2. Ajuda on-line para melhores práticas de implementação
5.10.7.1.3. Ajuda on-line para proteção de servidores de administração
5.10.7.1.4. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware.
5.10.7.1.5. Deve estar disponível página com informações de ciclo de vida das soluções e módulos;

5.11. PLANEJAMENTO DO PROJETO

5.11.1. Configuração do Ambiente

5.11.1.1. A CONTRATADA, deverá disponibilizar o ambiente em nuvem própria pré-configurada para a utilização da CONTRATANTE já com as licenças aplicadas.

5.11.1.2. A configuração das regras, bem como remoção dos endpoints atuais e instalação dos novos com apontamento para a nova console será de responsabilidade da CONTRATADA com a devida transferência de conhecimento para a CONTRATANTE.

CLÁUSULA SEXTA – DAS OBRIGAÇÕES

6.1. Da contratante:

6.1.1. Requisitar, por meio de servidor designado, execução do serviço, conforme as necessidades da Unidade Requisitante por meio da respectiva requisição, que atestará o recebimento gradual dos mesmos.

6.1.2. Conferir o fornecimento do produto e impedir que terceiros forneçam o objeto do Anexo I, já que a contratada será a única e exclusiva responsável pelo fornecimento nas condições especificadas.

6.1.3. Zelar pelo cumprimento dos atos relativos às obrigações que assumir contratualmente, bem como pela aplicação de eventuais penalidades decorrentes do descumprimento do contrato em que figure como parte.

6.1.4. Comunicar à contratada qualquer irregularidade na execução do serviço interromper imediatamente o fornecimento se for o caso.

6.1.5. Solicitar a substituição do serviço que não apresentar condições de ser utilizado.

6.1.6. Atestar o adimplemento da obrigação, desde que satisfaça às exigências editalícias.

6.1.7. Fiscalizar a manutenção das condições de habilitação e qualificações do Fornecedor, exigidas no edital, durante toda a execução do fornecimento, em cumprimento ao disposto no Art. 92. da Lei Federal nº 14.133/2021.

6.1.8. Notificar o Fornecedor, fixando-lhe prazo para corrigir defeitos ou irregularidades encontradas na execução do fornecimento e interromper imediatamente o fornecimento se for o caso, assim como solicitar a substituição do serviço que não apresentar condições de ser utilizado.

6.2. Da licitante vencedora:

6.2.1. Dar ciência, imediatamente, do recebimento das Notas de Empenho, Ordem de Fornecimento ou outros instrumentos hábeis enviados pela Unidade Requisitante.

6.2.2. Entregar de forma sistemática e periódica, pelo preço contratado os produtos objeto deste Edital, segundo as necessidades e as requisições da Unidade Requisitante.

6.2.3. Entregar o produto especificado na Ordem de Fornecimento, de acordo com as necessidades e o interesse da Unidade Requisitante, obedecendo rigorosamente aos prazos e às condições estabelecidas no Termo de Referência.

6.2.4. Responsabilizar-se integralmente pela entrega, nos termos da legislação vigente e exigências editalícias, observadas as especificações, normas e outros detalhamentos, quando for o caso ou no que for aplicável, fazer cumprir, por parte de seus empregados e prepostos, as normas da Unidade Requisitante.

6.2.5. Atender, de imediato, as solicitações relativas à substituição, reposição ou troca do produto que não atenda ao especificado.

6.2.6. Atender a todos os pedidos de fornecimento, não se admitindo procrastinação em função de pedido de revisão de preço ou substituição de marca.

6.2.7. Praticar, sempre, o(s) preço(s) e as marca(s) vigente(s) publicado(s) na Ata de Registro de Preços.

6.2.8. Responsabilizar-se pelo transporte adequado do(s) produto(s) de seu estabelecimento até o local determinado, bem como pelo seu descarregamento até o interior do local de entrega.

6.2.9. Executar o serviço no prazo estabelecido, informando em tempo hábil qualquer motivo impeditivo ou que impossibilite assumir o estabelecido.

6.2.10. Assumir inteira responsabilidade quanto à garantia e qualidade do produto, reservando à Unidade Requisitante o direito de recusá-lo caso não satisfaça aos padrões especificados.

6.2.11. Comunicar imediatamente à Unidade Requisitante quando for o caso, qualquer anormalidade verificada, inclusive de ordem funcional, para que sejam adotadas as providências de regularização necessárias.

6.2.12. Responder objetivamente por quaisquer danos pessoais ou materiais decorrentes da entrega do produto, seja por vício de fabricação ou por ação ou omissão de seus empregados e prepostos.

6.2.13. Assumir inteira responsabilidade quanto à qualidade do produto entregue.

6.2.14. Responder direta e exclusivamente pela execução do contrato de fornecimento, não podendo, em nenhuma hipótese, transferir a responsabilidade pelo fornecimento do produto a terceiros, sem o expresso consentimento da Unidade Requisitante.

6.2.15. Arcar com o pagamento de todos os encargos trabalhistas, fiscais, previdenciários, securitários e outros advindos da execução do objeto, de forma a eximir a Unidade Requisitante de quaisquer ônus e responsabilidades, renovando as certidões sempre que vencidas e apresentando-as ao setor competente da Unidade Requisitante, quando solicitadas.

6.2.16. Apresentar, sempre que solicitado pela Unidade Requisitante, comprovação de cumprimento das obrigações tributárias e sociais, bem como outras legalmente exigidas.

6.2.17. Arcar com todas as despesas pertinentes ao fornecimento contratado, tais como tributos, fretes, embalagem e demais encargos.

6.2.18. Responder por quaisquer danos ou prejuízos que venham, direta ou indiretamente, por sua culpa ou dolo, a causar à Unidade Requisitante ou a terceiros, durante a execução do fornecimento, inclusive por atos praticados por seus funcionários e prepostos, ficando, assim, afastada qualquer responsabilidade da Unidade Requisitante, podendo esta, para o fim de garantir eventuais ressarcimentos, adotar as seguintes providências:
a) dedução de créditos da licitante vencedora;
b) medida judicial apropriada, a Unidade Requisitante.

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

6.2.20. Comunicar à Unidade Requisitante toda e qualquer alteração de dados cadastrais para atualização.

6.2.21. Respeitar todas as condições impostas pela legislação para a execução do serviço, além das exigências e padrões definidos no Termo de Referência.

6.2.22. Fornecer acesso à console de forma ininterrupta durante todo o tempo de duração do contrato, ficando proibida a expiração do sistema, ou qualquer tipo de redução de funcionalidade, em tempo inferior ao contratado.

6.2.23. A CONTRATADA deverá comprovar que é fornecedora autorizada da solução de segurança fornecida, por meio de declaração emitida pelo fabricante do software antivírus.

6.2.24. A CONTRATADA deverá apresentar pelo menos 01 (um) atestado de capacidade técnica fornecido por pessoa jurídica pública ou privada comprovando aptidão para o fornecimento e suporte em características, quantidades e prazos compatíveis com o objeto do Anexo I.

6.2.25. A CONTRATADA deverá comprovar que possui pelo menos 01 (um) profissional certificado na solução pelo FABRICANTE, para prestação dos serviços de configuração necessários.

6.2.26. A CONTRATADA deverá realizar diagnósticos de problemas e prestar suporte remoto, via conexão de dados segura;

6.2.27. Entregar o objeto contratual, na forma, prazo e local previstos no Anexo I. Caso o atendimento não seja feito dentro do prazo, a CONTRATADA ficará sujeita às sanções previstas em Contrato;

6.2.28. Cumprir o Acordo de Nível de Serviço (SLA) estabelecido no Anexo I. Referente aos serviços de suporte contratados. Item 7.2 do Anexo I.

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

6.2.30. 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;

6.2.31. 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;

6.2.32. 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;

6.2.33. 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 desta contratação;

6.2.34. 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;

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

6.2.36. 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;

6.2.37. Manter, durante toda a vigência do contrato, as condições de habilitação (comprovações de capacidade técnica e demais documentações apresentadas no ato da habilitação), consignadas no Anexo I;

6.2.38. 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, observando as legislações vigentes que tangenciam a proteção de dados como a Lei Geral de Proteção de dados (LGPD – Lei N. 13.709/2018), por exemplo.

6.2.39. 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;

6.2.40. 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;

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

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

6.2.43. 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.

6.2.44. 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;

6.2.45. Atender as demais condições estabelecidas no contrato.

6.3. REQUISITOS DE SEGURANÇA

6.3.1. Deverá ser possível ter um controle de acesso de forma parametrizada, possuindo a definição de perfis de utilização individuais ou de grupos, para que cada usuário ou grupo de usuários possa, ou não, ter acesso a determinados módulos, funções e objetos para a execução de tarefas administrativas ou operacionais conforme demanda.

6.3.2. Registrar um histórico de operações (trilhas de auditoria e registros de controle) no sistema que possa ser consultado contendo data, hora, usuário, função do sistema e dado manipulado, para todas as operações: adições, alterações, consultas, ativações, desativações e exclusões de dados no sistema, a fim de que todo o sistema possa ser auditado.

6.3.3. O sistema deverá estar em conformidade com a Nº 13.709/2018 LGPD (Lei geral de Proteção de Dados) e suas alterações, garantindo a existência de um caminho rápido para a solicitação de informações relacionadas ao tratamento dos dados pessoais caso seja necessário e se aplique.

6.3.4. A solução deve possuir mecanismos de segurança da informação, relacionados à integridade, privacidade e autenticidade dos dados.

6.3.5. A CONTRATADA deverá apresentar relatórios de testes de vulnerabilidades tipo pentest White Box do ambiente em nuvem após a assinatura do contrato e antecedendo a entrada do sistema em produção (de acordo com cronograma de implantação a ser estabelecido), e a cada 6 (seis) meses durante a vigência do contrato, relatando as falhas encontradas e as correções realizadas.

6.3.5.1. Os testes (pentest) deverão ser compostos por:

a) Scan de infraestrutura (análise de portas de serviços, versão dos webservers, versões do kernel servidores Linux), etc.
b) Scan de aplicação (SQL Error Message, Cross-Site Scripting, SQL Disclousure, Directory Browsing, Open Redirect).

6.3.6. O resultado dos testes com as vulnerabilidades encontradas e as correções aplicadas deverão ser entregues em formato digital aos gestores do contrato.

6.3.7. Para o acesso à console de gerenciamento deverá ser provido conexões com certificação segura e criptografadas no transporte das informações (HTTPS). O fornecimento de qualquer certificado necessário para a utilização da console fica sob responsabilidade da CONTRATADA.

6.4. REQUISITOS DE PROTEÇÃO DE DADOS

6.4.1. O ambiente de gestão em nuvem própria (console de gerenciamento) deverá se pautar pelos conceitos de privacy by design e privacy by default, nos moldes previstos nos artigos 46, §2º e 49 da Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/2018).

6.4.2. Devem ser observados os princípios da transparência na coleta de dados; adoção de ações preventivas de segurança de tratamento de dados pessoais; a privacidade por padrão, ou seja, projetar a configuração padrão do produto ou serviço ofertado objetivando sempre a privacidade dos dados; proteção durante todo o ciclo de vida do desenvolvimento do produto ou serviço, isto é, ter a proteção de dados pensada de ponta a ponta; foco no usuário; funcionalidade completa e bem protegida; além de visibilidade e transparência, de modo a permitir que o titular dos dados tenha ciência do processo de coleta com a maior transparência possível.

6.4.3. A console de gerenciamento em nuvem deve oferecer ferramentas de anonimização dos dados pessoais tratados em caso de coleta para cadastro, acesso e auditoria.

6.4.4. A fabricante deverá prover alerta de vazamento de dados, bem como interface com o titular dos dados pessoais (usuário que tenha seus dados coletados) para atendimento dos artigos 9º e 18 da LGPD. A CONTRATADA deverá intermediar o processo.

6.5. REQUISITOS DE INFRAESTRUTURA

6.5.1. Os serviços deverão ser prestados em regime integral, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana sem interrupção, inclusive fora do horário comercial, em finais de semana e feriados. Todos os serviços de Infraestrutura para suportar a presente contratação correrão por conta da Contratada, seja ela hospedada em provedor de nuvem pública ou privada ou ainda, em DataCenter próprio. A PJF não hospedará em suas dependências equipamentos e sistemas da presente contratação.

6.5.2. Os serviços deverão estar disponíveis em 99,7% do tempo contratado, de modo que o somatório mensal das indisponibilidades do serviço seja de, no máximo, 02 (duas) horas.

6.6. REQUISITOS LEGAIS

6.6.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, ao Decreto do Executivo de Juiz de Fora nº 15635/2022, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), Lei n° 10.520, de 17 de julho de 2001, Decreto 10.024, de 20 de setembro de 2019, e a outras legislações aplicáveis, devendo observar ainda posteriores alterações nas legislações supra e aplicáveis.

CLÁUSULA SÉTIMA - DA FISCALIZAÇÃO E ACOMPANHAMENTO

7.1. A CONTRATADA submeter–se–á a todas as medidas e procedimentos de Fiscalização. Os atos de fiscalização, inclusive inspeções e testes, executados pelo CONTRATANTE e/ou por seus prepostos, não eximem a CONTRATADA de suas obrigações no que se refere ao cumprimento das normas, especificações e projetos, nem de qualquer de suas responsabilidades legais e contratuais.

7.2. A Fiscalização da entrega dos bens caberá ao(s) servidor(es) designado(s) por ato do gestor da Unidade Requisitante. Incumbe à Fiscalização a prática de todos os atos que lhe são próprios nos termos da legislação em vigor, respeitados o contraditório e a ampla defesa.

7.3. A CONTRATADA declara, antecipadamente, aceitar todas as decisões, métodos e processos de inspeção, verificação e controle adotados pelo CONTRATANTE, se obrigando a fornecer os dados, elementos, explicações, esclarecimentos e comunicações de que este necessitar e que forem considerados necessários ao desempenho de suas atividades.

7.4. A CONTRATADA se obriga a permitir que o pessoal da fiscalização do CONTRATANTE acesse quaisquer de suas dependências, possibilitando o exame das instalações e também das anotações relativas aos equipamentos, pessoas e materiais, fornecendo, quando solicitados, todos os dados e elementos referentes à execução do contrato.

7.5. Compete à CONTRATADA fazer minucioso exame das especificações dos bens, de modo a permitir, a tempo e por escrito, apresentar à Fiscalização, para o devido esclarecimento, todas as divergências ou dúvidas porventura encontradas e que venham a impedir o bom desempenho do Contrato. O silêncio implica total aceitação das condições estabelecidas.

7.6. A atuação fiscalizadora em nada restringirá a responsabilidade única, integral e exclusiva da CONTRATADA no que concerne aos bens adquiridos, à sua entrega e às consequências e implicações, próximas ou remotas, perante o CONTRATANTE, ou perante terceiros, do mesmo modo que a ocorrência de eventuais irregularidades na execução contratual não implicará corresponsabilidade do CONTRATANTE ou de seus prepostos.

CLÁUSULA OITAVA – SANÇÕES ADMINISTRATIVAS

8.1. A recusa da adjudicatária em assinar o termo de contrato ou em retirar o instrumento equivalente dentro do prazo estabelecido caracteriza o descumprimento total das obrigações assumidas, independentemente do disposto no subitem **13.4** do Edital, sujeitando–a às penalidades previstas no subitem **8.2.**

8.2. Em razão das condutas previstas no art. 155 da Lei Federal n° 14.133/2021, a Unidade Requisitante poderá, sem prejuízo responsabilidade civil e criminal que couber, aplicar as seguintes **sanções**, previstas no art. 156 da Lei Federal nº 14.133/2021:
a) Advertência;
b) Multa;
c) Multa de até 20% (vinte por cento) sobre o valor do Contrato ou do saldo não atendido do Contrato, conforme o caso e respectivamente, nas hipóteses de inadimplemento total ou parcial da obrigação, inclusive nos casos de extinção por culpa da CONTRATADA;
d) Impedimento de licitar e contratar, pelo prazo de até 3 (três) anos;
e) Declaração de inidoneidade para licitar ou contratar.

8.3.A aplicação das sanções previstas nas alíneas “b” e “c” observará os seguintes parâmetros:

8.3.1. 0,1% (um décimo por cento) até 1,0% (um por cento) por dia útil sobre o valor da parcela em atraso do Contrato, em caso de **atraso** no fornecimento, a título de **multa moratória**, limitada a incidência a 15 (quinze) dias úteis. Após o décimo quinto dia útil e a critério da Administração, no caso de fornecimento com atraso, poderá ocorrer a não–aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, atraindo a aplicação da multa prevista na alínea "c", sem prejuízo da rescisão unilateral da avença;

8.3.1. 0,1% (um décimo por cento) até 0,2% (dois décimos por cento) por dia sobre o valor adjudicado em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

8.3.2. 10% (dez por cento) até 15% (quinze por cento) sobre o valor da parcela em atraso do Contrato, em caso de atraso no fornecimento por período superior ao previsto no subitem anterior ou de inadimplemento parcial da obrigação assumida;

8.3.2. 0,1% (um décimo por cento) até 10% (dez por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem acima, ou de inexecução parcial da obrigação assumida;

8.3.3. 15% (quinze por cento) até 20% (vinte por cento) sobre o valor do Contrato ou do saldo não atendido do Contrato, em caso de inadimplemento total da obrigação, inclusive nos casos de extinção por culpa da CONTRATADA; e

8.3.3. 0,1% (um décimo por cento) até 15% (quinze por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida;

8.3.4. 0,1% (um décimo por cento) do valor do Contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará o CONTRATANTE a promover a rescisão do Contrato.

8.3.5. As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

8.4. As sanções somente serão aplicadas após o decurso do prazo para apresentação de defesa prévia do interessado no respectivo processo, no prazo de 15 (quinze) dias úteis, observadas as demais formalidades legais.

8.5. As sanções previstas nas alíneas "a", "d" e "e" do caput desta Cláusula poderão ser aplicadas juntamente com aquelas previstas nas alíneas "b" e "c", e não excluem a possibilidade de rescisão unilateral do Contrato.

8.6. As multas previstas nas alíneas "b" e "c" do item 20.2 não possuem caráter compensatório, e, assim, o pagamento delas não eximirá a CONTRATADA de responsabilidade pelas perdas e danos decorrentes das infrações cometidas.

8.7. 0,2% a 3,2% por dia sobre o valor do contrato, conforme detalhamento constante das tabelas 1 e 2, abaixo.

8.8. 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato;

Tabela 1

GRAU	CORRESPONDÊNCIA
1	0,2% ao dia sobre o valor do contrato
2	0,4% ao dia sobre o valor do contrato
3	0,8% ao dia sobre o valor do contrato
4	1,6% ao dia sobre o valor do contrato
5	3,2% ao dia sobre o valor do contrato

Tabela 2

INFRAÇÃO		
ITEM	**DESCRIÇÃO**	**GRAU**
1	No caso de indisponibilidade crítica que ultrapasse 72 horas de ausência de acesso ao console de gerenciamento impactando significativamente nas atividades correlatas à utilização do console de gerenciamento.	05
2	No caso de indisponibilidade crítica que ultrapasse 48 horas de ausência de acesso ao console de gerenciamento impactando significativamente nas atividades correlatas à utilização do console de gerenciamento.	04
3	No caso de indisponibilidade crítica que ultrapasse 24 horas de ausência de acesso ao console de gerenciamento impactando significativamente nas atividades correlatas à utilização do console de gerenciamento.	03
4	A estabilidade nos módulos gerenciais é fundamental para garantir a eficiência da gestão da proteção aplicada aos computadores do parque tecnológico desta Prefeitura.	02
5	O cumprimento dos acordos de nível de serviço (SLA) estabelecidos no contrato é essencial para assegurar o bom funcionamento da solução de segurança. Em situações em que a empresa não cumprir os prazos estipulados, será considerado infração;	01

8.9. Também ficam sujeitas às penalidades do art. 156, III e IV da Lei nº 14.133, de 2021, as empresas ou profissionais que:

A) tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos
B) tenham praticado atos ilícitos visando a frustrar os objetivos da licitação
C) demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados

8.10. As multas aplicadas poderão ser compensadas com valores devidos à CONTRATADA mediante requerimento expresso nesse sentido.

8.11. Ressalvada a hipótese de existir requerimento de compensação devidamente formalizado, nenhum pagamento será efetuado à CONTRATADA antes da comprovação do recolhimento da multa ou da prova de sua relevação por ato da Administração, bem como antes da recomposição do valor original da garantia, que tenha sido descontado em virtude de multa imposta, salvo decisão fundamentada da autoridade competente que autorize o prosseguimento do processo de pagamento.

8.12. A aplicação das sanções previstas no item 8.2 não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

8.13. A personalidade jurídica poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos nesta Lei ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, a pessoa jurídica sucessora ou a empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o sancionado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

CLÁUSULA NONA – RECURSOS

9.1. A CONTRATADA poderá apresentar:

9.1.1. Recurso a ser interposto perante a autoridade que tiver proferido a decisão recorrida, no prazo de **15 (quinze) dias úteis** contados da intimação da aplicação das penalidades estabelecidas nas alíneas “a”, “b”, “c” e “d” do item 8.2 deste contrato;

9.1.2. Recurso a ser interposto perante a autoridade que tiver proferido a decisão recorrida, no prazo de **3 (três) dias úteis** contados da intimação da extinção do contrato quando promovido por ato unilateral e escrito da Administração;

9.1.3. Pedido de Reconsideração no prazo de**15 (quinze) dias úteis** contados da ciência da aplicação da penalidade estabelecida na alínea “e” do caput da Cláusula anterior;

9.2. Os recursos a que aludem os itens 9.1.1 e 9.1.2 desta cláusula serão dirigidos à autoridade que tiver proferido a decisão recorrida, que, se não reconsiderar a decisão recorrida, encaminhará o recurso com sua motivação à autoridade superior para decisão.

CLÁUSULA DÉCIMA –EXTINÇÃO

10.1. O CONTRATANTE poderá extinguir administrativamente o Contrato, por ato unilateral, na ocorrência das hipóteses previstas no art. 137, incisos I a IX, da Lei Federal nº 14.133/2021, mediante decisão fundamentada, assegurado o contraditório e a ampla defesa, e observado o art. 138, § 2º, da Lei Federal nº 14.133/2021.

10.2. A extinção operará seus efeitos a partir da publicação do ato administrativo no Portal Nacional de Contratações Públicas (PNCP).

10.3. Extinto o Contrato, a CONTRATANTE assumirá imediatamente o seu objeto no local e no estado em que a sua execução se encontrar.

10.4. Na hipótese de extinção por culpa da contratada, a CONTRATADA, além das demais sanções cabíveis, ficará sujeita à **multa** de até 20% (vinte por cento) calculada sobre o saldo reajustado do Contrato, ou, ainda, sobre o valor do Contrato, conforme o caso, na forma do item 8.1, alínea "c", deste Contrato.

10.4.1. A **multa** referida no item anterior não tem caráter compensatório e será descontada do valor da garantia. Se a garantia for insuficiente, o débito remanescente, inclusive o decorrente de penalidades anteriormente aplicadas, poderá ser compensado com eventuais créditos devidos pelo CONTRATANTE.

10.5. Nos casos de extinção com culpa exclusiva da CONTRATANTE, deverão ser promovidos:
a) a devolução da garantia;
b) os pagamentos devidos pela execução do Contrato até a data da extinção;
c) o pagamento do custo de desmobilização, caso haja;
d) o ressarcimento dos prejuízos comprovadamente sofridos.

10.6. Na hipótese de extinção do Contrato por culpa da CONTRATADA, esta somente terá direito ao valor das faturas relativas às parcelas do objeto efetivamente adimplidas até a data da rescisão do Contrato, após a compensação prevista no item **10.4.1** desta Cláusula.

10.7. No caso de extinção amigável, esta será reduzida a termo, tendo a CONTRATADA direito aos pagamentos devidos pela execução do Contrato, conforme atestado em laudo da comissão especial designada para esse fim e à devolução da garantia.

CLÁUSULA DÉCIMA PRIMEIRA - DA CESSÃO E COMUNICAÇÃO

11.1. Havendo incontestável e justificado interesse público e autorização prévia e expressa da Prefeitura, o Contrato poderá ser cedido ou transferido parcialmente.

11.1.1. 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.

11.2. 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.

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

CLÁUSULA DÉCIMA SEGUNDA – DISPOSIÇÕES FINAIS

12.1. A CONTRATADA se obriga a manter, durante todo o período de execução do Contrato, as condições de habilitação jurídica, qualificação técnica, qualificação econômico–financeira, regularidade fiscal e regularidade trabalhista exigidas no Edital por meio do qual foi licitada a aquisição objeto do presente instrumento e o teor da sua proposta de preço, sob pena de rescisão do Contrato;

12.2. Fazem parte do presente contrato as prerrogativas constantes do art. 104 da Lei Federal nº 14.133/2021.

12.3. Na contagem dos prazos, é excluído o dia de início e incluído o do vencimento, e considerar–se–ão os dias consecutivos, salvo disposição em contrário. Os prazos somente se iniciam e vencem em dias de expediente no CONTRATANTE.

CLÁUSULA DÉCIMA TERCEIRA – DISPOSIÇÕES GERAIS E DO FORO

13.1. 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.....

GESTOR(ES) RESPONSÁVEL(IS)

EMPRESA
Representante Legal
Cargo

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

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: E107-383F-271E-2312

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

ARTUR DE HOLLANDA BATITUCCI (CPF 052.XXX.XXX-70) em 12/09/2024 15:42:19 (GMT-03:00)
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://juizdefora.1doc.com.br/verificacao/E107-383F-271E-2312