Governo do Estado de Roraima
Comissão Permanente de Licitação do Estado de Roraima
"*Amazônia: patrimônio dos brasileiros*"

EDITAL DE ABERTURA

PREGÃO ELETRÔNICO Nº: 070/2021
SOB O SISTEMA DE REGISTRO DE PREÇO

PROCESSO Nº: 22101.005846/2021.73 – SEFAZ

1. PREÂMBULO

1.1. O(A) pregoeiro(a) da **Comissão Permanente de Licitação – CPL/RR**, designado(a) pelos **Decreto nº 51-P**, de 11/01/2019 e **Decreto nº 1336-P**, de 07/10/2021, torna público aos interessados que, na forma da **Lei nº 10.520**, de 17/07/2002; do **Decreto nº 29.468-E**, de 13/10/2020, d o **Decreto nº 10.024**, de 20/09/2019, do **Decreto nº 29.467-E**, de 13/10/2020, d a **Lei Complementar nº 123**, de 14/12/2006; e do **Decreto nº 8.538**, de 06/10/2015; aplicando-se, subsidiariamente, a **Lei nº 8.666/93**, de 21/06/1993, realizará licitação na modalidade **Pregão**, na forma **Eletrônica sob o Sistema de Registro de Preços**, mediante as condições estabelecidas neste edital e seus anexos.

2. DA SESSÃO PÚBLICA DO PREGÃO ELETRÔNICO

Dia: 29 de dezembro de 2021

Horário: 09h30 (horário de Brasília/DF)

Endereço Eletrônico: www.comprasgovernamentais.gov.br

Código UASG: 936001

2.1. Este pregão poderá ter a data e horário de abertura da sessão pública transferida, caso ocorra algum fato superveniente que impeça sua abertura na data já definida;

2.2. O edital e seus anexos estarão disponíveis para download nos sítios: **www.comprasgovernamentais.gov.br** e **www.cpl.rr.gov.br** ou no **Protocolo da Comissão Permanente de Licitação – CPL/RR**, localizada na Av. Nossa Senhora da Consolata, 472 – Centro, CEP: 69.301-011, Boa Vista-RR, de **segunda a sexta feira**, no horário das **07h30 às 13h30**, sem qualquer ônus, devendo apenas o interessado dispor de mídia que suporte os respectivos arquivos.

3. DO OBJETO

3.1. Este pregão tem por objeto a **eventual aquisição de software (licença) de proteção antivírus**, de acordo com as quantidades e especificações

técnicas constantes do **TERMO DE REFERÊNCIA – ANEXO I e MODELO DA PROPOSTA DE PREÇOS – ANEXO II** deste edital;

3.2. Este pregão dispõe de apenas 01 (um) **item**, conforme **TERMO DE REFERÊNCIA – ANEXO I e MODELO DA PROPOSTA DE PREÇOS – ANEXO II** deste edital;

3.3. O **critério de julgamento** adotado neste pregão será o de **menor preço**, observadas as exigências contidas neste edital e seus anexos quanto às especificações técnicas do objeto;

3.4. O **intervalo mínimo de diferença entre os lances**, adotado neste pregão, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de **R$ 1,00 (um real).**

3.5. A licitante deverá obedecer rigorosamente aos termos deste edital e seus anexos. Em caso de divergência entre as especificações descritas no Catálogo de Materiais (CATMAT) e Serviços (CATSER) do sistema eletrônico e as especificações constantes do **TERMO DE REFERÊNCIA – ANEXO I e MODELO DA PROPOSTA DE PREÇOS – ANEXO II** deste edital, prevalecerão as especificações dos Anexos mencionados.

4. DA DOTAÇÃO ORÇAMENTÁRIA

4.1. As despesas decorrentes do objeto desta licitação corresponderão ao demonstrativo a seguir:

Nº do Processo	Programa de trabalho	Fonte (Recurso)	Natureza de Despesa
22101.005846/2021.73	04.122.010.4520.9900	101	33.90.40

5. DO REGISTRO DE PREÇOS

5.1. São órgãos participantes deste pregão sob o Sistema de Registro de Preços:

Ord.	Órgão(s) Participante(s)
1.	Secretaria de Estado da Fazenda **- SEFAZ**
2.	Secretaria de Estado da Segurança Pública **- SESP**
3.	Secretaria do Trabalho e Bem - Estar Social - **SETRABES**
4.	Secretaria de Estado de Representação do Governo de Roraima em Brasília **- SERBRAS**
5.	Secretaria de Estado da Agricultura, Pecuária e Abastecimento **- SEAPA**
6.	Secretaria Estadual de Infraestrutura de Roraima **- SEINF**
7.	Secretaria de Estado do Índio **- SEI**
8.	Casa Militar de Roraima **- CM/RR**
9.	Procuradoria-Geral do Estado de Roraima **- PGE/RR**
10.	Comissão Permanente de Licitação do Estado de Roraima **- CPL/RR**
11.	Casa Civil do Estado de Roraima

12.	Secretaria de Estado de Articulação Municipal e Política Urbana **- SEAMPU**
13.	Secretaria de Estado da Cultura **- SECULT**
14.	Polícia Militar do Estado de Roraima **- PM/RR**
15.	Polícia Civil do Estado de Roraima – **PC/RR** Fundo Estadual de Segurança Pública do Estado de Roraima – **FESP/RR**
16.	Secretaria de Estado da Saúde de Roraima **- SESAU**
17.	Secretaria de Estado do Planejamento e Desenvolvimento **- SEPLAN**
18.	Secretaria de Estado de Gestão Estratégica e Administração **- SEGAD**

6. DO CREDENCIAMENTO

6.1. O Credenciamento é o nível básico do registro cadastral no Sistema de Cadastramento Unificado de Fornecedores – SICAF, que permite a participação dos interessados na modalidade licitatória pregão, em sua forma eletrônica;

6.2. O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio **www.comprasgovernamentais.gov.br**, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil;

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

6.4. A licitante responsabiliza-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;

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

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

7. DA PARTICIPAÇÃO NA LICITAÇÃO

7.1. Poderão participar desta licitação:

7.1.1. Empresas que estiverem previamente credenciadas no Sistema de Cadastramento Unificado de Fornecedores – SICAF e no sítio **www.comprasgovernamentais.gov.br** e que detenham ramo de atividade compatível com o objeto desta licitação;

7.1.1.1. Para ter acesso ao sistema eletrônico, os interessados em participar deste pregão deverão dispor de chave de identificação e senha pessoal, informando-se a respeito do funcionamento e regulamento do sistema;

7.1.1.2. O uso da senha de acesso pela é de sua responsabilidade exclusiva, incluindo qualquer transação por ela efetuada diretamente, ou por seu

representante, não cabendo ao provedor do sistema ou à Comissão Permanente de Licitação – CPL/RR responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

7.2. Não poderão participar direta ou indiretamente desta licitação:

7.2.1. Servidor público de qualquer órgão ou entidade vinculada ao órgão promotor da licitação, bem como a empresa da qual tal servidor seja sócio, dirigente ou responsável técnico;

7.2.2. Pessoa física;

7.2.3.Empresas concordatárias, em recuperação judicial ou que tenham tido suas falências declaradas, que se encontrem sob concurso de credores, em dissolução ou em liquidação;

7.2.4. Empresa impedida de licitar e contratar com o Estado, nos termos do art. 7° da Lei nº 10.520, de 17/07/2002;

7.2.5. Empresa suspensa temporariamente de participar de licitação e impedida de contratar com a administração, nos termos do art. 87, inciso III da Lei nº 8.666, de 21/06/1993;

7.2.6. Empresa que tenha sido declarada inidônea para licitar ou contratar com a administração pública, enquanto perdurarem os motivos da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, nos termos do art. 87, inciso IV da Lei nº 8.666, de 21/06/1993. E, caso participe do processo licitatório, estará sujeita às penalidades previstas no Código Penal Brasileiro;

7.2.7. Empresas em regime de consórcio, qualquer que seja sua forma de constituição;

7.2.8. Empresas ou sociedades estrangeiras que não funcionem no país;

7.2.9. Empresas que não estiverem cadastradas no SICAF.

8. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

8.1. A licitante encaminhará a proposta, concomitantemente com os documentos de habilitação exigidos neste edital e seus anexos, **exclusivamente por meio do sistema eletrônico**, até a data e horário estabelecidos para a abertura da sessão pública, quando, então, encerrar-se-á automaticamente a fase de recebimento de propostas e dos documentos de habilitação, **conforme determina o art. 26, do Decreto nº 29.648-E, de 13/10/2020**;

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

8.3. As microempresas e empresas de pequeno porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da LC nº 123, de 14/12/2006;

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

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

8.6. Os documentos complementares à proposta e à habilitação, quando necessários à confirmação daqueles exigidos neste edital e seus anexos e já apresentados, serão encaminhados pela licitante melhor classificada após o encerramento do envio de lances, observado o prazo de que trata o subitem

13.2 deste edital;

8.7. A licitante deverá descrever, no campo "descrição detalhada do objeto ofertado" disponível no sistema, a descrição similar à contida no **TERMO DE REFERÊNCIA – ANEXO I** e no **MODELO DA PROPOSTA DE PREÇOS – ANEXO II** deste edital. Podendo acrescentar quaisquer informações que julgar necessárias ou convenientes, devendo as especificações/informações serem redigida em língua portuguesa, sob pena de desclassificação, caso não atenda às exigências acima descritas;

8.8. Fica vedada a comunicação entre o pregoeiro e as licitantes durante a fase de lances do pregão eletrônico, por meio de "Chat" ou procedimento similar, exceto quanto aos avisos gerais e necessários para o andamento do certame, sendo permitido o contato destes antes e depois da referida fase através de "Chat";

8.9. A licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras sua proposta de preços e lances inseridos em sessão pública;

8.10. A licitante deverá declarar, em campo próprio do sistema eletrônico, que cumpre plenamente os requisitos de habilitação e que sua proposta está em conformidade com as exigências deste edital;

8.11. A licitante deverá declarar, em campo próprio do Sistema, que não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos, salvo menor, a partir de 14 (quatorze) anos, na condição de aprendiz, nos termos do inciso XXXIII, do art. 7º da Constituição Federal;

8.12. A licitante deverá declarar, em campo próprio do sistema, que inexistem fatos supervenientes que impeçam sua habilitação no certame;

8.13. A licitante deverá declarar, em campo próprio do sistema, que a proposta foi elaborada de forma independente, nos termos da Instrução Normativa SLTI/MP nº 02, de 16/09/2009;

8.14. A licitante enquadrada como microempresa ou empresa de pequeno porte deverá declarar, em campo próprio do Sistema, que atende aos requisitos do art. 3º da LC nº 123, de 14/12/2006, para fazer jus aos benefícios nela previstos;

8.15. A declaração falsa relativa ao cumprimento dos requisitos de habilitação, à conformidade da proposta ou ao enquadramento como microempresa ou empresa de pequeno porte ou ao direito de preferência, sujeitará a licitante às sanções previstas neste edital e seus anexos;

8.16. O pregoeiro verificará as propostas de preços enviadas, antes da abertura da fase de lances, desclassificando, motivadamente, aquelas que não estejam em conformidade com os requisitos estabelecidos neste edital e seus anexos, que forem omissas ou apresentarem irregularidades insanáveis.

9. DO PREENCHIMENTO DA PROPOSTA

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

9.1.1. Valor unitário e total do item ou percentual de desconto, conforme o caso;

9.1.2. Marca, Fabricante, Modelo / Versão, conforme exigido no **MODELO DA PROPOSTA DE PREÇOS – ANEXO II** deste edital;

9.1.3. Descrição detalhada do objeto, contendo as informações similares à especificação d o **TERMO DE REFERÊNCIA – ANEXO I** e do **MODELO DA**

PROPOSTA DE PREÇOS – ANEXO II deste edital;

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

10. DA ABERTURA DA SESSÃO PÚBLICA

10.1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico e será aberta pelo pregoeiro com a utilização de sua chave de acesso e senha, na data e horário indicado neste edital;

10.2. Durante a sessão pública, a comunicação entre o pregoeiro e as licitantes ocorrerá exclusivamente mediante troca de mensagens no "chat", em campo próprio do sistema eletrônico;

10.3. Incumbirá à licitante acompanhar as operações no sistema eletrônico durante a sessão pública deste pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem emitida pelo sistema ou de sua desconexão;

11. DA CLASSIFICAÇÃO DAS PROPOSTAS

11.1. As propostas apresentadas serão examinadas quanto ao atendimento das especificações técnicas e condições estabelecidas neste edital e seus anexos, sendo imediatamente desclassificadas aquelas que estiverem em desacordo ou contenham vícios insanáveis;

11.1.1. Qualquer elemento que possa identificar a licitante importará a desclassificação da proposta, sem prejuízo das sanções previstas neste edital e seus anexos;

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

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

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

12. DA FORMULAÇÃO DOS LANCES

12.1. Aberta a etapa competitiva, as licitantes classificadas poderão encaminhar lances sucessivos, exclusivamente por meio do sistema eletrônico, sendo imediatamente informadas do horário e valor consignados no registro de cada lance.

12.2. O lance deverá ser ofertado pelo valor unitário do item ou percentual de desconto, conforme o caso.

12.3. O licitante somente poderá oferecer valor inferior ou maior percentual de desconto ao último lance por ele ofertado e registrado pelo sistema, observado, quando houver, o intervalo mínimo de diferença de valores ou de percentuais entre os lances estabelecido no subitem 3.4 deste edital.

12.4. Não serão aceitos dois ou mais lances iguais e prevalecerá aquele que for recebido e registrado primeiro.

12.5. Durante o transcurso da sessão pública, as licitantes serão informadas, em tempo real, do valor do menor lance registrado, vedada a identificação da licitante.

12.6. Os lances apresentados e levados em consideração para efeito de julgamento serão de exclusiva e total responsabilidade da licitante, não lhe cabendo o direito de pleitear qualquer alteração.

12.7. Durante a fase de lances, o pregoeiro poderá excluir, justificadamente, lance cujo valor seja manifestamente inexequível.

12.8. Na hipótese de o sistema eletrônico desconectar para o pregoeiro no decorrer da etapa de envio de lances da sessão pública e permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

12.9. No caso de a desconexão do pregoeiro persistir no tempo superior a 10 (dez) minutos, a sessão pública do pregão será suspensa e reiniciada somente decorridas 24 (vinte e quatro) horas após a comunicação expressa do fato aos participantes no sítio **www.comprasgovernamentais.gov.br**.

12.10. Neste pregão será adotado para o envio de lances o **modo de disputa "aberto"**, em que as licitantes apresentarão lances públicos e sucessivos, com prorrogações, assim definido no art. 31, inciso I do Decreto nº 29.468-E, de 13/10/2020.

12.10.1. A etapa de lances da sessão pública terá duração de 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 02 (dois) minutos do período de duração da sessão pública.

12.10.2. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de 02 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

12.10.3. Não havendo novos lances na forma estabelecida no subitem anterior, a sessão pública encerrar-se-á automaticamente.

12.10.4. Encerrada a fase competitiva sem que haja a prorrogação automática pelo sistema, nos termos do subitem 12.10.2 deste edital, o pregoeiro poderá, assessorado pela equipe de apoio, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

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

12.12. Por se tratar de licitação não exclusiva para participação de microempresas e empresas de pequeno porte, uma vez 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, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como com as demais classificadas, para o fim de aplicação do disposto nos arts. 44 e 45 da LC nº 123, de 14/12/2006, regulamentada pelo Decreto nº 8.538, de 06/10/2015.

12.13. 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.

12.14. A licitante 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 05 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

12.15. 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 encontrarem no intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

12.16. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrarem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

12.17. 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.

12.18. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 21/06/1993, assegurando-se a preferência, sucessivamente, aos bens e serviços:

12.18.1. Produzidos no País;

12.18.2.Produzidos ou prestados por empresas brasileiras;

12.18.3. Produzidos ou prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

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

12.19. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas, conforme dispõe o art. 37, Parágrafo único, do Decreto nº 29.468-E, de 13/10/2020.

13. DA NEGOCIAÇÃO

13.1. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta à licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste edital e seus anexos;

13.1.1. A negociação será realizada por meio do sistema eletrônico, podendo ser acompanha pelas demais licitantes.

13.2. O pregoeiro solicitará à licitante melhor classificada que, **no prazo de 02 (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 seus anexos e já apresentados, nos termos do art. 38, § 2º do Decreto nº 29.468-E, de 13/10/2020;

13.2.1. A proposta e os documentos de que trata o subitem anterior deverão ser encaminhados devidamente assinados pelo representante legal da licitante.

13.3. Após a fase de negociação de preços, o pregoeiro iniciará a fase de aceitação e julgamento da proposta.

14. DA ACEITABILIDADE DA PROPOSTA VENCEDORA

14.1. Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao **valor máximo** estabelecido para contratação neste edital e seus anexos, observado o disposto no parágrafo único do art. 7º e no §

9º do art. 26 do Decreto nº 29.468-E, de 13/10/2020;

14.2. O pregoeiro poderá convocar a licitante para enviar documento digital complementar, por meio da funcionalidade "**Enviar Anexo**" disponível no sistema, **no prazo de 02 (duas) horas**, sob pena de não aceitação da proposta;

14.2.1. Dentre os documentos passíveis de solicitação pelo pregoeiro, destacam-se os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

14.3. O pregoeiro poderá solicitar parecer de técnicos pertencentes ao quadro geral de pessoal do Governo do Estado de Roraima ou, ainda, de pessoas físicas ou jurídicas estranhas a ele, para orientar sua decisão;

14.4. Não se admitirá proposta que apresente valores simbólicos ou irrisórios, incompatíveis com os preços de mercado, exceto quando se referirem a materiais e instalações de propriedade da licitante, para os quais ela renuncie à parcela ou à totalidade de remuneração;

14.5. Não serão aceitas propostas com valor unitário ou global superior ao estimado ou com preços manifestamente inexequíveis;

14.5.1.Os critérios de aceitabilidade são cumulativos, verificando-se tanto o valor global quanto os valores unitários estimativos da contratação;

14.5.2. Considerar-se-á inexequível a proposta que não venha a ter demonstrada sua viabilidade por meio de documentação que comprove que os custos envolvidos na contratação são coerentes com os de mercado do objeto deste pregão.

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

14.7. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema eletrônico com, no mínimo, 24 (vinte e quatro) horas de antecedência, e a ocorrência será registrada em ata;

14.8. Será desclassificada a proposta que não corrigir ou não justificar eventuais falhas apontadas pelo pregoeiro;

14.9. A licitante que abandonar o certame, deixando de enviar a documentação indicada neste edital e seus anexos, será desclassificada e sujeitar-se-á às sanções previstas neste instrumento convocatório;

14.10. Se a proposta não for aceitável, ou se a licitante não atender às exigências de habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que melhor atenda a este edital e seus anexos;

14.11. Constatado o atendimento às exigências fixadas neste edital e seus anexos, a licitante será declarada vencedora;

14.12. A indicação da licitante vencedora, a classificação dos lances apresentados e demais informações relativas à sessão pública deste pregão constarão de ata divulgada no sistema eletrônico, bem como nos demais meios de publicidade previstos na legislação pertinente.

15. DA HABILITAÇÃO

15.1. Como condição prévia ao exame da documentação de habilitação da licitante detentora da proposta classificada em primeiro lugar, o pregoeiro verificará o eventual descumprimento das condições de participação estabelecidas neste edital e seus anexos, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, **mediante consulta**:

15.1.1. Ao SICAF, a fim de verificar a composição societária das empresas e certificar eventual participação indireta de servidor ou dirigente de órgão ou entidade contratante ou responsável pela licitação, nos termos do art. 9º, inciso III da Lei nº 8.666, de 21/06/1993;

15.1.2. Ao Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça – CNJ, no endereço eletrônico www.cnj.jus.br/improbidade_adm/consultar_requerido.php;

15.1.3. Ao Cadastro Nacional das Empresas Inidôneas e Suspensas – CEIS, no endereço eletrônico http://www.portaltransparencia.gov.br/sancoes/ceis.

15.2. As consultas previstas nas condições anteriores serão realizadas em nome da licitante e também de eventual matriz ou filial e de seu sócio majoritário, por força do art. 12 da Lei n° 8.429, de 02/06/1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário;

15.2.1. Caso conste na consulta de **"Situação do Fornecedor"** a existência de Ocorrências Impeditivas Indiretas, o pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas;

15.2.2. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros;

15.2.3. A licitante será convocada para manifestação previamente à sua desclassificação.

15.3. Constatada a existência de sanção, o pregoeiro reputará a licitante inabilitada, por falta de condição de participação;

15.4. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da LC nº 123, de 14/12/2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente;

15.5. A habilitação das licitantes será verificada por meio do Sistema de Cadastramento Unificado de Fornecedores – SICAF, nos documentos por ele abrangidos, quando os procedimentos licitatórios forem realizados por órgãos ou entidades que aderirem ao SICAF.

15.5.1. Os documentos exigidos para habilitação que não estejam contemplados no SICAF serão enviados nos termos do disposto no art. 43, **§ 1º** do Decreto 29.468-E, de 13/10/2020**;**

15.6. As licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, conforme dispõe o art. 26, § 2º, do Decreto 29.468-E, de 13/10/2020;

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

15.8. O descumprimento do subitem anterior implicará a inabilitação da licitante, exceto se a consulta aos sítios eletrônicos oficiais de órgãos e entidades emissores de certidões, feita pelo pregoeiro, lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme dispõe o art. 43, § 3º do Decreto 29.468-E, de 13/10/2020;

15.9. Sob pena de inabilitação, os documentos encaminhados deverão estar no nome da licitante, com indicação do número de inscrição no CNPJ;

15.10. Se a licitante for a matriz, os documentos de habilitação jurídica e regularidade fiscal e trabalhista deverão estar em nome da matriz, e se a licitante for a filial, os documentos mencionados deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, forem emitidos somente em nome da matriz. Quanto aos atestados de capacidade técnica, quando solicitados, poderão ser apresentados em nome da matriz e/ou filial;

15.11. As microempresas e as empresas de pequeno porte, por ocasião da participação em certames licitatórios, deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal e trabalhista, mesmo que esta apresente alguma restrição, conforme dispõe o art. 43 da LC nº 123, de 14/12/2006;

15.11.1. Havendo alguma restrição na comprovação da regularidade fiscal e trabalhista, será assegurado o prazo de 05 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que o proponente for declarado vencedor do certame, prorrogável por igual período, a critério da administração pública, para regularização da documentação, para pagamento ou parcelamento do débito e para emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa, conforme dispõe o art. 43, § 1º da LC nº 123, de 14/12/2006;

15.11.1.1. A prorrogação do prazo previsto no subitem anterior poderá ser concedida, a critério da Administração Pública, **quando requerida pela licitante**, mediante apresentação de justificativa.

15.11.2. A não-regularização da documentação, no prazo previsto no subitem 15.11.1 deste edital, implicará a decadência do direito à contratação, sem prejuízo das sanções previstas no art. 81 da Lei nº 8.666, de 21/06/1993, sendo facultado à Administração convocar as licitantes remanescentes, na ordem de classificação, para a assinatura do contrato, ou revogar a licitação, conforme dispõe o art. 43, § 2º da LC nº 123, de 14/12/2006;

15.12. Os documentos de habilitação deverão ser encaminhados, concomitantemente com a proposta, exclusivamente por meio do sistema eletrônico, até a data e horário estabelecidos para a abertura da sessão pública;

15.13. Efetuada a verificação referente ao cumprimento das condições de participação no certame, a habilitação das licitantes será realizada mediante a apresentação dos seguintes documentos, **observado o disposto no subitem 15.6 deste edital**:

15.14. HABILITAÇÃO JURÍDICA:

15.14.1. No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

15.14.2. No caso de sociedade empresária ou empresa individual de responsabilidade limitada – EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

15.14.3. No caso de sociedade simples: inscrição do ato constitutivo no

Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

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

15.15. REGULARIDADE FISCAL E TRABALHISTA:

15.15.1. Prova de regularidade com a Fazenda Estadual do domicílio ou sede da licitante;

15.15.2. Prova de regularidade com a Fazenda Municipal do domicílio ou sede da licitante;

15.15.3. Prova de regularidade com a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil – RFB e pela Procuradoria-Geral da Fazenda Nacional – PGFN, referente a todos os tributários federais e à Dívida Ativa da União – DAU por elas administrados, inclusive aqueles relativos à Seguridade Social;

15.15.4. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS), demonstrando a situação regular;

15.15.5. Prova de inexistência de débitos inadimplidos perante a justiça do trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos da Lei nº 12.440, de 07/07/2011, do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 01/05/1943.

15.16. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA:

15.16.1. Certidão negativa de falência ou recuperação judicial ou extrajudicial, expedida pelo distribuidor da sede da pessoa jurídica, há menos de **60 (sessenta) dias** da data prevista para a abertura da licitação, exceto quando dela constar o prazo de validade.

15.17. QUALIFICAÇÃO TÉCNICA:

15.17.1. Apresentar ATESTADO DE CAPACIDADE TÉCNICA, emitido por pessoa jurídica de direito público ou privado, declarando que a licitante já forneceu ou está fornecendo o objeto desta Licitação, compatível em qualidade, quantidade e prazos estabelecidos;

15.17.2. Atestado do fabricante em que comprove uma parceria de no mínimo 03 (três) anos.

16. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

16.1. A proposta final da licitante declarada vencedora deverá ser encaminhada, no prazo estabelecido no subitem 13.2 deste edital, a contar da solicitação do pregoeiro, na forma descrita abaixo:

16.1.1. Constar a descrição detalhada do objeto, as informações similares à especificação do **TERMO DE REFERÊNCIA – ANEXO I** e do **MODELO DA PROPOSTA DE PREÇOS – ANEXO II** deste edital, conforme exigido no item 9 deste edital;

16.1.2. Ser redigida em língua portuguesa, digitada, em uma única via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pela licitante ou seu representante legal;

16.1.3. Constar a Razão Social e CNPJ da empresa, endereço completo, telefone, endereço eletrônico (e-mail), este último se houver, bem como nome do proponente ou de seu representante legal, CPF, RG e cargo na empresa;

16.1.4. Constar a indicação do banco, número da conta e agência da licitante vencedora, para fins de pagamento;

16.1.5. Constar os preços em moeda corrente nacional (Real), o valor unitário em numeral e o valor global em numeral e por extenso (art. 5º da Lei nº 8.666/93), contendo 02 (duas) casas decimais após a vírgula (exemplo: R$ 0,00);

16.1.5.1. 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.

16.1.6. Constar o **PRAZO DE VALIDADE DA PROPOSTA será de, no mínimo, 90 (noventa) dias**, a contar da data de sua apresentação, nos termos do art. 48, § 3º do Decreto 29.468-E, de 13/10/2020. As propostas omissas ou que indicarem prazo inferior serão válidas e consideradas com o prazo mínimo estabelecido neste subitem;

16.1.7. Constar o **PRAZO DE GARANTIA DO OBJETO: Conforme descrito no item 6 do Termo de Referência (Anexo I) deste edital;**

16.2. 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;

16.3. A proposta enviada implicará plena aceitação, por parte da licitante, das condições estabelecidas neste edital e seus anexos.

17. DO RECURSO

17.1. Declarada a vencedora, o pregoeiro abrirá prazo mínimo de 30 (trinta) minutos, durante o qual qualquer licitante poderá, de forma imediata e motivada, em campo próprio do sistema, manifestar sua intenção de recurso;

17.1.1. A falta de manifestação no prazo estabelecido autoriza o pregoeiro a adjudicar o objeto à licitante vencedora;

17.1.2. O pregoeiro examinará a intenção de recurso, aceitando-a ou, motivadamente, rejeitando-a, em campo próprio do sistema;

17.1.3. A licitante que tiver sua intenção de recurso aceita deverá registrar as razões do recurso, em campo próprio do sistema, no prazo de 03 (três) dias, ficando as demais licitantes, desde logo, intimadas a apresentar contrarrazões, também via sistema, em igual prazo, que começará a correr do término do prazo da recorrente.

17.2. O acolhimento do recurso implicará a invalidação apenas dos atos insuscetíveis de aproveitamento;

17.3. Os autos do processo permanecerão com vista franqueada aos interessados, conforme dispõe o art. 109, § 5º da Lei nº 8.666, de 21/06/1993, no endereço mencionado no subitem 2.2 deste edital;

18. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

18.1. O objeto deste pregão será adjudicado pelo pregoeiro, salvo quando houver recurso, hipótese em que a adjudicação caberá à autoridade competente para homologação;

18.2. A homologação eletrônica deste pregão caberá à autoridade competente

da COMISSÃO PERMANENTE DE LICITAÇÃO – CPL/RR;

18.3. A homologação física deste pregão caberá à autoridade competente do órgão originário do processo;

18.4. O objeto deste pregão será adjudicado à licitante vencedora.

19. DA ATA DE REGISTRO DE PREÇOS

19.1. Homologado o resultado da licitação, o adjudicatário terá o prazo de 05 (cinco) dias úteis, contado a partir da data de sua convocação, para assinar a Ata de Registro de Preços, cujo prazo de validade encontra-se nela fixado, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste edital;

19.2. O prazo estabelecido no subitem anterior para assinatura da Ata de Registro de Preços poderá ser prorrogado uma única vez, por igual período, quando solicitado pela(s) licitante(s) vencedor(as), durante o seu transcurso, e desde que ocorra motivo justificado aceito pela administração;

19.3. Serão formalizadas tantas Atas de Registro de Preços quanto necessárias para o registro de todos os itens constantes do **TERMO DE REFERÊNCIA – ANEXO I** e do **MODELO DA PROPOSTA DE PREÇOS – ANEXO II** deste edital, com a indicação da licitante vencedora, a descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais condições;

20. DAS OBRIGAÇÕES DA CONTRATADA E DA CONTRATANTE

20.1. Conforme MINUTA DE CONTRATO – ANEXO IV deste edital.

21. DO PAGAMENTO

21.1. Conforme MINUTA DE CONTRATO – ANEXO IV deste edital.

22. DAS SANÇÕES ADMINISTRATIVAS

22.1. Conforme MINUTA DE CONTRATO – ANEXO IV deste edital.

23. DA IMPUGNAÇÃO AO EDITAL E DOS PEDIDOS DE ESCLARECIMENTO

23.1. Até 03 (três) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa poderá impugnar este edital e seus anexos mediante petição a ser enviada **exclusivamente para o endereço eletrônico pregoeiros.cplrr@gmail.com**;

23.2. O pregoeiro, auxiliado pelo setor técnico competente, decidirá sobre a impugnação no prazo de até 02 (dois) dias úteis, contado da data de recebimento da impugnação;

23.3. Acolhida a impugnação, será designada nova data para a realização do certame, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas, conforme dispõe o art. 21, § 4º da Lei 8.666, de 21/06/1993;

23.4. Os pedidos de esclarecimentos devem ser enviados ao pregoeiro, até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, **exclusivamente para o endereço eletrônico pregoeiros.cplrr@gmail.com**;

23.5. O pregoeiro, auxiliado pelo setor técnico competente, responderá os

pedidos de esclarecimentos no prazo de até 02 (dois) dias úteis, contado da data de recebimento do pedido;

23.6. As respostas às impugnações e aos pedidos de esclarecimentos serão divulgadas no sistema eletrônico e vincularão os participantes e a administração;

23.7. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos neste edital e seus anexos;

23.8. Quando a impugnação ou pedido de esclarecimento tratar de temas alheios à competência do pregoeiro, ou seja, sobre especificações técnicas ou diretamente vinculados ao Termo de Referência, a petição poderá ser encaminhada ao órgão originário do processo para que se pronuncie acerca da demanda, cabendo ao órgão responder no prazo pré-estabelecido. Caso não o faça, o certame deverá ser adiado *"sine-die"*, até que os questionamentos sejam sanados;

24. DAS DISPOSIÇÕES FINAIS

24.1. Quando a licitação tratar de **contratações de bens e serviços de informática**, o pregoeiro poderá solicitar **Parecer Técnico** da **Coordenadoria de Tecnologia da Informação – CTI**, que compõe a estrutura do Centro de Tecnologia de Informação Fazendária – CETIF, da Secretaria de Estado da Fazenda – SEFAZ, para auxiliá-lo em resolução de dúvida específica e pontual que surgir em qualquer fase da licitação, com amparo no **Decreto nº 6.090-E**, de 09/12/2004, e no **PARECER Nº 196/2019/PAD/PGE/RR.** Com exceção da Procuradoria Geral do Estado – PROGE e Secretaria de Estado da Fazenda – SEFAZ, que conforme os **DECRETOS 10.188-E DE 08 DE JUNHO DE 2009 E 10.675-E DE 16 DE NOVEMBRO DE 2009**, respectivamente não se aplica as normas previstas no **DECRETO N. 6.090-E DE 9 DE DEZEMBRO DE 2004**;

24.2. A autoridade competente para homologar este procedimento licitatório, poderá revogá-lo somente em razão do interesse público, por motivo de fato superveniente devidamente comprovado, pertinente e suficiente para justificar a revogação, e deverá anulá-lo por ilegalidade, de ofício ou por provocação de qualquer pessoa, por meio de ato escrito e fundamentado;

24.2.1. A anulação do pregão induz à do contrato;

24.2.2. As licitantes não terão direito à indenização em decorrência da anulação do procedimento licitatório, ressalvado o direito do contratado de boa-fé de ser ressarcido pelos encargos que tiver suportado no cumprimento do contrato.

24.3. É facultado ao pregoeiro e à autoridade superior, em qualquer fase deste pregão, promover diligência destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de informação ou documentos que deveriam ter sido apresentados para fins de classificação e habilitação;

24.4. 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 decisão fundamentada, registrada em ata e acessível a todos, e lhes atribuirá validade e eficácia para fins de habilitação e classificação, observando o disposto na Lei nº 418 de 15/01/2004;

24.5. Não serão aceitos **"protocolos de entrega"** ou **"solicitação/requerimento de documento"** em substituição aos documentos exigidos neste edital e seus anexos;

24.6. A **proposta** e os **documentos de habilitação** exigidos neste edital e seus anexos, **caso sejam solicitados**, deverão ser encaminhados, em prazo a ser estabelecido pelo pregoeiro, na forma **original** ou de acordo com o disposto na Lei nº 13.726, de 08/10/2018, à **COMISSÃO PERMANENTE DE LICITAÇÃO**

– CPL/RR, localizada na **Av. Nossa Senhora da Consolata, 472 – Centro, CEP: 69.301-011, Boa Vista-RR**;

24.7. Qualquer modificação neste edital e seus anexos será divulgada pela mesma forma que se deu o texto original, reabrindo-se o prazo inicialmente estabelecido, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas, nos termos art. 21, § 4º da Lei nº 8.666, de 21/06/1993;

24.8. As licitantes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase desta licitação;

24.9. Após apresentação da proposta não caberá desistência, salvo por motivo justo decorrente de fato superveniente e aceito pelo pregoeiro;

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

24.11. As normas disciplinadoras desta 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;

24.12. Na contagem dos prazos estabelecidos neste edital e seus anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento, e considerar-se-ão os dias consecutivos, exceto quando for explicitamente disposto em contrário. Só se iniciam e vencem os referidos prazos em dia de expediente nesta COMISSÃO PERMANENTE DE LICITAÇÃO – CPL/RR, nos termos do art. 110 da Lei nº 8.666, de 21/06/1993;

24.13. Quaisquer informações complementares sobre este edital e seus anexos, poderão ser obtidas pelo e-mail **pregoeiros.cplrr@gmail.com**;

24.14. O resultado desta licitação será publicado no Diário Oficial do Estado de Roraima (**www.imprensaoficial.rr.gov.br**), no Diário Oficial da União (**www.in.gov.br**), quando se tratar de recursos federais, e divulgado em Jornal de grande circulação local, no sítio **www.comprasgovernamentais.gov.br**, no sítio desta Comissão Permanente de Licitação – CPL/RR (**www.cpl.rr.gov.br**) e afixado no Quadro de Avisos desta Comissão Permanente de Licitação – CPL/RR;

24.15. Aplica-se à presente licitação, subsidiariamente, a **Lei nº 8.078 – Código de Proteção e Defesa do Consumidor**, de 11/09/1990, e demais normas legais pertinentes;

24.16. As minutas deste edital foram elaboradas pelos seguintes setores desta Comissão Permanente de Licitação - CPL/RR: Departamento de Apoio Operacional – DAO (Minuta do edital - ep. 3540469) e Assessoria Especializada (Minuta do contrato - ep. 3561752), em estrita consonância com as regras definidas pela Secretaria de Estado Solicitante em seu Termo de Referência, cujo teor foi transcrito na íntegra no anexo I deste edital;

24.17. Ao pregoeiro designado para conduzir este certame coube a revisão do edital, o ato de divulgação da abertura da sessão e sua consequente condução até a conclusão, e demais atribuições legalmente previstas, especialmente no art. 17 do Decreto nº 29.468-E de 13 de outubro de 2020.

25. DOS ANEXOS

25.1. ANEXO I – TERMO DE REFERÊNCIA;

25.2. ANEXO I-A **–** INFORMAÇÕES COMPLEMENTARES

25.3. ANEXO II – MODELO DA PROPOSTA DE PREÇOS;

25.4. ANEXO III – MINUTA DA ATA DE REGISTRO DE PREÇOS;

25.5. ANEXO IV – MINUTA DE CONTRATO.

26. DO FORO

26.1. O Foro para dirimir os possíveis litígios que decorrerem do presente procedimento licitatório será o da comarca de Boa Vista/RR.

Boa Vista – RR, 14 de dezembro de 2021.

KETWLLEN MONIQUI FERREIRA DE CARVALHO
Pregoeira da CPL/RR

ANEXO I

TERMO DE REFERÊNCIA N° 13 /2021

1. OBJETO

1.1. Eventual aquisição de software (licença) de proteção antivírus para atender as necessidades da Secretaria de Estado da Fazenda – SEFAZ/RR, conforme especificações, quantidades e exigências estabelecidas neste Termo e em seu Anexo I.

1.1.1 O objeto deverá ser entregue de acordo com as especificações técnicas mínimas (Anexo I). A aquisição a ser realizada deve compreender antivírus corporativo Kaspersky Endpoint Security for Business Advanced, visando a utilização de solução de AntiMalware, abrangendo: ativação da licença e transferência de conhecimento, com garantia de atualizações e suporte técnico por período de 36 (trinta e seis) meses.

1.2. A licitação deverá ser realizada na modalidade Pregão, na forma eletrônica, sob o Sistema de Registro de Preços, cujo critério de julgamento das propostas será: menor preço do item.

2. FUNDAMENTAÇÃO LEGAL

2.1. Lei nº 8.666/1993, que institui normas para licitações e contratos da Administração Pública;

2.2. Lei 8.078, de 11/09/1990, que dispõe sobre a proteção do consumidor e dá outras providências (Código de Defesa do Consumidor);

2.3. Lei nº 10.520/2002, que dispõe sobre o Pregão Eletrônico como modalidade de licitação;

2.4. Lei Complementar nº 147, de 7 de agosto de 2014 que altera a Lei Complementar nº 123 /2006, institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte;

2.5. Decreto nº 19.213-E, de 23 de julho de 2015, que regulamenta a fiscalização dos contratos no âmbito da Administração Pública Direta e Indireta do Estado de Roraima;

2.6. Decreto nº 29.467 – E, de 13/10/2020, que regulamenta o Sistema de Registro de Preços – SRP no âmbito do Estado de Roraima;

2.7. Decreto nº 29.468 – E, de 13/10/2020, que regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns no âmbito do Estado de Roraima;

2.8. Decreto nº 29.593-E de 13/11/2020, que regulamenta os procedimentos para registro de preços concernentes à aquisição de bens comuns e prestação de serviços comuns a serem executados de forma centralizada pela administração direta do Estado de Roraima.

3. **JUSTIFICATIVA**

3.1. O Centro de Tecnologia da Informação Fazendária – CETIF da SEFAZ/RR, por meio da Coordenadoria de Infraestrutura de TI – CITI atua diretamente nas ações de segurança da rede multisserviços denominada NetFisco-RR, e recomenda que é imprescindível a aquisição do antivírus corporativo tendo em vista que as licenças atuais encerram o suporte em dezembro de 2021, conforme Contrato Nº 06/2018 celebrado entre a SEFAZ/RR e a empresa VTech Comércio, Serviços e Equipamentos de Informática Eirelli EPP, publicado no Diário Oficial nº 3359,de 21/11/2018;

3.2. A descontinuidade do serviço de proteção do antivírus corporativo, junto aos ativos do parque computacional que provém os sistemas corporativos da SEFAZ/RR impedirá as atribuições diárias desta secretaria relacionadas aos serviços de Tecnologia da Informação e Comunicação – TIC. Ressalta-se que em um órgão com as atribuições relevantes ao Estado como é a SEFAZ/RR, não tem como realizar suas atividades fim sem o suporte do serviço do antivírus corporativo, a ausência desse recurso influencia diretamente na: Entrada de vírus e spams; E-mails maliciosos; Ataque e intrusão na rede; Roubo de senhas; Implantação de sistemas maliciosos; Lentidão na rede NetFisco-RR; Acesso indevido a documentos compartilhados; Perda de dados e informações importantes da SEFAZ-RR; Indisponibilidade dos serviços corporativos;

3.3. Sabe-se que novos vírus e ameaças digitais aos sistemas computacionais são criados diariamente, sendo necessária a atualização constante da versão dos softwares de antivírus, das vacinas de proteção e do suporte para auxílio na resolução de incidentes relacionados a estas ameaças;

3.4. Conforme contrato 06/2018, a solução utilizada atualmente é a Kaspersky Endpoint Security for Business Advanced, tem funcionado a contento, e no momento, se mostra apropriada em relação ao custo x benefício para a SEFAZ/RR, sendo necessária a adequação do quantitativo de licenças que se encontram disponibilizadas ao total efetivo de máquinas existentes (e futuros) no parque computacional da secretaria;

3.5. A curva de aprendizagem é um outro importante ponto considerado para manter com a solução já implantada. Caso haja a adoção de outra solução acarretará na diminuição da curva e no aumento do tempo para o domínio de uma nova ferramenta haja vista que os analistas e técnicos que trabalham diretamente com a proteção do parque computacional da SEFAZ/RR já possuem

domínio sobre a ferramenta Kaspersky Endpoint Security for Business Advanced, sendo esta contratação apenas a expansão da cobertura atual vigente dos ativos, seguindo também a padronização necessária para este tipo de rotina;

3.6. Ainda em relação a padronização, uma eventual alteração da atual plataforma enseja na retirada deste software para instalação de uma nova ferramenta de proteção, tendo em vista a dimensão do parque computacional (sede na capital e agências no interior do estado) tal atividade levaria um tempo considerado, o que poderia ensejar em uma janela de vulnerabilidade significativa;

3.7. Por fim, cumpre destacar que apesar das plataformas de antivírus seguirem o mesmo direcionamento em linhas gerais (proteção contra ameaças), os softwares não se comunicam entre si, levando a uma dificuldade na padronização de políticas, atualização das bases de conhecimento e gerenciamento do ambiente como um todo;

3.8. Os quantitativos de licenças de software para aquisição foram definidos conforme especificações da Coordenadoria de Infraestrutura de TI – CITI, e também baseado no contrato anterior firmado pela SEFAZ/RR, sendo o Contrato nº 06/2018, cujo objeto foi renovação e atualização de licenças de software antivírus Kaspersky.

4. CLASSIFICAÇÃO DOS BENS COMUNS

4.1. A natureza do objeto a ser adquirido é definida como bens comuns, nos termos do Parágrafo único do Art. 1° da Lei nº 10.520, de 17/07/2002; E inciso II, Art. 3º, do Decreto nº 29.468 – E, de 13/10/2020; Bem como Art. 2° do Decreto nº 29.593-E de 13/11/2020.

5. LOCAL DA ENTREGA, PRAZO E CRITÉRIOS DE ACEITAÇÃO DO OBJETO

5.1. A entrega das licenças deverá ser realizada em meio eletrônico, com código de ativação das chaves de licenciamento, via e-mail indicado pelo (a) Fiscal do contrato;

5.2. O fornecimento ocorrerá conforme necessidade da Contratante. O prazo de entrega será de até 10 (dez) dias úteis contados a partir do recebimento da Nota de Empenho, acompanhada do Pedido de Fornecimento devidamente autuado pelo setor competente;

5.3. As licenças serão recebidos provisoriamente no prazo de 10 (dez) dias úteis, pelo(a) responsável por acompanhar e fiscalizar o contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Anexo I neste Termo de Referência;

5.4. As licenças poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 05 (cinco) dias úteis, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades;

5.5. As licenças serão recebidos definitivamente no prazo de 10 (dez) dias úteis, contados do recebimento provisório, após a verificação da qualidade e quantidade e consequente aceitação mediante termo circunstanciado;

5.6. Na hipótese da verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo;

5.7. O recebimento provisório ou definitivo do objeto não exclui a

responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

6. GARANTIAS, TRANSFERÊNCIA DE CONHECIMENTO E SUPORTE TÉCNICO

6.1. Dispor garantia de reposição e/ou correção da solicitação pendente em caso de constatação de erro técnico nas licenças, no prazo máximo de 05 (cinco) dias úteis após a emissão das licenças;

6.2. As licenças deverão possuir garantia de atualizações e suporte técnico por período de 36 (trinta e seis) meses;

6.3. A transferência de conhecimento deverá incluir a implementação, ativação e configuração, proporcionando a habilidade para configurar e administrar a solução proposta, sendo capaz de passar este conhecimento a outros usuários da Instituição;

6.4. A CONTRATADA deverá transferir o conhecimento de toda solução, demonstrando todas as suas funcionalidades para, pelo menos, dois servidores do CONTRATANTE, em uma carga horária mínima de 10 horas, preferencialmente na modalidade virtual (remota), para que estes repliquem este conhecimento para as equipes de suporte do CONTRATANTE. De acordo com o perfil, ao final, os servidores do CETIF/SEFAZ/RR deverão estar aptos, pelo menos, à: Ser administradores do Sistema; Alterar as configurações e políticas em todas as suas aplicações conforme políticas da SEFAZ/RR; Compreender o ambiente tecnológico associado a solução e ao processo de configuração disponível; Realizar toda e qualquer atividade para permitir a correta configuração da solução possibilitando a operacionalização do sistema por parte dos Administradores;

6.5. Deverá também elaborar e fornecer os documentos técnicos e manuais de toda a solução.

7. OBRIGAÇÕES DA CONTRATANTE

7.1. São obrigações da Contratante:

7.1.1. Receber o objeto no prazo e condições estabelecidas neste Termo de Referência e em seu Anexo I;

7.1.2. Verificar minuciosamente, no prazo fixado, a conformidade do objeto recebido provisoriamente com as especificações constantes no Anexo I e na proposta, para fins de aceitação e recebimento definitivo;

7.1.3. Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

7.1.4. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado;

7.1.5. Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos neste Termo de Referência e em seu Anexo I;

7.2. A Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

8. OBRIGAÇÕES DA CONTRATADA

8.1. A Contratada deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

8.1.1. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Termo de Referência e em seu Anexo I, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo/versão, procedência e prazo de garantia;

8.1.2. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

8.1.3. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos;

8.1.4. Comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

8.1.5. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

8.1.6. Durante todo o período de garantia deverá ser disponibilizado para a instalação em até 15 dias de seu lançamento, todas as atualizações de produto, assim como, novas versões;

8.1.7. Comprovar a existência de equipe técnica com no mínimo 2 (dois) profissionais capacitados e certificados pelo fabricante.

9. QUALIFICAÇÃO TÉCNICA

9.1. Apresentar ATESTADO DE CAPACIDADE TÉCNICA, emitido por pessoa jurídica de direito público ou privado, declarando que a licitante já forneceu ou está fornecendo o objeto desta Licitação, compatível em qualidade, quantidade e prazos estabelecidos;

9.2. Atestado do fabricante em que comprove uma parceria de no mínimo 03 (três) anos.

10. FISCALIZAÇÃO

10.1. A execução do contrato será acompanhada por representante(s) do Contratante, denominado(a) FISCAL(IS), especialmente designado(s) para esse fim, nos termos do Decreto n° 19.213-E de 23 de julho de 2015.

10.2. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante a terceiros, por qualquer irregularidade resultante de imperfeições técnicas, emprego de materiais inadequados ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade do Contratante ou de seus agentes e prepostos (Art.70 da Lei n° 8.666/93).

11. PAGAMENTO

11.1. O CONTRATANTE efetuará o pagamento, mediante ordem bancária

creditada em conta corrente indicada pela Contratada, em até 30 (trinta) dias após o protocolo da Nota Fiscal e/ou Fatura, devidamente atestada pela Contratante;

11.2. Nenhum pagamento será efetuado à Contratada, enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência.

12. VIGÊNCIA

12.1. O prazo de vigência do Contrato obedecerá ao disposto no caput do Art. 57 da Lei 8.666/93 e suas alterações, a contar da data da sua assinatura, tendo sua validade e eficácia legal após a publicação do seu extrato do Diário Oficial do Estado;

12.2. A ata de registro de preços terá validade de 12 (doze) meses, a contar da data da sua assinatura, tendo sua validade e eficácia legal após a publicação do seu extrato do Diário Oficial do Estado;

13. SANÇÕES ADMINISTRATIVAS

13.1. O descumprimento total ou parcial das condições estabelecidas neste instrumento poderá acarretar na aplicação das sanções administrativas previstas nos Arts. 86 a 88 da Lei n° 8.666/93, Art. 7º da Lei nº 10.520/2002 e Art. 49 do Decreto n° 29.468-E/2020, ressalvado o direito da CONTRATANTE de rescindir administrativamente o contrato, conforme art. 77 da Lei nº 8.666/1993.

14. ESTIMATIVA DE PREÇOS

14.1. Os preços foram obtidos conforme Art. 5º da Instrução Normativa nº 73, de 05/08/2020;

14.2. O custo estimado para a despesa pretendida é de R$59.500,00 (cinquenta e nove mil e quinhentos reais).

ITEM	DESCRIÇÃO	UND	QTD	VALOR UNITÁRIO ESTIMADO	VALOR TOTAL ESTIMADO
1	Aquisição de software (licenças) de proteção antivírus Kaspersky EndPoint Security for Business Advanced, incluindo transferência de conhecimento, com garantia de atualizações e suporte técnico por período de 36 (trinta e seis) meses. Observação: Considerar a unidade de fornecimento "licença".	Unidade	350	R$170,00	R$59.500,00

TOTAL		R$59.500,00

15. **RECURSOS ORÇAMENTÁRIOS**

15.1. As despesas decorrentes da aquisição do objeto deste Termo de Referência correrão à conta:

a) Unidade orçamentária: 22101

b) Programa de trabalho: 04.122.010.4520.9900

c) Elemento de despesas: 33.90.40

d) Fonte de recurso: 101

e) Tipo do empenho: estimativo

16. RESPONSÁVEL PELO TERMO DE REFERÊNCIA

16.1. Secretaria de Estado da Fazenda de Roraima – SEFAZ/RR.

16.1.1. Centro de Tecnologia da Informação Fazendária - CETIF/SEFAZ/RR

Boa Vista/RR, data registrada no sistema.

Elaborado por:

(Assinatura eletrônica)
CLENYA REJANE BARROS DE LIMA
Analista de Sistema – CETIF/SEFAZ/RR

De acordo:

(Assinatura eletrônica)
KLEBER DA SILVA LYRA
Secretário Adjunto - CETIF/SEFAZ/RR

Aprovo:

(Assinatura eletrônica)
MANOEL SUEIDE FREITAS
Secretário Adjunto de Estado da Fazenda - SEFAZ/RR

ANEXO I DO TERMO DE REFERÊNCIA

ESPECIFICAÇÕES MÍNIMAS E DETALHAMENTO DO OBJETO

ITEM	DESCRIÇÃO	UND	QTD

1	Aquisição de software (licenças) de proteção antivírus Kaspersky EndPoint Security for Business Advanced, incluindo transferência de conhecimento, com garantia de atualizações e suporte técnico por período de 36 (trinta e seis) meses. Observação: Considerar a unidade de fornecimento "licença".	Unidade	350

1. DO SERVIDOR DE ADMINISTRAÇÃO E CONSOLE ADMINISTRATIVA

1.1. Compatibilidade

1.1.1. Microsoft Windows Server 2003 (Todas edições);

1.1.2. Microsoft Windows Server 2008 (Todas edições);

1.1.3. Microsoft Windows Server 2008 x64 SP1 (Todas edições);

1.1.4. Microsoft Windows Server 2008 R2 (Todas edições);

1.1.5. Microsoft Windows Server 2012 (Todas edições);

1.1.6. Microsoft Windows Server 2012 R2 (Todas edições);

1.1.7. Microsoft Windows Server 2016 x64 ou superior;

1.1.8. Microsoft Windows Small Business Server 2008 (Todasedições);

1.1.9. Microsoft Windows Small Business Server 2011 (Todasedições);

1.1.10. Microsoft Windows XP Professional x32 e x64 SP2 ou superior;

1.1.11. Microsoft Windows Vista Business / Enterprise / Ultimate x32 e x64 SP1 ou posterior;

1.1.12. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;

1.1.13. Microsoft Windows 8 SP1 Professional / Enterprise x32/x64;

1.1.14. Microsoft Windows 8 Professional / Enterprise x64;

1.1.15. Microsoft Windows 8.1 Professional / Enterprise x32;

1.1.16. Microsoft Windows 8.1 Professional / Enterprise x64;

1.1.17. Microsoft Windows 10 todas edições x32 e x64 ou superior;

1.1.18. Microsoft Windows Server 2003 (Todas edições);

1.1.19. Microsoft Windows Server 2008 (Todas edições);

1.1.20. Microsoft Windows Server 2008 x64 SP1 (Todas edições);

1.1.21. Microsoft Windows Server 2008 R2 (Todas edições);

1.1.22. Microsoft Windows Server 2012 (Todas edições);

1.1.23. Microsoft Windows Server 2012 R2 (Todas edições);

1.1.24. Microsoft Windows Server 2016 x64 ou superior;

1.1.25. Microsoft Windows Server 2019 64-bit;

1.1.26. Microsoft Windows Small Business Server 2008 (Todasedições);

1.1.27. Microsoft Windows Small Business Server 2011 (Todasedições);

1.1.28. Microsoft Windows XP Professional x32 e x64 SP2 ou superior;

1.1.29. Microsoft Windows Vista Business / Enterprise / Ultimate x32 e x64 SP1

ou posterior;

1.1.30. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;

1.1.31. Microsoft Windows 8 SP1 Professional / Enterprise x32/x64;

1.1.32. Microsoft Windows 8 Professional / Enterprise x64;

1.1.33. Microsoft Windows 8.1 Professional / Enterprise x32;

1.1.34. Microsoft Windows 8.1 Professional / Enterprise x64;

1.1.35. Microsoft Windows 10 todas as edições x32 e x64 ou superior.

1.2. Suportar as seguintes bases de dados

1.2.1. Microsoft sql server 2008 express 32-bits;

1.2.2. Microsoft sql server 2008 r2 express 64-bits;

1.2.3. Microsoft sql server 2012 express 64-bits;

1.2.4. Microsoft sql server 2014 express 64-bits;

1.2.5. Microsoft sql server 2016 express 64-bits;

1.2.6. Microsoft sql server 2017 express 64-bits;

1.2.7. Microsoft sql server 2008 (todas as versões) 32-bit/64-bits;

1.2.8. Microsoft sql server 2008 r2 (todas as versões) 64-bits;

1.2.9. Microsoft sql server 2008 r2 service pack 2 (todas as versões) 64-bits;

1.2.10. Microsoft sql server 2012 (todas as versões) 64-bits;

1.2.11. Microsoft sql server 2014 (todas as versões) 64-bits;

1.2.12. Microsoft sql server 2016 (todas as versões) 64-bits;

1.2.13. Microsoft sql server 2017 on windows 64-bits;

1.2.14. Mysql standard edition 5.6 32-bit/64-bits;

1.2.15. Mysql enterprise edition 5.6 32-bit/64-bits;

1.2.16. Mysql standard edition 5.7 32-bit/64-bits;

1.2.17. Mysql enterprise edition 5.7 32-bit/64-bits.

1.3. Características

1.3.1. A console deverá ser acessada via WEB (HTTPS) ou MMC;

1.3.2. Console deverá ser baseada no modelo cliente/servidor;

1.3.3. Compatibilidade com Windows FailoverClustering ou outra solução de alta disponibilidade;

1.3.4. Permitir a instalação e configuração da console de gerenciamento em modo híbrido;

1.3.5. Deve permitir incluir usuários do AD para logaremna console de administração;

1.3.6. Deverá permitir a atribuição de perfis para os administradores da Solução de AntiMalware;

1.3.7. Deverá permitir incluir usuários do AD para logaremna console de administração

1.3.8. Console deverá ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;

1.3.9. As licenças deverão ser perpétuas, ou seja, expirado a validade do produto deverá permanecer funcional para a proteção contra códigos maliciosos

utilizando as definições até o momento da expiração do suporte da licença;

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

1.3.11. Capacidade de instalar remotamente a solução de AntiMalware nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;

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

1.3.13. Deverá armazenar histórico das alterações feitas em políticas;

1.3.14. Deverá permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;

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

1.3.16. A solução de gerência deverá permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

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

1.3.18. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Android e Windows;

1.3.19. Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;

1.3.20. A solução de gerência centralizada deverá permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

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

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

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

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

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

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

1.3.27. Capacidade de fazer distribuição remota de qualquer software, ou seja, deverá ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de AntiMalware para que seja instalado nas máquinas clientes;

1.3.28. A comunicação entre o cliente e servidor de administração deverá ser criptografada;

1.3.29. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

1.3.30. Deverá permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

1.3.31. Nome do computador;

1.3.32. Nome do domínio;

1.3.33. Range de IP;

1.3.34. Sistema Operacional;

1.3.35. Máquina virtual.

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

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

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

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

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

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

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

1.3.43. Deverá fornecer as seguintes informações dos computadores:

1.3.43.1. Se o AntiMalware está instalado;

1.3.43.2. Se o AntiMalware está iniciado;

1.3.43.3. Se o AntiMalware está atualizado;

1.3.43.4. Minutos/horas desde a última conexão da máquina com o servidor administrative;

1.3.43.5. Minutos/horas desde a última atualização de vacinas;

1.3.43.6. Data e horário da última verificação executada na máquina;

1.3.43.7. Versão do AntiMalware instalado na máquina;

1.3.43.8. Se é necessário reiniciar o computador para aplicar mudanças;

1.3.43.9. Data e horário de quando a máquina foi ligada;

1.3.43.10. Quantidade de vírus encontrados (contador) na máquina;

1.3.43.11. Nome do computador;

1.3.43.12. Domínio ou grupo de trabalho do computador;

1.3.43.13. Data e horário da última atualização de vacinas;

1.3.43.14. Sistema operacional com Service Pack;

1.3.43.15. Quantidade de processadores;

1.3.43.16. Quantidade de memória RAM;

1.3.43.17. Usuário (s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);

1.3.43.18. Endereço IP;

1.3.43.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;

1.3.43.20. Atualizações do Windows Updates instaladas;

1.3.43.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;

1.3.43.22. Vulnerabilidades de aplicativos instalados na máquina;

1.3.44. Deverá permitir bloquear as configurações do AntiMalware instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

1.3.45. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

1.3.45.1. Alteração de Gateway Padrão;

1.3.45.2. Alteração de subrede;

1.3.45.3. Alteração de domínio;

1.3.45.4. Alteração de servidor DHCP;

1.3.45.5. Alteração de servidor DNS;

1.3.45.6. Alteração de servidor WINS;

1.3.45.7. Resolução de Nome;

1.3.45.8. Disponibilidade de endereço de conexão SSL;

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

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

1.3.47. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de AntiMalware;

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

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

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

1.3.51. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;

1.3.52. Capacidade de gerar traps SNMP para monitoramento de eventos;

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

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

1.3.55. Deverá encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;

1.3.56. Deverá possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;

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

1.3.58. Deverá possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).

1.3.59. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc.), inclusive de máquinas que estejam em subnets diferentes do servidor;

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

1.3.61. Deverá através de opções de otimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o AntiMalware ativo, porém sem comprometer o desempenho do computador;

1.3.62. Deverá permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);

1.3.63. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação;

1.3.64. Deverá ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;

1.3.65. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

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

1.3.66.1. Nome do vírus;

1.3.66.2. Nome do arquivo infectado;

1.3.66.3. Data e hora da detecção;

1.3.66.4. Nome da máquina ou endereço IP;

1.3.66.5. Ação realizada.

1.3.67. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

1.3.68. Capacidade de listar updates nas máquinas com o respectivo link para download;

1.3.69. Deverá criar um backup de todos os arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;

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

1.3.71. Capacidade de realizar inventário de hardware de todas as máquinas clientes;

1.3.72. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;

1.3.73. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

1.4. Criptografia

1.4.1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;

1.4.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

1.4.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;

1.4.4. Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;

1.4.5. Permitir criar vários usuários de autenticação pré-boot;

1.4.6. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;

1.4.7. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

1.4.7.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

1.4.7.2. Criptografar todos os arquivos individualmente;

1.4.7.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

1.4.7.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

1.4.8. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;

1.4.9. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

1.4.10. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

1.4.11. Verificar compatibilidade de hardware antes de aplicar a criptografia;

1.4.12. Possibilita estabelecer parâmetros para a senha de criptografia;

1.4.13. Bloqueia o reuso de senhas;

1.4.14. Bloqueia a senha após um número de tentativas pré-estabelecidas;

1.4.15. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

1.4.16. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo;

1.4.17. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;

1.4.18. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

1.4.19. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de áudio, etc;

1.4.20. Permite criar um grupo de extensões de arquivos a serem criptografados;

1.4.21. Capacidade de criar regra de criptografia para arquivos gerados por

aplicações;

1.4.22. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento;

1.4.23. Capacidade de deletar arquivos de forma segura após a criptografia;

1.4.24. Capacidade de criptografar somente o espaço em disco utilizado;

1.4.25. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;

1.4.26. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;

1.4.27. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;

1.4.28. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;

1.4.29. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;

1.4.30. Capacidade de fazer “Hardware encryption”;

1.5. Gerenciamento de sistemas

1.5.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;

1.5.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;

1.5.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;

1.5.4. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;

1.5.5. Capacidade de gerenciar licenças de softwares de terceiros;

1.5.6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;

1.5.7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc.), informando data de compra, local onde se encontra, servicetag, número de identificação e outros;

1.5.8. Possibilita fazer distribuição de software de forma manual e agendada;

1.5.9. Suporta modo de instalação silenciosa;

1.5.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;

1.5.11. Possibilita fazer a distribuição através de agentes de atualização;

1.5.12. Utiliza tecnologia multicast para evitar tráfego na rede;

1.5.13. Possibilita criar um inventário centralizado de imagens;

1.5.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;

1.5.15. Suporte a WakeOnLan para deploy de imagens;

1.5.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;

1.5.17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;

1.5.18. Capacidade de gerar relatórios de vulnerabilidades e patches;

1.5.19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;

1.5.20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;

1.5.21. Permite baixar atualizações para o computador sem efetuar a instalação

1.5.22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;

1.5.23. Capacidade de instalar correções de vulnerabilidades de acordo com a Severidade;

1.5.24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;

1.5.25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc.;

1.5.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;

1.5.27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;

1.5.28. Capacidade de configurar o reinício do computador após a aplicação das atualizações e correções de vulnerabilidades;

1.5.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;

1.5.30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes.

2. ENDPOINT PARA CLIENTES WINDOWS

2.1. Compatibilidade.

2.1.1. Microsoft Windows XP Professional x86 SP3 e superior;

2.1.2. Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e posterior;

2.1.3. Microsoft Windows 8 Professional/Enterprise x86 / x64;

2.1.4. Microsoft Windows 8.1 Pro / Enterprise x86 / x64;

2.1.5. Microsoft Windows 10 Pro / Enterprise x86 / x64;

2.1.6. Microsoft Windows Server 2012 R2 Standard x64;

2.1.7. Microsoft Windows Server 2012 Foundation x64;

2.1.8. Microsoft Windows Server 2012 Standard x64;

2.1.9. Microsoft Small Business Server 2011 Standard x64;

2.1.10. Microsoft Windows Server 2008 R2 Standard/Enterprise x64 SP1;

2.1.11. Microsoft Windows Server 2008 Standard/Enterprise x86/x64 SP2;

2.1.12. Microsoft Windows Server 2003 (Todas as edições);

2.1.13. Microsoft Windows Server 2016 Standard/Enterprise/datacenter x64 ou

posterior.

2.2. Características

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

2.2.2. Autoproteção contra-ataques aos serviços/processos do antivírus;

2.2.3. Firewall com IDS;

2.2.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

2.2.5. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

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

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

2.2.7.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

2.2.7.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

2.2.7.3. Leitura de configurações;

2.2.7.4. Modificação de configurações;

2.2.7.5. Gerenciamento de Backup e Quarentena;

2.2.7.6. Visualização de relatórios;

2.2.7.7. Gerenciamento de relatórios;

2.2.7.8. Gerenciamento de chaves de licença;

2.2.7.9. Gerenciamento de permissões (adicionar/excluir permissões acima);

2.2.8. Antivírus de E -mail (módulo para verificação de e -mails recebidos e enviados, assim como seus anexos);

2.2.9. Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas);

2.2.10. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;

2.2.11. Controle de dispositivos externos;

2.2.12. Controle de acesso a sites por categoria;

2.2.13. Controle de acesso a sites por horá rio;

2.2.14. Controle de acesso a sites por usuários;

2.2.15. Controle de execução de aplicativos;

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

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

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

2.2.17. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;

2.2.18. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede;

2.2.19. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);

2.2.20. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS);

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

2.2.22. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;

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

2.2.24. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;

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

2.2.26. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

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

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

2.2.29. Capacidade de verificar somente arquivos novos e alterados;

2.2.30. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);

2.2.31. Capacidade de verificar objetos usando heurística;

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

2.2.33. Capacidade de agendar uma pausa na verificação;

2.2.34. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

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

2.2.35.1.1. Perguntar o que fazer, ou;

2.2.35.1.2. Bloquear acesso ao objeto;

2.2.35.1.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador);

2.2.35.1.4. Caso positivo de desinfecção, restaurar o objeto para uso;

2.2.35.1.5. Caso negativo de desinfecção, mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador).

2.2.36. Anteriormente a qualquer tentativa de desinfecção ou exclusão

permanente, o antivírus deve realizar um backup do objeto;

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

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

2.2.39. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa;

2.2.40. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros;

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

2.2.42. Capacidade de verificar e -mails recebidos e enviados nos protocolos POP 3, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);

2.2.43. Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;

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

2.2.45. Capacidade de verificar tráfego nos browsers : Internet Explorer, Firefox e Google Chrome, Opera, etc.;

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

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

2.2.47.1. Perguntar o que fazer, ou;

2.2.47.2. Bloquear o e-mail;

2.2.48. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré -estabelecida pelo administrador);

2.2.49. Caso positivo de desinfecção: Restaurar o e-mail para o usuário;

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

2.2.51. Caso o e-mail conter código que parece ser , mas não é definitivamente malicioso , o mesmo deve ser mantido em quarentena;

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

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

2.2.54. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas;

2.2.55. Deve ter suporte total ao protocolo IPv6;

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

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

2.2.57.1. Perguntar o que fazer, ou;

2.2.57.2.Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

2.2.57.3. Permitir acesso ao objeto.

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

2.2.59. Verificaçãoon-the-fly, onde os dados são verificados enquanto são recebidos em tempo real , ou;

2.2.60. Verificação de buffer , onde os dados são recebidos e armazenados para posterior verificação;

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

2.2.62. Deve possuir módulo que analise as ações de cada aplicação em execução no computador , gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

2.2.63. Deve possuir módulo que analise cada macro de VBA executada , procurando por sinais de atividade maliciosa;

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

2.2.65. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas , obtidas pelo Anti-PhishingWorkingGroup (http://www.antiphishing.org/);

2.2.66. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

2.2.67. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra portscans e exploração de vulnerabilidades de softwares. A base de dados de aná lise deve ser atualizada juntamente com as vacinas

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

2.2.69. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

2.2.69.1.1. Discos de armazenamento locais;

2.2.69.1.2. Armazenamento removível;

2.2.69.1.3. Impressoras;

2.2.69.1.4. CD/DVD;

2.2.69.1.5. Drives de disquete;

2.2.69.1.6. Modems;

2.2.69.1.7. Dispositivos de fita;

2.2.69.1.8. Dispositivos multifuncionais;

2.2.69.1.9. Leitores de smartcard;

2.2.69.1.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);

2.2.69.1.11. Wi-Fi;

2.2.69.1.12. Adaptadores de rede externos;

2.2.69.1.13. Dispositivos MP3 ou smartphones; 2.2.69.1.14. Dispositivos

Bluetooth;

2.2.69.1.15. Câmeras e Scanners.

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

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

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

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

2.2.74. Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc.), com possibilidade de configuração por usuário ou grupos de usuários e agendamento;

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

2.2.76. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

2.2.77. Capacidade de limitar o acesso dos aplicativos a recursos do sistema , como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;

2.2.78. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;

2.2.79. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada , desde regras de firewall até controle de aplicativos , dispositivos e acesso à web.

3.ENDPOINT PARA CLIENTES MAC OS X

3.1. Compatibilidade

3.1.1. Mac OS X 10.7 (Lion);

3.1.2. Mac OS X 10.8 (Mountain Lion);

3.1.3. Mac OS X 10.9 (Mavericks);

3.1.4. Mac OS X 10.10 (Yosemite);

3.1.5. Mac OS X 10.11 (El Capitan);

3.1.6. Mac OS X 10.12 (Sierra);

3.1.7. Mac OS X 10.13 (High Sierra);

3.1.8. Mac OS X 10.14 (Mojave);

3.1.9. Mac OS X 10.15 (Catalina);

3.1.10. Mac OS X 11 (Big sur).

3.2. Características

3.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

3.2.2. Possuir módulo de web-AntiMalware para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https;

3.2.3. Possuir módulo de bloqueio á ataques na rede;

3.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;

3.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;

3.2.6. Possibilidade de importar uma chave no pacote de instalação;

3.2.7. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

3.2.8. A instalação e primeira execução do produto deve ser feita sem necessidade de reinicialização do computador, de modo que o produto funcione com toda sua capacidade;

3.2.9. Deve possuir suportes a notificações utilizando o Growl;

3.2.10. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

3.2.11. Capacidade de voltar para a base de dados de vacina anterior;

3.2.12. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;

3.2.13. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do AntiMalware, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

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

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

3.2.15.1. Capacidade de verificar somente arquivos novos e alterados;

3.2.15.2. Capacidade de verificar objetos usando heurística;

3.2.15.3. Capacidade de agendar uma pausa na verificação;

3.2.15.4. O AntiMalware de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

3.2.15.5. Perguntar o que fazer, ou;

3.2.15.6. Bloquear acesso ao objeto;

3.2.15.7. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré- estabelecida pelo administrador);

3.2.15.8. Caso positivo de desinfecção, restaurar o objeto para uso;

3.2.16. Caso negativo de desinfecção, mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

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

3.2.18. Capacidade de verificar arquivos de formato de email;

3.2.19. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o AntiMalware e iniciar o AntiMalware pela linha de comando;

3.2.20. Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

4. ENDPOINT PARA CLIENTES LINUX

4.1. Compatibilidade (Plataforma 32 e 64 bits)

4.1.1. RedHat Enterprise Linux 6.2 Desktop e Superiores;

4.1.2. Fedora 16 e Superiores;

4.1.3. CentOS-6.2 e Superiores;

4.1.4. SUSE Linux Enterprise Desktop 10 SP4 e Superiores;

4.1.5. OpenSUSE Linux 12.2 e Superiores;

4.1.6. Debian GNU/Linux 6.0.5 e Superiores;

4.1.7. Mandriva Linux 2011 e Superiores;

4.1.8. Ubuntu 10.04 LTS e Superiores.

4.2. Características

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

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

4.2.3. Capacidade de configurar a permissão de acesso às funções do AntiMalware;

4.2.4. Capacidade de criar exclusões por local, máscara e nome da ameaça;

4.2.5. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

4.2.6. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

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

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

4.2.8.1. Alta;

4.2.8.2. Média;

4.2.8.3. Baixa;

4.2.8.4. Recomendado;

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

4.2.10. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

4.2.11. Em caso erros, deve ter capacidade de criar logs automaticamente, sem

necessidade de outros softwares;

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

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

5. ENDPOINT PARA SERVIDORES WINDOWS

5.1. Compatibilidade plataforma 32 bits

5.1.1. Windows Server 2008 Standard/Enterprise/Datacenter SP1 e posterior;

5.1.2. Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 e posterior.

5.2. Compatibilidade plataforma 64 bits

5.2.1. Microsoft Windows Server 2003 (Todas as edições);

5.2.2. Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);

5.2.3. Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior).

5.2.4. Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior);

5.2.5. Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior);

5.2.6. Microsoft Windows Storage Server 2008 R2;

5.2.7. Microsoft Windows Storage Server 2008 SP2 Standard Edition;

5.2.8. Microsoft Windows Storage Server SP2 Workgroup Edition;

5.2.9. Microsoft Windows Hyper-V Server 2008 R2 SP1 e posterior;

5.2.10. Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;

5.2.11. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;

5.2.12. Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;

5.2.13. Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;

5.2.14. Microsoft Windows Storage Server 2012 (Todas edições);

5.2.15. Microsoft Windows Storage Server 2012 R2 (Todas edições);

5.2.16. Microsoft Windows Hyper-V Server 2012;

5.2.17. Microsoft Windows Hyper-V Server 2012 R2 ou superior;

5.2.18. Windows Server 2016 Essentials/Standard/Datacenter/Core ou posterior;

5.2.19. Windows Storage Server 2016 ou posterior;

5.2.20. Windows Hyper-V Server 2016.

5.2.21. Microsoft Windows Server 2019 Essentials/Standard/Datacenter/Core ou posterior;

5.2.22. Windows Storage Server 2019 ou posterior;

5.2.23. Windows Hyper-V Server 2019.

5.3. Características:

5.3.1. Deve possuir as seguintes proteções:

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

5.3.1.2. Autoproteção contra-ataques aos serviços/processos do antivírus;

5.3.1.3. Firewall com IDS;

5.3.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

5.3.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

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

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

5.3.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

5.3.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

5.3.4.3. Leitura de configurações;

5.3.4.4. Modificação de configurações;

5.3.4.5. Gerenciamento de Backup e Quarentena;

5.3.4.6. Visualização de relatórios;

5.3.4.7. Gerenciamento de relatórios;

5.3.4.8. Gerenciamento de chaves de licença;

5.3.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima).

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

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

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

5.3.6. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;

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

5.3.8. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);

5.3.9. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS);

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

5.3.11. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;

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

5.3.13. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;

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

5.3.15. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

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

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

5.3.18. Capacidade de verificar somente arquivos novos e alterados;

5.3.19. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);

5.3.20. Capacidade de verificar objetos usando heurística;

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

5.3.22. Capacidade de agendar uma pausa na verificação;

5.3.23. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

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

5.3.24.1. Perguntar o que fazer, ou;

5.3.24.2. Bloquear acesso ao objeto;

5.3.24.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador);

5.3.24.4. Caso positivo de desinfecção, restaurar o objeto para uso;

5.3.24.5. Caso negativo de desinfecção, mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador);

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

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

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

5.3.28. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa;

5.3.29. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros;

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

6. ENDPOINT PARA SERVIDORES LINUX

6.1. Compatibilidade plataforma 64 bits

6.1.1. RedHat Enterprise Linux Server 7 e Superiores;

6.1.2. CentOS-7.0 e Superiores;

6.1.3. SUSE Linux Enterprise Server 12 e Superiores;

6.1.4. Novell Open Enterprise Server 11 SP2 e Superiores;

6.1.5. Ubuntu Server 14.04 LTS e Superiores;

6.1.6. Ubuntu Server 14.10 e Superiores;

6.1.7. Oracle Linux 6.5 e Superiores;

6.1.8. Oracle Linux 6.5 e Superiores;

6.1.9. Debian GNU/Linux 7.5, 7.6, 7.7 e Superiores;

6.1.10. OpenSUSE® 13.1 e Superiores.

6.2. Características

6.2.1. Deve possuir as seguintes proteções

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

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

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

6.2.2.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

6.2.2.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

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

6.2.2.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;

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

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

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

6.2.6. Capacidade de verificar objetos usando heurística;

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

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

6.2.9. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

7. ENDPOINT PARA DISPOSITIVOS MÓVEIS (TABLETS/SMARTPHONES)

7.1. Compatibilidade:

7.1.1. Apple iOS 9.0-10.3 ou superior;

7.1.2. Android 4.1 – 7.1.1 ou superior;

7.1.3. Windows Phone 8x ou superior.

7.2. Deve possuir as seguintes proteções

7.2.1. Proteção contra adware e autodialers;

7.2.2. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;

7.2.3. Arquivos abertos no smartphone;

7.2.4. Programas instalados usando a interface do smartphone

7.2.5. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;

7.2.6. Deverá isolar em área de quarentena os arquivos infectados;

7.2.7. Deverá atualizar as bases de vacinas de modo agendado;

7.2.8. Deverá bloquear spams de SMS através de Blacklists;

7.2.9. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado com mensagem de aviso ao utilizador do dispositivo;

7.2.10. Capacidade de desativar por política:

7.2.10.1. Wi-fi;

7.2.10.2. Câmera;

7.2.10.3. Bluetooth.

7.3. Características:

7.3.1. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;

7.3.2. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;

7.3.3. Deverá ter firewall pessoal (Android);

7.3.4. Capacidade de tirar fotos quando a senha for inserida incorretamente;

7.3.5. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;

7.3.6. Capacidade de enviar comandos remotamente de:

7.3.6.1. Localizar;

7.3.6.2. Bloquear.

7.3.7. Capacidade de detectar Jailbreak em dispositivos iOS;

7.3.8. Capacidade de bloquear o acesso a site por categoria em dispositivos;

7.3.9. Capacidade de bloquear o acesso a sites phishing ou malicioso;

7.3.10. Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;

7.3.11. Capacidade de bloquear o dispositivo quando o cartão “SIM” for substituído;

7.3.12. Capacidade de configurar White e blacklist de aplicativos;

7.3.13. Capacidade de localizar o dispositivo quando necessário;

7.3.14. Permitir atualização das definições quando estiver em “roaming”;

7.3.15. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

7.3.16. Deve permitir verificar somente arquivos executáveis;

7.3.17. Deve ter a capacidade de desinfectar o arquivo se possível;

7.3.18. Capacidade de agendar uma verificação;

7.3.19. Capacidade de enviar URL de instalação por e-mail;

7.3.20. Capacidade de fazer a instalação através de um link QRCode;

7.3.21. Capacidade de executar as seguintes ações caso a desinfecção falhe;

7.3.21.1. Deletar;

7.3.21.2. Ignorar;

7.3.21.3. Quarentena;

7.3.21.4. Perguntar ao usuário.

Documento assinado eletronicamente por **Clenya Rejane Barros de Lima - SEFAZ**, **Analista de Sistemas**, em 11/10/2021, às 09:33, conforme Art. 5º, XIII, "b", do Decreto Nº 27.971-E/2019.

Documento assinado eletronicamente por **Manoel Sueide Freitas**, **Secretário Adjunto de Estado**, em 11/10/2021, às 10:50, conforme Art. 5º, XIII, "b", do Decreto Nº 27.971-E/2019.

Documento assinado eletronicamente por **Kleber da Silva Lyra**, **Secretário de Estado Adjunto do Centro de Tecnologia da Informação Fazendária**, em 11/10/2021, às 11:24, conforme Art. 5º, XIII, "b", do Decreto Nº 27.971-E/2019.

A autenticidade do documento pode ser conferida no endereço https://sei.rr.gov.br/autenticar informando o código verificador **3103342** e o código CRC **663EA3FB**.

ANEXO I-A – INFORMAÇÕES COMPLEMENTARES

1. PLANILHA DEMONSTRATIVA DA DEMANDA

Item	Und.	Quant.	Valor de Ref. Unitário (R$)	Valor de Ref. Total (R$)
1.	Und.	5.841	170,00	992.970,00
VALOR TOTAL **R$ 992.970,00**				

Obs: A descrição dos itens está disposta no MODELO DA PROPOSTA DE PREÇOS – ANEXO II deste edital.

2. DA DOTAÇÃO ORÇAMENTÁRIA DOS PARTICIPANTES

- **PC/RR**

Unidade orçamentária: 19105 e 19603

Programa de trabalho: 06.122.010.4514.9900 e 06.181.037.2461.9900

Elemento de despesas: 33.90.40

Fonte de recurso: 101 / 150/ 650

Tipo do empenho: Ordinário

- **FESP/RR**

Unidade Orçamentária: 19604 - Fundo Estadual de Segurança Pública do Estado de Roraima - FESP/RR

Função: 06 - Segurança Pública

Subfunção: 181 - Policiamento

Programa de Governo: 037 - Segurança e Defesa do Cidadão

PAOE: 2485 - Enfrentamento à Criminalidade Violenta / 2486 - Valorização do Profissional de Segurança Pública

Natureza de Despesa: 449052

Fonte: 185/385.

3. VALOR GLOBAL MÁXIMO ACEITÁVEL PELA ADMINISTRAÇÃO

R$ 992.970,00 (Novecentos e noventa e dois mil e novecentos e setenta reais).

(TIMBRE DA EMPRESA)

ANEXO II

MODELO DA PROPOSTA DE PREÇOS

PROCESSO N°: **22101.005846/2021.73 - SEFAZ** PREGÃO ELETRÔNICO SOB O SISTEMA DE REGISTRO DE PREÇOS Nº: **070/2021**	**CNPJ**

Item	Descrição	Marca	Und.	Qtd.	Preço Unit.	Preço Total
1.	Aquisição de software (licenças) de proteção antivírus Kaspersky EndPoint Security for Business Advanced, incluindo transferência de conhecimento, com garantia de atualizações e suporte técnico por período de 36 (trinta e seis) meses. Conforme especificações mínimas e detalhamento descritas no anexo I do Termo de Referência (Anexo I) deste edital. Observação: Considerar a unidade de fornecimento "licença".	**Marca**	Und.	5.841		
VALOR TOTAL DA PROPOSTA						R$ 0,00

Boa Vista – RR, 00 de xxxxxxxxx de 2021.

VALIDADE DA PROPOSTA:

PRAZO DE GARANTIA: Conforme descrito no item 6 do Termo de Referência (Anexo I) deste edital;

BANCO:

AGÊNCIA:

CONTA CORRENTE:

FONE(S):

_____
Proponente

ANEXO III

MINUTA DA ATA DE REGISTRO DE PREÇOS

PREGÃO ELETRÔNICO Nº 000/2021

PROCESSO Nº 22101.005846/2021.73 - SEFAZ

Aos _____ dias do mês de _____ de 2021, na **COMISSÃO PERMANENTE DE LICITAÇÃO – CPL/RR**, localizada na Av. Nossa Senhora da Consolata, nº 472 – Centro, CEP: 69.301-011, Boa Vista – RR, neste ato representada por seu(ua) Presidente, o(a) Sr.(a) ....., juntamente com o(a) Pregoeiro(a), Sr.(a) ....., doravante denominado **ÓRGÃO GERENCIADOR** desta Ata de Registro de Preços, na forma da **Lei nº 10.520**, de 17/07/2002; do **Decreto nº 29.468-E**, de 13/10/2020, do **Decreto nº 10.024**, de 20/09/2019, do **Decreto nº 29.467-E**, de 13/10/2020, da **Lei Complementar nº 123**, de 14/12/2006; e do **Decreto nº 8.538**, de 06/10/2015; aplicando-se, subsidiariamente, a **Lei nº 8.666/93**, de 21/06/1993 e das demais normas legais aplicáveis, decorrente da licitação na modalidade Pregão, na forma Eletrônica, sob o Sistema de Registro de Preços, e, de outro lado, a empresa ....., CNPJ nº ....., com sede na ....., nº ....., Bairro: ....., ... (Estado), Telefone: ....., Banco: ....., Agência: ....., Conta Corrente: ....., vencedora e adjudicatária da licitação supramencionada, neste ato representada por seu representante legal ou procurador, conforme documento comprobatório, resolvem firmar o presente instrumento, objetivando registrar preço dos bens discriminados na Cláusula Primeira, que serão fornecidos em conformidade com as cláusulas e condições seguintes:

Empresas:

Ord.	Empresa(s) Classificada(s)	Item	Vr. Total do(s) Item

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. Esta Ata refere-se aos preços registrados para **eventual aquisição de software (licença) de proteção antivírus,** conforme as seguintes especificações:

Item	Especificação	Marca	Modelo	Und.	Qtd.	Vr. Unit. (R$)	Vr. Total (R$)

1.2. São Órgãos participantes deste Registro de Preços:

Ord.	Órgão(s) Participante(s)
1.	Secretaria de Estado da Fazenda **- SEFAZ**
2.	Secretaria de Estado da Segurança Pública **- SESP**
3.	Secretaria do Trabalho e Bem - Estar Social - **SETRABES**
4.	Secretaria de Estado de Representação do Governo de Roraima em Brasília **- SERBRAS**
5.	Secretaria de Estado da Agricultura, Pecuária e Abastecimento **- SEAPA**
6.	Secretaria Estadual de Infraestrutura de Roraima **- SEINF**
7.	Secretaria de Estado do Índio **- SEI**
8.	Casa Militar de Roraima **- CM/RR**
9.	Procuradoria-Geral do Estado de Roraima **- PGE/RR**
10.	Comissão Permanente de Licitação do Estado de Roraima **- CPL/RR**
11.	Casa Civil do Estado de Roraima
12.	Secretaria de Estado de Articulação Municipal e Política Urbana **- SEAMPU**
13.	Secretaria de Estado da Cultura **- SECULT**
14.	Polícia Militar do Estado de Roraima **- PM/RR**
15.	Polícia Civil do Estado de Roraima – **PC/RR** Fundo Estadual de Segurança Pública do Estado de Roraima – **FESP/RR**
16.	Secretaria de Estado da Saúde de Roraima **- SESAU**
17.	Secretaria de Estado do Planejamento e Desenvolvimento **- SEPLAN**
18.	Secretaria de Estado de Gestão Estratégica e Administração **- SEGAD**

1.3. Do quantitativo de cada Órgão Participante:

ORD.	ORGÃOS	ITEM 01
1.	**SEFAZ**	350
2.	**SESP**	191
3.	**SETRABES**	400
4.	**SERBRAS**	40
5.	**SEAPA**	150
6.	**SEINF**	200
7.	**SEI**	40
8.	**CM**	25
9.	**PGE**	170
10.	**CPL**	50
11.	**CASA CIVIL**	120
12.	**SEAMPU**	100
13.	**SECULT**	50
14.	**PM/RR**	500

15.	**PC/FESP**	1.000
16.	**SESAU**	2.000
17.	**SEPLAN**	200
18.	**SEGAD**	255
Qtd. Total		**5.841**

1.4. Da utilização da Ata de Registro de Preços por órgão ou entidade não participante:

Item	**Qtd. Total**
1.	11.682

CLÁUSULA SEGUNDA – DA VALIDADE DA ATA DE REGISTRO DE PREÇOS

2.1. Esta Ata de Registro de Preços terá a validade de **12 (doze) meses**, a partir de sua assinatura;

2.2. O prazo de validade desta Ata de Registro de Preços não será superior a doze meses, incluídas eventuais prorrogações, conforme art. 15, § 3º, inciso III, da Lei nº 8.666, de 21/06/1993.

2.3. A existência de preços registrados não obriga a Administração a firmar as contratações que deles poderão advir, ficando-lhe facultada a utilização de outros meios, respeitada a legislação relativa às licitações, sendo assegurado ao beneficiário do registro preferência em igualdade de condições.

2.4. É vedado efetuar acréscimos nos quantitativos fixados pela Ata de Registro de Preços, inclusive o acréscimo de que trata o art. 65, § 1°, da Lei nº 8.666, de 21/06/1993;

2.5. O contrato decorrente do Sistema de Registro de Preços deverá ser assinado no prazo de validade desta Ata de Registro de Preços;

CLÁUSULA TERCEIRA – DA ASSINATURA DA ATA E DA CONTRATAÇÃO COM FORNECEDORES REGISTRADOS

3.1. Homologado o resultado da licitação, o fornecedor mais bem classificado será convocado para assinar a ata de registro de preços, no prazo e nas condições estabelecidos no instrumento convocatório, podendo o prazo ser prorrogado uma vez, por igual período, quando solicitado pelo fornecedor e desde que ocorra motivo justificado aceito pela administração.

3.2. É facultado à administração, quando o convocado não assinar a Ata de Registro de Preços no prazo e condições estabelecidos, convocar os licitantes do cadastro reserva.

3.3. Na hipótese de inexistir cadastro reserva, é facultado à administração convocar os licitantes remanescentes, na ordem de sua classificação.

3.4. A Ata de Registro de Preços implicará compromisso de fornecimento nas condições estabelecidas, após cumpridos os requisitos de publicidade;

3.4.1. A publicação da síntese da ARP, devidamente assinada, é condição para a contratação.

3.4.2. A recusa injustificada de fornecedor classificado em assinar a Ata de Registro de Preços, dentro do prazo estabelecido nesta cláusula, ensejará a aplicação das penalidades legalmente estabelecidas, inclusive em relação aos fornecedores que compõem o cadastro reserva.

CLÁUSULA QUARTA – DA REVISÃO E DO CANCELAMENTO DOS PREÇOS REGISTRADOS

4.1. Os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos serviços ou bens registrados, cabendo ao órgão gerenciador promover as negociações junto aos fornecedores;

4.2. Quando o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, o órgão gerenciador convocará os fornecedores para negociarem a redução dos preços aos valores praticados pelo mercado;

4.3. Os fornecedores que não aceitarem reduzir seus preços aos valores praticados pelo mercado serão liberados do compromisso assumido, sem aplicação de penalidade;

4.4. A ordem de classificação dos fornecedores que aceitarem reduzir seus preços aos valores de mercado observará a classificação original;

4.5. Quando o preço de mercado tornar-se superior aos preços registrados e o fornecedor não puder cumprir o compromisso, o órgão gerenciador poderá:

4.5.1. Liberar o fornecedor do compromisso assumido, caso a comunicação ocorra antes do pedido de fornecimento, e sem aplicação da penalidade se confirmada a veracidade dos motivos e comprovantes apresentados; e

4.5.2. Convocar os demais fornecedores para assegurar igual oportunidade de negociação.

4.6. Não havendo êxito nas negociações, o órgão gerenciador procederá à revogação desta Ata de Registro de Preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

4.7. O registro do fornecedor será cancelado quando:

4.7.1. Descumprir as condições da Ata de Registro de Preços;

4.7.2. Não retirar a nota de empenho ou instrumento equivalente no prazo estabelecido pela Administração, sem justificativa aceitável;

4.7.3. Não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado; ou

4.7.4. Sofrer sanção prevista nos incisos III ou IV, do caput do art. 87, da Lei nº 8.666, de 1993, ou no art. 7º da Lei nº 10.520, de 2002.

4.8. O cancelamento de registros nas hipóteses previstas nos subitens 4.7.1, 4.7.2 e 4.7.4 desta cláusula, será formalizado por despacho do órgão gerenciador, assegurado o contraditório e a ampla defesa;

4.9. O cancelamento do Registro de Preços poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da Ata, devidamente comprovados e justificados:

4.9.1. Por razão de interesse público; ou

4.9.2. A pedido do fornecedor.

CLÁUSULA QUINTA – DA UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS POR ÓRGÃO OU ENTIDADE NÃO PARTICIPANTE E DO REMANEJAMENTO DE QUANTITATIVOS

5.1. A ARP, durante sua vigência, poderá ser utilizada por qualquer órgão ou

entidade não participante do certame licitatório, mediante anuência do órgão gerenciador.

5.1.1. O fornecedor beneficiário da ARP deverá ser consultado pelo órgão não participante para que se manifeste acerca da aceitação ou não do pedido.

5.1.2. No caso previsto no subitem anterior, o fornecedor só poderá aceitar o pedido, desde que não prejudique as obrigações presentes e futuras decorrentes da ARP.

5.1.3. O órgão ou entidade não participante, ao formalizar o pedido de adesão, deverá encaminhar ao órgão gerenciador a anuência por escrito do fornecedor beneficiário da ARP em relação ao aceite do pedido.

5.1.4. As aquisições ou contratações adicionais a que se refere o subitem 5.1 não poderão exceder, por órgão ou entidade, a cinquenta por cento dos quantitativos dos itens do instrumento convocatório e registrados nesta Ata de Registro de Preços para o órgão gerenciador e órgãos participantes;

5.1.5. O quantitativo decorrente das adesões a esta Ata de Registro de Preços não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado para o órgão gerenciador e órgãos participantes, independente do número de órgãos não participantes que aderirem;

5.1.6. Após a autorização do órgão gerenciador, o órgão não participante deverá efetivar a aquisição ou contratação solicitada em até noventa dias, observado o prazo de vigência da ata;

5.1.7. Compete ao órgão não participante os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação às suas próprias contratações, informando as ocorrências ao órgão gerenciador;

5.1.8. Órgão ou entidade que não participar de todos os lotes ou itens do registro de preços poderá aderir à ARP, na qualidade de órgão não participante, nos demais lotes e itens do mesmo registro de preços;

5.2. As quantidades previstas para os itens e lotes com preços registrados poderão ser remanejadas pelo órgão gerenciador para os órgãos participantes, mediante acordo entre os interessados, observada como limite máximo a quantidade total registrada para cada órgão;

5.2.1. É vedado o remanejamento de item ou lote que possua preço distinto por localidade, exceto quando o remanejamento ocorrer entre órgãos participantes em que o item ou lote não tenha preços diferentes;

5.2.2. O remanejamento de quantidades entre órgãos participantes do procedimento licitatório não requer autorização do beneficiário da ARP, observado o subitem anterior;

5.2.3. Para efeito do disposto no caput, caberá ao órgão gerenciador autorizar o remanejamento solicitado, com a redução do quantitativo inicialmente informado pelo órgão participante, desde que haja prévia anuência do órgão que vier a sofrer redução dos quantitativos informados;

5.2.4. Os órgãos e entidades da Administração Pública Estadual poderão aderir à ARP de órgãos e entidades de outros Estados, dos Municípios, do Distrito Federal ou da União, desde que os preços sejam compatíveis com os praticados no mercado e demonstrada a vantagem econômica da adesão.

5.2.5. É facultada aos órgãos ou entidades municipais, distritais ou estaduais a adesão a esta Ata de Registro de Preços da Administração Pública Estadual.

CLÁUSULA SEXTA – DO FORO

6.1. O Foro para dirimir os possíveis litígios que decorrem da utilização da presente Ata de Registro de Preços será o da comarca de Boa Vista/RR.

XXXXXXXXXXXXXXXXXX
Presidente da CPL/RR

XXXXXXXXXXXXXXXXXX
Pregoeiro(a) da CPL/RR

XXX nome do representante XXX
XXX nome da empresa XXX

MINUTA DE CONTRATO

ANEXO IV

CONTRATO PARA AQUISIÇÃO DE SOFTWARE (LICENÇA) DE PROTEÇÃO ANTIVÍRUS QUE ENTRE SI CELEBRAM O ESTADO DE RORAIMA E A EMPRESA _____, NA FORMA ABAIXO MENCIONADA.

O **Estado de Roraima**, pessoa jurídica de direito público interno, inscrito no CNPJ sob o n° 84.012.012/0001-26, com sede no Palácio Senador Hélio Campos, situado na Praça do Centro Cívico, s/n°, Centro, nesta cidade, doravante denominado **CONTRATANTE**, neste ato representado pelo(a) Excelentíssimo(a) Senhor(a) Secretário(a) de Estado _____, nomeado(a) pelo Decreto n° _____, inscrito(a) no C.P.F sob o n° _____, e de outro lado a empresa _____, estabelecida na _____, inscrita no CNPJ sob o n° _____, neste ato representada pelo(a) Senhor(a) _____, de nacionalidade _____, estado civil _____, portador(a) da cédula de identidade n° _____ e inscrito(a) no C.P.F. sob o n° _____, residente e domiciliado na cidade de _____, doravante denominada **CONTRATADA**, pactuam o presente Contrato, cuja celebração foi autorizada nos autos do Processo n° _____, que se regerá pela **Lei nº. 10.520/2002**; pelo **Decreto nº.**

4.794-E, de 03 de junho de 2002; **Decreto nº 29.468-E** de 13 de outubro de 2020; **Decreto n° 29.467-E** de 13 de outubro de 2020; **Decreto n° 10.024/2019**, no que couber, e de forma subsidiária, à disciplina da **Lei nº. 8.666/93; Lei Complementar nº. 123/2006**; pelos termos da proposta vencedora, e atendidas às cláusulas e condições que se enunciam a seguir:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O presente contrato tem por objeto a **aquisição de software (licença) de proteção antivírus**, de acordo com a(s) quantidade(s) e especificação(ões) técnica(s) constante(s) no **Anexo I (Termo de Referência), Anexo I-A (Informações Complementares)** e no **Anexo II (Modelo da Proposta de Preços)**, que integram o Edital de Pregão Eletrônico, sob o sistema de registro de preços, nº _____/2021, que passam a compor o presente Termo de Contrato, independentemente de transcrição.

1.2. **Discriminação do objeto:**

Item	Descrição	Marca	Und.	Qtd.	Preço Unit.	Preço Total
1.	Aquisição de software (licenças) de proteção antivírus Kaspersky EndPoint Security for Business Advanced, incluindo transferência de conhecimento, com garantia de atualizações e suporte técnico por período de 36 (trinta e seis) meses. Conforme especificações mínimas e detalhamento descritas no anexo I do Termo de Referência (Anexo I) do edital. Observação: Considerar a unidade de fornecimento "licença".	**Marca**	Und.	5.841		
VALOR TOTAL DA PROPOSTA						R$ 0,00

CLÁUSULA SEGUNDA – DO PRAZO E LOCAL DE ENTREGA DO OBJETO

2.1. **Prazo de Entrega**

2.1.1. O fornecimento do OBJETO ocorrerá conforme necessidade da CONTRATANTE. O prazo de entrega será de até 10 (dez) dias úteis contados a partir do recebimento da Nota de Empenho, acompanhada do Pedido de Fornecimento devidamente autuado pelo setor competente;

2.2. **Local de Entrega**

2.2.1. A entrega do OBJETO deverá ser realizada em meio eletrônico, com código de ativação das chaves de licenciamento, via e-mail indicado pelo (a) Fiscal do contrato, nos exatos termos conforme descrito no Termo de Referência (anexo I do Edital);

CLÁUSULA TERCEIRA – DAS CONDIÇÕES DE RECEBIMENTO DO OBJETO

3.1. O OBJETO deve ser recebido provisoriamente no prazo de 10 (dez) dias úteis, pelo(a) responsável por acompanhar e fiscalizar o contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Anexo I do Termo de Referência (Anexo I do Edital).

3.2. O OBJETO poderá ser rejeitado, no todo ou em parte, quando em desacordo com as especificações constantes no Termo de Referência (anexo I do Edital) e na proposta, devendo ser substituídos no prazo de 05 (cinco) dias úteis, a contar da notificação da CONTRATADA, às suas custas, sem prejuízo da aplicação das penalidades;

3.3. O OBJETO será recebido definitivamente no prazo de 10 (dez) dias úteis, contados do recebimento provisório, após a verificação da qualidade e quantidade e consequente aceitação mediante termo circunstanciado;

3.4. Na hipótese da verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo;

3.5. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato.

CLÁUSULA QUARTA – DA GARANTIA, TRANFERÊNCIA DE CONHECIMENTO E SUPORTE TÉCNICO DO OBJETO

4.1. Dispor garantia de reposição e/ou correção da solicitação pendente em caso de constatação de erro técnico nas licenças, no prazo máximo de 05 (cinco) dias úteis após a emissão das licenças;

4.2. O OBJETO deverá possuir garantia de atualizações e suporte técnico por período de 36 (trinta e seis) meses;

4.3. A transferência de conhecimento deverá incluir a implementação, ativação e configuração, proporcionando a habilidade para configurar e administrar a solução proposta, sendo capaz de passar este conhecimento a outros usuários da Instituição;

4.4. A CONTRATADA deverá transferir o conhecimento de toda solução, demonstrando todas as suas funcionalidades para, pelo menos, dois servidores do CONTRATANTE, em uma carga horária mínima de 10 horas, preferencialmente na modalidade virtual (remota), para que estes repliquem este conhecimento para as equipes de suporte do CONTRATANTE. De acordo com o perfil, ao final, os servidores do CETIF, pertencentes a CONTRATANTE, deverão estar aptos, pelo menos, à: Ser administradores do Sistema; Alterar as configurações e políticas em todas as suas aplicações conforme políticas da CONTRATANTE; Compreender o ambiente tecnológico associado a solução e ao processo de configuração disponível; Realizar toda e qualquer atividade para permitir a correta configuração da solução possibilitando a operacionalização do sistema por parte dos Administradores;

4.5. Deverá também elaborar e fornecer os documentos técnicos e manuais de toda a solução.

CLÁUSULA QUINTA – DO PREÇO E DAS CONDIÇÕES DE PAGAMENTO

5.1. **Do Preço**

5.1.1. O valor total do Contrato é de _____ (_____);

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

5.2. **Das Condições de Pagamento**

5.2.1. O CONTRATANTE efetuará o pagamento mediante Ordem Bancária creditada em Conta Corrente indicada pela CONTRATADA, até 30 (trinta) dias após o protocolo da Nota Fiscal e/ou Fatura devidamente atestada pelo CONTRATANTE;

5.2.2. O pagamento será efetuado mediante Ordem Bancária, na Conta Corrente nº _____, Agência _____, Banco _____;

5.2.3. Nenhum pagamento será efetuado à CONTRATADA, enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência;

5.2.4. Caso haja aplicação de multa, o valor será descontado de qualquer fatura ou crédito existente no Contratante em favor da CONTRATADA. Caso o valor da multa seja superior ao crédito eventualmente existente, a diferença será cobrada administrativamente ou judicialmente, se necessário;

5.2.5. O pagamento será precedido de consulta de regularidade fiscal para verificação das condições exigidas na contratação, cujos resultados serão juntados aos autos do processo próprio;

5.2.6. Será, também, observado para o pagamento, o Regulamento aprovado pelo Decreto nº 4.335-E, de 03 de agosto de 2001, e suas alterações;

5.2.7. Os encargos moratórios devidos em razão do atraso no pagamento, em decorrência de ato imputável exclusivamente ao Contratante, poderão ser calculados com utilização da seguinte fórmula:

EM = N x VP x I

Onde:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga;

I = Índice de compensação financeira, assim apurado:

I = (TX/100)

365

TX = Percentual da taxa anual do IPCA – Índice de Preços ao Consumidor Ampliado, do Instituto Brasileiro de Geografia e Estatística - IBGE.

CLÁUSULA SEXTA – DA DOTAÇÃO ORÇAMENTÁRIA

6.1. A despesa correrá à conta da seguinte Dotação Orçamentária:

I – Unidade Orçamentária: _____

II – Programa de Trabalho: _____

III – Elemento de Despesa: _____

IV – Fonte de Recursos: _____

6.2 – Para cobertura das despesas decorrentes desta contratação foi emitida Nota de Empenho nº _____, em ___/___/___/, tipo _____, no valor de _____.

CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DA CONTRATADA

7.1. A CONTRATADA deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

7.1.1. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes neste contrato, no Termo de Referência (anexo I do Edital) e em seu respectivo anexo I, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo/versão, procedência e prazo de garantia;

7.1.2. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

7.1.3. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste contrato, o objeto com avarias ou defeitos;

7.1.4. Comunicar à CONTRATANTE, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

7.1.5. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

7.1.6. Durante todo o período de garantia deverá ser disponibilizado para a instalação em até 15 dias de seu lançamento, todas as atualizações de produto, assim como, novas versões;

7.1.7. Comprovar a existência de equipe técnica com no mínimo 2 (dois) profissionais capacitados e certificados pelo fabricante.

CLÁUSULA OITAVA – DAS OBRIGAÇÕES DA CONTRATANTE

8.1. São obrigações da CONTRATANTE:

8.1.1. Receber o objeto no prazo e condições estabelecidas neste contrato;

8.1.2. Verificar minuciosamente, no prazo fixado, a conformidade do objeto recebido provisoriamente com as especificações constantes no Anexo I do Termo de Referência (anexo I do Edital) e na proposta, para fins de aceitação e recebimento definitivo;

8.1.3. Comunicar à CONTRATADA, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

8.1.4. Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA, através de comissão/servidor especialmente designado;

8.1.5. Efetuar o pagamento à CONTRATADA no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos neste contrato;

8.2. A Administração não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados.

CLÁUSULA NONA – DA FISCALIZAÇÃO

9.1. A execução do Contrato será acompanhada por representante(s) do CONTRATANTE, neste ato denominado(s) FISCAL(IS), especialmente designado(s) para esse fim, nos termos do Decreto n° 19.213-E de 23 de julho de 2015;

9.2. O Fiscal de Contrato deve ser, preferencialmente, nomeado dentre servidores efetivos, que não sejam diretamente subordinados à unidade ou a outros setores responsáveis pela elaboração ou gerência deste contrato, na respectiva Secretaria ou Órgão de Gestão.

9.2.1. Na hipótese da impossibilidade de atendimento do dispositivo acima, a nomeação do servidor deve ser precedida da devida justificativa.

9.3. O Fiscal de Contrato deve ter, preferencialmente, fundado conhecimento técnico atinente ao serviço executado ou ao produto adquirido;

9.4. Compete ao(s) FISCAL(IS) do Contrato:

9.4.1. Anotar em registro próprio todas as ocorrências relacionadas com a execução do Contrato, determinando o que for necessário à regularização das faltas ou defeitos observados;

9.4.2. Solicitar a seus superiores, em tempo hábil para a adoção das medidas convenientes, as decisões e providências que ultrapassarem sua competência;

9.4.3. Proceder às avaliações e emitir os atestados previstos no Decreto n° 19.213-E, de 23 de julho de 2015;

9.5. A fiscalização de que trata esta Cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, inclusive resultante de imperfeições técnicas, emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica co-responsabilidade do CONTRATANTE ou de seus agentes e prepostos (Art. 70, da Lei nº 8.666/93).

CLÁUSULA DÉCIMA – DAS SANÇÕES ADMINISTRATIVAS

10.1. O atraso injustificado na execução, bem como, a inexecução total ou parcial do Contrato sujeitará a Contratada às sanções administrativas previstas nas seguintes hipóteses, sem prejuízo das sanções previstas no art. 87, da Lei Federal nº 8.666/93, facultada ao Estado de Roraima, em todo caso, a rescisão unilateral:

a) Advertência por escrito;

b) Multa, nos termos seguintes:

b.1) 15 % (quinze por cento), sobre o valor da proposta, em caso de recusa da **CONTRATADA** em assinar o Contrato dentro de 05 (cinco dias úteis), contados da data de sua convocação;

b.2) 0,3% (três décimos por cento) sobre o valor do empenho, por dia de atraso na execução do objeto contratual, limitado este atraso em até 15 (quinze) dias;

b.3) 5% (cinco por cento) sobre o valor do empenho, por atraso na execução do objeto contratual quando superior a 15 (quinze) dias;

b.4) 15% (quinze por cento) sobre o valor do empenho do Contrato não realizado, no caso de:

b.4.1) Atraso superior a 30 (trinta) dias, na entrega do objeto contratado;

b.4.2) Desistência da entrega do objeto contratado;

b.5) 15% (quinze por cento) sobre o valor do empenho, caso a CONTRATADA venha a dar causa à rescisão contratual, sem prejuízo das ações cíveis ou criminais aplicáveis à espécie.

c) Suspensão temporária do direito de participar de licitações e firmar contrato com a **CONTRATANTE** por prazo não superior a 02 (dois) anos;

d) Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação, que será concedida sempre que a **CONTRATADA** ressarcir a Administração pelos prejuízos resultantes e após decorrido prazo da sanção aplicada com base no item anterior;

10.2. As penalidades estabelecidas nas alíneas **b.2** e **b.3**, do subitem **10.1**, poderão ser suspensas em face de casos fortuitos, ou de força maior, desde que devidamente justificados e comprovados.

10.3. As sanções previstas nas alíneas ***"c"*** e ***"d"***, subitem **10.1**, poderão ser aplicadas em conjunto com as demais sanções, facultada a defesa prévia da Contratada no prazo de 05 (cinco) dias úteis;

10.4. As sanções previstas nas alíneas ***"c"*** e ***"d"***, do subitem **10.1**, poderão também ser aplicadas à CONTRATADA quando, em razão dos compromissos assumidos:

a) seu (s) representante(s) legal(ais) tenha(m) sofrido condenação criminal definitiva por prática, nesta condição, de fraude fiscal no recolhimento de quaisquer tributos;

b) praticarem ilícitos, visando frustrar os objetivos da licitação, demonstrando não possuir idoneidade para contratar com a Administração Pública.

Parágrafo Único. Os valores das multas referidas nesta Cláusula serão descontados de qualquer fatura ou crédito da CONTRATADA.

10.5. Garantido o direito à ampla defesa, ficará impedido de licitar e contratar com a

Administração Pública, e será descredenciado do Sistema de Cadastramento de Fornecedores da CPL/RR, pelo prazo de **até 05 (cinco) anos**, sem prejuízo das multas previstas neste Contrato e das demais cominações legais, nos termos do **artigo 49 do Decreto nº 29.468-E, de 13 de outubro de 2020,** aquele que:

10.5.1 Não assinar o contrato ou a ata de registro de preços, quando convocado dentro do prazo de validade de sua proposta;

10.5.2 Deixar de entregar documentação exigida no Edital;

10.5.3. Apresentar documentação falsa;

10.5.4 Causar o atraso na execução do objeto;

10.5.5 Não mantiver a proposta;

10.5.6 Falhar ou fraudar a execução do Contrato;

10.5.7 Comportar-se de modo inidôneo;

10.5.8. Fizer declaração falsa ou cometer fraude fiscal.

10.6. As penalidades previstas no item anterior serão obrigatoriamente registradas no respectivo sistema de cadastro de fornecedor.

CLÁUSULA DÉCIMA PRIMEIRA – DA RESCISÃO

11.1. O presente Termo de Contrato poderá ser rescindido na forma do art. 79, nas hipóteses previstas no art. 78, com as consequências indicadas no art. 80, todos da Lei 8.666/93, sem prejuízo das sanções aplicáveis.

11.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

11.3. A CONTRATADA reconhece os direitos do CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666/1993.

11.4. O termo de rescisão, sempre que possível, será precedido de Relatório indicativo dos seguintes aspectos:

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

11.4.2. Relação dos pagamentos já efetuados e ainda devidos;

11.4.3. Indenizações e multas.

CLÁUSULA DÉCIMA SEGUNDA – DA VIGÊNCIA E EFICÁCIA

12.1. O prazo de vigência do Contrato obedecerá ao disposto no caput do Art. 57 da Lei 8.666/93.

12.2. Este Contrato terá eficácia legal após a publicação do seu extrato no Diário Oficial do Estado – DOE/RR.

CLÁUSULA DÉCIMA TERCEIRA – DA ALTERAÇÃO CONTRATUAL

13.1. Este Contrato somente sofrerá alterações ante as circunstâncias de fatos supervenientes dispostas no art. 65 da Lei Federal nº 8.666/93 e alterações posteriores.

Parágrafo Primeiro**.** Toda e qualquer alteração deverá ser processada mediante a celebração de Termo Aditivo, numerado em ordem crescente e publicado no Diário Oficial do Estado – DOE/RR. Será vedada a modificação do objeto.

Parágrafo Segundo**.** A alteração de valor contratual, decorrente do reajuste de preço, compensação ou penalização financeira, prevista no Contrato, bem como, o empenho de dotações orçamentárias suplementares até o limite do seu valor corrigido, pode ser registrado por simples apostila, dispensando a celebração de aditamento.

13.2. A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

13.2.1. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

CLÁUSULA DÉCIMA QUARTA – DOS CASOS OMISSOS

14.1. Aplicam-se à execução do Contrato e, especialmente aos casos omissos, as disposições contidas na Lei nº. 10.520/2002, na Lei 8.666/1993 e demais normas nacionais e estaduais de licitações e contratos administrativos e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 - Código de Defesa do Consumidor - e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA QUINTA - DA PUBLICAÇÃO E DO REGISTRO

15.1. O CONTRATANTE providenciará a publicação deste contrato, por extrato, no Diário Oficial do Estado – DOE/RR, nos termos do Art. 61, parágrafo único, da Lei nº 8.666/93.

CLÁUSULA DÉCIMA SEXTA – DO FORO

16.1. Fica eleito o foro da comarca de Boa Vista - Roraima para dirimir quaisquer dúvidas relativas ao cumprimento deste Contrato.

E por se acharem justas e acordadas, as partes assinam eletronicamente o presente instrumento para que surta todos os efeitos em Direito previstos.

Boa Vista-RR, _____de_____ de 2021.

PELO CONTRATANTE:

_____

CONTRATANTE

PELA CONTRATADA:

_____

CONTRATADA

Documento assinado eletronicamente por **Ketwllen Moniqui Ferreira de Carvalho**, **Pregoeira**, em 14/12/2021, às 09:57, conforme Art. 5º, XIII, "b", do Decreto Nº 27.971-E/2019.

A autenticidade do documento pode ser conferida no endereço https://sei.rr.gov.br/autenticar informando o código verificador **3632160** e o código CRC **2E848039**.