Secretaria de Estado de Meio Ambiente e Desenvolvimento Sustentável

ESTADO DE GOIÁS
SECRETARIA DE ESTADO DE MEIO AMBIENTE E DESENVOLVIMENTO SUSTENTÁVEL

Edital

EDITAL DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 19/2021 – SEMAD

TIPO: MENOR PREÇO (POR LOTE)

OBJETO**:** AQUISIÇÃO DE SOLUÇÃO DE SEGURANÇA DE ENDPOINTS (ANTIVÍRUS)COM INSTALAÇÃO E IMPLANTAÇÃO.

ABERTURA DA SESSÃO PÚBLICA: 08/11/2021, às 09:00 horas

AVISO DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 19/2021

O ESTADO DE GOIÁS, através Secretaria de Estado de Meio Ambiente e Desenvolvimento Sustentável, por intermédio de seu Pregoeiro e Equipe de Apoio designados pela Portaria nº 167/2021, publicada no DOE em 06/07/2021, torna público, para conhecimento dos interessados, que realizará licitação na modalidade **Pregão (Eletrônico)**, tipo Menor Preço (POR LOTE), em sessão pública eletrônica a partir das **09 :00 horas** (horário de Brasília-DF) do dia **08/11/2021,** através do *site* www.comprasnet.go.gov.br, destinado à AQUISIÇÃO DE SOLUÇÃO DE SEGURANÇA DE ENDPOINTS (ANTIVÍRUS)COM INSTALAÇÃO E IMPLANTAÇÃO, de acordo com as condições e especificações constantes no Termo de Referência, Anexo I e demais disposições fixadas neste Edital e seus Anexos, relativo ao Processo nº 202100017010097, nos termos da Lei Federal Complementar nº 123/2006, Lei Estadual nº 17.928/2012, Decretos Estaduais nº 9.666/2020 e nº 7.466/2011, Lei Federal nº 10.520/2002, e, subsidiariamente, a Lei Federal 8.666/1993 e suas alterações e demais normas regulamentares aplicáveis à espécie. O Edital e seus anexos encontram-se disponíveis no endereço citado abaixo ou nos *sites* www.comprasnet.go.gov.br e www.meioambiente.go.gov.br

Secretaria de Estado de Meio Ambiente e Desenvolvimento Sustentável
GERÊNCIA DE COMPRAS GOVERNAMENTAIS-GECG
Rua 82, Nº 400 Palácio Pedro Ludovico Teixeira – 2º andar, Ala Leste – Centro
CEP 74.015-908 – Goiânia - GO
Fone: (62) 3201 5237
E-mail: licitacao.meioambiente@goias.gov.br

Morian Scussel Malburg

Pregoeiro

EDITAL DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 19/2021

O ESTADO DE GOIÁS, ATRAVÉS DA Secretaria de Estado de Meio Ambiente e Desenvolvimento Sustentável-SEMAD, localizada na Rua 82, nº. 400 Palácio Pedro Ludovico Teixeira – 2º andar - Ala Leste – Centro – CEP: 74.015-908 – Goiânia – GO – Fone: (62) 3201-5210 – sítio www.meioambiente.go.gov.br, inscrita no CNPJ sob o nº 00.638.357/0001-08, representada por sua Secretária, **Dra. ANDRÉA VULCANIS[1],** brasileira, inscrita na OAB/DF sob o nº 37.330 e no CPF sob o nº. 845.216.009-72, residente domiciliada nesta capital, por intermédio de seu Pregoeiro e Equipe de Apoio designados pela Portaria nº 167/2021, publicada no DOE em 06/07/2021, torna público para conhecimento dos interessados, que realizará licitação na modalidade **Pregão (Eletrônico)**, tipo Menor Preço (POR LOTE), em sessão pública eletrônica, através do *site* www.comprasnet.go.gov.br, relativo ao Processo nº 202100017010097, nos termos da Lei Estadual nº 17.928/2012, Decretos Estaduais nº 9.666/2020 e nº 7.466/2011, Lei Federal nº 10.520/2002, e, subsidiariamente, a Lei Complementar nº 123/2006, a Lei Federal 8.666/1993 e suas alterações e demais normas regulamentares aplicáveis à espécie, bem como as condições estabelecidas neste Edital e seus anexos.

1. **DO OBJETO**

1.1. O presente pregão tem por objeto à AQUISIÇÃO DE SOLUÇÃO DE SEGURANÇA DE ENDPOINTS (ANTIVÍRUS)COM INSTALAÇÃO E IMPLANTAÇÃO, de acordo as condições e especificações constantes no Termo de Referência, Anexo I e demais disposições fixadas neste Edital e seus Anexos.

1.2. Nenhum item será adjudicado acima do valor estimado no Termo de Referência (Anexo I), o qual poderá ser revisto através de impugnação fundamentada nas condições e nos prazos previstos neste edital.

2. **DO LOCAL, DATA E HORA**

2.1. O Pregão Eletrônico será realizado em sessão pública, através do site www.comprasnet.go.gov.br, no dia **08/11/2021** a partir das **09:00h**, por meio do Sistema Eletrônico de Administração de Compras e Serviços do Estado de Goiás – SEACS, mediante condições de segurança, criptografia e autenticação, em todas as suas fases.

2.2. Os documentos de habilitação (que permanecerão ocultos até o final da fase de lances) e as Propostas Comerciais deverão ser encaminhadas de forma eletrônica, através do site www.comprasnet.go.gov.br., a proposta contendo o valor unitário da cada item e o valor total do lote único, de acordo com o Modelo do anexo III, no período compreendido entre as **08:00h** do dia **22/10/2021** e as **09:00h** do dia **08/11/2021.**

2.3. A fase competitiva (lances) terá início previsto para o dia **08/11/2021** às **09:10 horas**, com seu encerramento por prorrogação automática 2+2 ativado às **09:20 horas** deste dia**.**

2.4. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, independentemente de nova comunicação,

desde que não haja comunicação do Pregoeiro em contrário.

2.5. Todas as referências de tempo contidas neste Edital, no Aviso e durante a Sessão Pública observarão, obrigatoriamente, o horário de Brasília – DF e, dessa forma, serão registradas no sistema eletrônico e na documentação relativa ao certame.

2.6. Os avisos que o Pregoeiro julgar necessários, serão publicados no sistema comprasnet.

3. **DO PEDIDO DE ESCLARECIMENTO E DA IMPUGNAÇÃO DO EDITAL**

3.1. Qualquer cidadão ou licitante poderá solicitar esclarecimentos, providências ou impugnar o ato convocatório em até 3 (três) dias úteis antes da data fixada para a realização da sessão pública do pregão.

3.2. Caberá ao Pregoeiro decidir sobre a petição no prazo de 02 (dois) dias úteis.

3.3. Se reconhecida a procedência das impugnações ao instrumento convocatório, a administração procederá à sua retificação e republicação com devolução dos prazos.

3.4. Os pedidos de esclarecimentos, impugnação ou providências ao Edital deverão ser encaminhados, exclusivamente, de forma eletrônica, pelo site www.comprasnet.go.gov.br.

4. **DAS CONDIÇÕES DE PARTICIPAÇÃO E DO TRATAMENTO DIFERENCIADO CONCEDIDO ÀS MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE**

4.1. Poderão participar deste Pregão as empresas:

a) do ramo pertinente ao seu objeto, legalmente constituídos;

b) que atendam as condições estabelecidas neste Edital e seus anexos;

c) que possuam cadastro obrigatório (certificado de registro cadastral– CRC emitido pelo CADFOR ou por certificado de registro cadastral que atenda aos requisitos previstos na legislação geral). O certificado de registro cadastral deverá estar homologado e válido na data de realização do Pregão. Caso o CRC apresente *"status* irregular*"*, será assegurado a licitante o direito de apresentar, via eletrônica, a documentação atualizada e regular na própria sessão. O licitante vencedor que se valer de outros cadastros para participar de pregão por meio eletrônico deverá providenciar sua inscrição junto ao CADFOR, como condição obrigatória para a sua contratação;

d) que, previamente, realizem o credenciamento junto ao ComprasNet.GO.

4.2. A participação neste pregão eletrônico dar-se-á por meio da digitação de login e senha privativa da licitante e subsequente encaminhamento da Proposta Comercial em data e horário previstos neste Edital, exclusivamente por meio eletrônico.

4.3. Como requisito para participação neste Pregão, a licitante deverá manifestar, em campo próprio do sistema eletrônico www.comprasnet.go.gov.br, o pleno conhecimento e atendimento das exigências de habilitação previstas no Edital.

4.4. É vedada a participação de empresa:

4.4.1. Em processo de falência, sob concurso de credores, em dissolução ou em liquidação.

4.4.2. Que tenha sido declarada inidônea pela Administração Pública e, caso participe do processo licitatório, estará sujeita às penalidades previstas no Art. 97, parágrafo Único da Lei Federal 8.666/93.

4.4.3. Que esteja suspensa e/ou impedida de licitar junto ao Cadastro Unificado do Estado –CADFOR.

4.4.4. De acordo com o Art. 9º da Lei 8.666/93, não poderá participar da licitação, direta ou indiretamente:

I - o autor do projeto, básico ou executivo, pessoa física ou jurídica;

II - empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou executivo ou da qual o autor do projeto seja dirigente, gerente, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto ou controlador, responsável técnico ou subcontratado;

III - servidor ou dirigente de órgão ou entidade contratante ou responsável pela licitação.

IV - Aplica-se o disposto no item 4.4.4.1 aos membros da Comissão de Licitação, ao pregoeiro e à equipe de apoio

4.4.5. É permitida a participação do autor do projeto ou da empresa a que se refere o inciso II deste artigo, na licitação de obra ou serviço, ou na execução, como consultor ou técnico, nas funções de fiscalização, supervisão ou gerenciamento, exclusivamente a serviço da Administração interessada.

4.4.6. Considera-se participação indireta, para fins do disposto neste artigo, a existência de qualquer vínculo de natureza técnica, comercial, econômica, financeira ou trabalhista entre o autor do projeto, pessoa física ou jurídica, e o licitante ou responsável pelos serviços, fornecimentos e obras, incluindo-se os fornecimentos de bens e serviços a estes necessários.

4.5. As licitantes arcarão com todos os custos decorrentes da elaboração e apresentação de suas propostas, sendo que a SEMAD não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

4.6. Não poderão se beneficiar do regime diferenciado e favorecido em licitações concedido às microempresas e empresas de pequeno porte, art. 3º, §4º, incisos I a XI, pela Lei Complementar nº 123, de 14 de dezembro de 2006, licitantes que se enquadrem em qualquer das exclusões relacionadas em seu artigo terceiro.

4.6.1. A falsa declaração ou a não apresentação da documentação comprobatória quando solicitada, implicará na abertura de processo administrativo e consequente aplicação das sanções cabíveis.

4.7. Para usufruir dos benefícios estabelecidos no Decreto Estadual nº 7.466/2011, a licitante que se enquadrar como microempresa ou empresa de pequeno porte, deverá declarar-se como tal, devendo apresentar certidão que ateste o enquadramento expedida pela Junta Comercial ou, alternativamente, documento gerado pela Receita Federal, por intermédio de consulta realizada no sítio www.receita.fazenda.gov.br/simplesnacional, podendo ser confrontado com as peças contábeis apresentadas ao certame licitatório.

4.7.1. O próprio sistema disponibilizará a licitante a opção de declarar-se como microempresa ou empresa de pequeno porte. A não manifestação de enquadramento, quando indagado pelo sistema eletrônico, implicará no decaimento do direito de reclamar, posteriormente, essa condição, no intuito de usufruir dos benefícios estabelecidos na Lei supramencionada.

5. **DO CREDENCIAMENTO**

5.1. O acesso ao credenciamento se dará aos licitantes com cadastro homologado pelo Cadastro Unificado do Estado – CADFOR da Superintendência de Suprimentos e Logística da SEAD e/ou ao licitante com cadastro simplificado, caso o licitante pretenda utilizar-se de outros cadastros, em atendimento a Instrução Normativa nº 04/2011, da SEGPLAN, conforme o texto abaixo:

Art. 10. (…)
§ 3 Em caso do licitante pretender utilizar-se de outros cadastros que atendam a legislação pertinente para participar do Pregão Eletrônico, efetuará seu credenciamento de forma simplificada junto ao CADFOR, caso em que ficará dispensado de apresentar toda a documentação abrangida pelo referido cadastro,

mediante a apresentação do mesmo ao CADFOR e terá registrado apenas a condição de “credenciado”.

5.1.1. Para cadastramento, renovação cadastral e regularização, o interessado deverá atender a todas as exigências do Cadastro Unificado do Estado - CADFOR da Superintendência Central de Compras Governamentais e Logística da SEAD até o 5º (quinto) dia útil anterior à data de registro das propostas. A relação de documentos para cadastramento está disponível no *site* www.comprasnet.go.gov.br.

5.1.2. Não havendo pendências documentais será emitido o CRC - Certificado de Registro Cadastral pelo CADFOR, no prazo de 04 (quatro) dias úteis contados do recebimento da documentação.

5.1.3. A simples inscrição do pré-cadastro no sistema Comprasnet.go, não dará direito à licitante de credenciar-se para participar deste Pregão, em razão do bloqueio inicial da sua senha.

5.1.4. O desbloqueio do login e da senha do fornecedor será realizado após a homologação do cadastro da licitante.

5.1.5. Conforme Instrução Normativa nº 004/2011 – SEGPLAN, em caso do licitante pretender utilizar-se de outros cadastros que atendam a legislação pertinente para participar do pregão eletrônico, efetuará seu credenciamento de forma simplificada junto ao CADFOR, caso em que ficará dispensado de apresentar toda a documentação abrangida pelo referido cadastro, mediante a apresentação do mesmo ao CADFOR e terá registrado apenas a condição de “credenciado”.

5.1.6. O licitante com status "credenciado" deverá encaminhar todos os documentos de habilitação via sistema comprasnet e, caso, após a fase da disputa de lances, tenha a melhor oferta, terá os documentos encaminhados eletronicamente ao CADFOR para homologação do seu cadastro.

5.2. Os interessados que estiverem com o cadastro homologado ou “credenciados” (conforme item 4.1) deverão credenciar-se pelo *site* www.comprasnet.go.gov.br, opção “login do FORNECEDOR”, conforme instruções nele contidas.

5.3. O credenciamento dar-se-á de forma eletrônica por meio da atribuição de chave de identificação ou senha individual.

5.4. O credenciamento do usuário será pessoal e intransferível para acesso ao sistema, sendo o mesmo responsável por todos os atos praticados nos limites de suas atribuições e competências;

5.5. O credenciamento do usuário implica sua responsabilidade legal e a presunção de sua capacidade técnica para realização das transações inerentes ao pregão eletrônico.

5.6. O uso da senha de acesso pelo licitante é de sua exclusiva responsabilidade, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou a SEMAD, promotora da licitação, responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

5.7. As informações complementares para cadastro e credenciamento poderão ser obtidas pelos telefones **(62) 3201-6625, 3201-6629 e 98304-9641;** Para operação no sistema Comprasnet.go pelo telefone **(62) 3201-8752.**

5.8. **Incumbirá à licitante providenciar seu acesso para Assinatura Digital de Documentos e Processos (usuário externo) pelo site: http://sei.goias.gov.br/, instruções no site: http://sei.goias.gov.br/como_se_cadastrar.php ou pelos telefones (62) 3201-5723, (62) 3201-5127, e-mail: sei@goias.gov.br, horário de atendimento das 8h às 12h e das 14h às 18h.**

6. DAS PROPOSTAS COMERCIAIS

6.1. Concluída a fase de credenciamento, as licitantes registrarão suas propostas conforme item 2.2. Só será aceita uma proposta para cada licitante e, ao término do prazo estipulado para a fase de registro de propostas, o sistema automaticamente bloqueará o envio de novas propostas.

6.2. As propostas comerciais deverão ser enviadas através do *site* www.comprasnet.go.gov.br na data e hora estabelecidas neste edital, após o preenchimento do formulário eletrônico, com manifestação em campo próprio do sistema de que tem pleno conhecimento e que atende às exigências de habilitação previstas no Edital.

6.2.1. O ônus de comprovar a exequibilidade da proposta caberá exclusivamente à licitante, caso solicitado pelo Pregoeiro.

6.3. A Proposta Comercial deverá ser formulada e enviada, exclusivamente por meio do Sistema Eletrônico, indicando o preço unitário de cada item. **A disputa na fase de lances será feita pelo valor total do lote**.

6.3.1. Não serão adjudicados valores maiores que os estimados, tanto para Lote(s) quanto para valores unitários.

6.3.2. O sistema comprasnet.go possibilita à licitante a exclusão/alteração da proposta dentro do prazo estipulado no edital para registro de propostas. Ao término desse prazo, definido no item 2.2, não haverá possibilidade de exclusão/alteração das propostas, as quais serão analisadas conforme definido no edital.

6.4. A licitante se responsabilizará por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas, assim como os lances inseridos durante a sessão pública.

6.5. Incumbirá ao Licitante acompanhar as operações no sistema durante a sessão pública do pregão eletrônico, ficando responsável pelo ônus decorrente da perda de negócios, resultante da inobservância de quaisquer mensagens emitidas pelo pregoeiro ou pelo sistema, ainda que ocorra sua desconexão.

6.6. As propostas deverão atender as especificações contidas no Termo de Referência, Anexo I deste Edital.

6.7. Todas as empresas deverão cotar seus preços com todos os tributos cabíveis inclusos, bem como os demais custos diretos e indiretos necessários ao atendimento do Edital e seus anexos. Entretanto, as empresas enquadradas no regime normal de tributação (empresas não optantes do simples), estabelecidas em Goiás, deverão registrar a proposta com preços desonerados do ICMS conforme disposições do Art. 6º, Inc. XCI do Regulamento do Código Tributário do Estado de Goiás - RCTE, que concede isenção de ICMS nas operações e prestação internas, relativas à aquisição de bem, mercadoria e serviço por órgãos da Administração Pública Estadual Direta e suas fundações e autarquias, ficando mantido o crédito, observado, dentre outras coisas, à transferência do valor correspondente ao ICMS ao adquirente mediante a redução do preço do bem, mercadoria e serviço, devendo a redução ser demonstrada no documento fiscal.

6.7.1. Por determinação da Procuradoria-Geral do Estado através de seu Despacho “AG” nº 001203/2013, para as empresas estabelecidas em Goiás, isentas do ICMS, conforme item 5.7 acima, as propostas comerciais, enviadas pelas empresas detentoras das melhores ofertas após a fase de lances, deverão conter, obrigatoriamente, além do preço normal de mercado dos produtos ou serviços ofertados (valor bruto), o preço resultante da isenção do ICMS conferida (valor líquido), que deverá ser o preço considerado como base de julgamento. O valor líquido será aquele registrado no sistema comprasnet.go, como proposta, e será considerado como base para etapa de lances. O valor bruto (com ICMS) servirá apenas para efeito de análise do desconto concedido e para que as ordens de fornecimento possam apresentar os dois valores, facilitando a execução do contrato ou instrumento equivalente.

6.7.2. Para o licitante que não estiver obrigado a promover a desoneração do ICMS, deverá apresentar na proposta, no campo referente ao valor desonerado, o mesmo valor onerado, porém, com alíquota zero.

6.8. Quaisquer tributos, custos e despesas diretas ou indiretas omitidos na proposta ou incorretamente cotados, serão considerados como inclusos nos preços, não sendo aceitos pleitos de acréscimos, a esse ou qualquer outro título.

6.9. A licitante detentora da melhor oferta, após a fase de lances, deverá enviar, em **até 02hs (duas horas)** Declaração de Enquadramento na Lei Complementar nº 123/06 (conforme Anexo IV, se for o caso) e a Proposta Comercial, pelo sistema comprasnet, em formato PDF, limitado o tamanho em 10Mb, devendo a mesma conter, obrigatoriamente:

a) Nome da Empresa, CNPJ, endereço, fone/fax, nº da conta-corrente, Banco, nº da agência, nome do responsável;

b) Nº do Pregão;

c) Preço em Real, unitário e total com no máximo duas casas decimais, onde deverá estar inclusas todas as despesas que influam nos custos, tais como: transporte, frete, tributos (impostos, taxas, emolumentos, contribuições fiscais e para fiscais), obrigações sociais, trabalhistas, fiscais, encargos comerciais ou de qualquer natureza, e os demais custos diretos e indiretos. O preço apresentado deverá ser aquele resultante da fase de lances e/ou negociação com o Pregoeiro;

d) Objeto ofertado, consoante exigências editalícias, indicando a marca e modelo e com a quantidade licitada;

e) Prazo de validade da proposta de **60 (sessenta) dias**, a contar da data da sessão deste Pregão Eletrônico. Caso não apresente prazo de validade será este considerado;

f) Data e assinatura do responsável;

g) Valores readequados ao valor ofertado e registrado como de melhor lance.

h) Apresentar, caso seja necessário, Procuração Particular com firma reconhecida ou Procuração Pública, em nome do representante legal, outorgando poderes para formular ofertas, lances de preços, assumir obrigações, financeiras, e praticar todos os demais atos pertinentes a este certame em nome da Licitante.

i) cópia autenticada por cartório competente ou por servidor da administração do documento pessoal do sócio ou representante legal da licitante;

j) a indicação da marca ofertada para cada item licitado;

7. **DA SESSÃO DO PREGÃO**

7.1. O Pregoeiro, via sistema eletrônico, dará início à Sessão Pública, na data e horário previstos neste Edital.

7.2. Iniciada a sessão pública do pregão eletrônico, não cabe desistência da proposta, salvo por motivo justo, decorrente de fato superveniente e aceito pelo Pregoeiro;

7.3. O Pregoeiro realizará a análise preliminar das propostas registradas conforme item 6.3 acima.

7.3.1. O Pregoeiro verificará as propostas apresentadas, desclassificando aquelas que não estejam em conformidade com os requisitos estabelecidos no edital.

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

7.3.3. Em seguida, no horário marcado será dado início à fase de lances através do sistema eletrônico, observada as regras de aceitação dos mesmos. Todos os licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do seu recebimento e respectivo horário de registro e valor.

7.4. Durante o transcurso da sessão pública eletrônica os licitantes serão informados, em tempo real, as mensagens trocadas no *chat* do sistema, inclusive valor e horário do menor lance registrado apresentado pelas licitantes, vedada a identificação do detentor do lance.

7.5. As licitantes poderão oferecer lances sucessivos, **pelo valor total do lote**, observando o horário fixado e as regras de aceitação dos mesmos.

7.5.1. A licitante somente poderá oferecer lance inferior ao último por ela ofertado e registrado pelo sistema, obedecendo ao percentual ou valor mínimo exigido entre os lances, de R$ 10,00 (dez reais).

7.5.2. O sistema eletrônico rejeitará automaticamente os lances em valores superiores aos anteriormente apresentados pela mesma licitante.

7.6. Não serão aceitos, para o mesmo **lote**, 2 (dois) ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado no sistema em primeiro lugar.

7.7. Caso a licitante não realize lances, permanecerá o valor da proposta eletrônica apresentada para efeito da classificação final.

7.8. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do pregão, o sistema eletrônico permanecerá acessível às licitantes para a recepção dos lances. O Pregoeiro, quando possível, dará continuidade à sua atuação no certame, sem prejuízo dos atos realizados. Quando a desconexão persistir por tempo superior a dez minutos, a sessão do pregão será suspensa e terá reinício somente após comunicação expressa aos participantes.

7.9. A etapa de envio de lances na sessão pública adotará o modo de disputa aberto e durará 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 2 (dois) minutos do período de duração da sessão pública.

7.9.1. A prorrogação automática da etapa de envio de lances, de que trata o item 7.9, será de 2 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive quando se tratar de lances intermediários.

7.9.2. Na hipótese de não haver novos lances na forma estabelecida nos itens 7.9 e 7.9.1, a sessão pública será encerrada automaticamente.

7.9.3. Encerrada a sessão pública sem prorrogação automática pelo sistema, nos termos do disposto no item 7.9.1, o pregoeiro poderá, assessorado pela equipe de apoio, admitir o reinício da etapa de envio de lances em prol da consecução do melhor preço disposto no parágrafo único do art. 7º do Decreto 9.666/2020, mediante justificativa.

7.10. Após encerradas as operações referidas no item acima, o sistema ficará impedido de receber novos lances.

7.11. O Pregoeiro deverá negociar diretamente com o proponente, ofertando uma contra-proposta, para que seja obtido preço melhor.

7.12. Do direito de preferência como critério de desempate:

7.12.1. Encerrada a fase de lances, em caso de ocorrência de participação de licitante que detenha a condição de microempresa ou empresa de pequeno porte nos termos da Lei Complementar nº 123/06, o sistema averiguará se houve empate.

7.12.2. Será assegurado, como critério de desempate, preferência de contratação para as microempresas e empresas de pequeno porte.

7.12.2.1. Entendendo-se por empate aquela situação em que as propostas apresentadas pelas microempresas e empresas de pequeno porte sejam iguais ou até 5% (cinco por cento) superiores ao menor preço registrado para o item.

7.12.2.2. O critério de desempate, preferência de contratação, aqui disposto somente se aplicará quando a melhor oferta válida não tiver sido apresentada por microempresas, empresas de pequeno porte ou equiparada.

7.12.3. Para efeito do disposto no item acima, a preferência será concedida da seguinte forma:

I - Ocorrendo empate, a microempresa, empresa de pequeno porte ou equiparada melhor classificada poderá apresentar proposta comercial inferior àquela considerada vencedora do certame, situação em que será adjudicado o objeto licitado em seu favor;

II - O direito de preferência previsto no inciso I será exercido, sob pena de preclusão, após encerramento da rodada de lances, devendo ser apresentada nova proposta no máximo de cinco minutos para o item em situação de empate;

III - No caso de igualdade de valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem em situação de empate, será realizado sorteio entre elas para que se identifique aquela que poderá exercer o direito de preferência previsto no inciso I;

IV - - Na hipótese da não contratação da microempresa ou empresa de pequeno porte ou equiparada com base no inciso I, serão convocadas as remanescentes que porventura se enquadrem em situação de empate, na ordem classificatória, para o exercício do mesmo direito.

7.13. O disposto nos itens 7.12.2.2 e 7.12.2.3 somente se aplicará quando a melhor oferta, após a fase de lances, não tiver sido apresentada por microempresa ou empresa de pequeno porte.

7.14. Na hipótese de não contratação nos termos previstos no item 7.12.1 acima, o objeto licitado será adjudicado em favor da proposta originalmente detentora da melhor oferta.

8. **DO JULGAMENTO DAS PROPOSTAS**

8.1. O critério de julgamento é baseado no **menor preço.**

8.2. Considerar-se-á vencedora aquela que, tendo sido aceita, estiver de acordo com os termos deste Edital e seus Anexos, ofertar o menor preço, após a fase de lances e for devidamente habilitada após apreciação da documentação, salvo a situação prevista no item 8.8 deste Edital.

8.3. Declarado o encerramento da etapa competitiva, o Pregoeiro examinará a aceitabilidade da primeira oferta classificada, quanto ao objeto e valor e negociará com o licitante, efetuando uma contraproposta.

8.4. Caso não se realizem lances será verificada a conformidade da proposta de menor preço com as exigências do Edital.

8.5. Havendo apenas uma proposta, desde que atenda a todas as condições do edital e estando o seu preço compatível com os praticados no mercado, poderá ela ser aceita, devendo o Pregoeiro negociar, visando a obter preço melhor.

8.6. Sendo aceitável a oferta de menor preço, o pregoeiro analisará a documentação de habilitação enviada através do sistema comprasnet, em formato PDF, limitado o tamanho em 10mb por arquivo.

8.6.1. A verificação da situação de regularidade do Licitante pela Equipe de Apoio do certame, nos sítios oficiais de órgãos e entidades emissores de certidões, as quais constituem-se meio legal de prova. Tal verificação tem finalidade complementar de constatação e não substitui a sua obrigação de envio completo de toda a documentação de habilitação.

8.6.2. A licitante que, na condição de microempresa e empresa de pequeno porte, tenha sido declarada detentora da melhor oferta por utilização do benefício previsto na Lei Complementar nº 123, deverá encaminhar junto a proposta, após a fase de lances, prova de enquadramento da referida condição conforme definido no inciso I do artigo 10 do Decreto Estadual nº 7.466/2011. Será aceito para este fim certidão que ateste o enquadramento expedida pela Junta Comercial ou, alternativamente, documento gerado pela Receita Federal, por intermédio de consulta realizada no sítio www.receita.fazenda.gov.br/simplesnacional, podendo ser confrontado com as peças contábeis apresentadas ao certame licitatório.

8.7. Constatado o atendimento das exigências fixadas no edital, a licitante será declarada vencedora.

8.8. Se a oferta não for aceita ou se o licitante desatender às exigências habilitatórias, salvo na situação prevista no item 9.6, o pregoeiro restabelecerá a etapa competitiva de lances entre os licitantes (Art. 20-A Lei 17.928/12)**.**

8.9. Serão desclassificadas as propostas que:

a) Forem elaboradas em desacordo com as exigências do Edital e seus Anexos;

b) Apresentarem preços irrisórios, simbólicos ou abusivos, ou seja, as que apresentarem preços manifestamente inexequíveis ou superiores ao preço de mercado, de conformidade, subsidiariamente com os Arts.43, inciso IV, 44, parágrafo 3º e 48, incisos I e II da Lei 8.666/93;

c) Apresentarem propostas alternativas tendo como opção de preço ou marca, ou oferta de vantagem baseada nas propostas das demais licitantes;

8.10. Caso se verifique que a desclassificação ou inabilitação de determinada licitante se deu por ato atentatório à lisura do procedimento de licitação, por ela praticado com má-fé, a mesma poderá sofrer as sanções previstas neste edital.

8.11. Da sessão pública do Pregão, o sistema gerará ata circunstanciada, na qual estarão registrados todos os atos do procedimento e as ocorrências relevantes, que estará disponível para consulta no *site* www.comprasnet.go.gov.br.

8.12. Havendo empate, no caso de todas licitantes desistirem da fase de lances e se negarem a negociar com o Pregoeiro, serão utilizados para fins de desempate os seguintes critérios:

1º) As disposições dos arts. 44 e 45 da Lei Complementar nº 123/2006;
2º) a ordem de preferência elencada, sucessivamente, no art. 3º, § 2º, da Lei Federal nº 8.666/93; e,
3º) sorteio, pelo sistema eletrônico, nos termos do § único do Art. 37 do decreto Estadual 9.666/2020.

9. **DA HABILITAÇÃO**

9.1. A habilitação da licitante detentora da melhor oferta será verificada ao final da etapa de lances.

9.2. A licitante detentora da melhor oferta, deverá atender, obrigatoriamente, às seguintes exigências, sob pena de inabilitação:

a) Encaminhar pelo sistema comprasnet, , em formato PDF, limitado o tamanho em 10mb por arquivo, a documentação de habilitação para as exigências não contempladas no cadastro obrigatório. Os documentos cuja regularidade deverá ser comprovada por meio de cadastro obrigatório (certificado de registro cadastral emitido pelo CADFOR ou por certificado de registro cadastral que atenda aos requisitos previstos na legislação geral) estão elencados no Anexo II deste Edital e dizem respeito à habilitação jurídica, regularidade fiscal e a qualificação econômico-financeira. O Certificado de Registro Cadastral – CRC, emitido pelo Cadastro Unificado do Estado – CADFOR da Superintendência de Suprimentos e Logística da SEAD, poderá ser impresso pelo Pregoeiro para averiguação da conformidade exigida. Caso o CRC apresente *"status* irregular*"*, será assegurado a licitante o direito de apresentar, via sistema, a documentação atualizada e regular na própria sessão. O licitante vencedor que se valer de outros cadastros para participar de pregão por meio eletrônico deverá providenciar sua inscrição junto ao CADFOR, como condição obrigatória para a sua contratação.

b) Apresentar **DECLARAÇÃO** (Anexo V) de que a empresa não se acha declarada inidônea para licitar e contratar com o Poder Público ou suspensa do direito de licitar ou contratar com a Administração Pública, e ainda que tem ciência de todas as cláusulas deste Edital;

c) Apresentar **DECLARAÇÃO** (Anexo VI), junto as demais documentações, declarando que atende plenamente ao que dispõe o Inciso XXXIII do Artigo 7º da Constituição Federal, em cumprimento ao Inciso XIII do Artigo 12 do Decreto Estadual nº 7.468/2011, atestando que não possui em seu quadro, funcionários menores de 18 anos que exerçam trabalho noturno, perigoso ou insalubre, bem como que não possui nenhum funcionário menor de 16 anos, salvo na condição de aprendiz, a partir de 14 anos;

d) Apenas para as certidões cujo órgão emitente não houver consignado expressamente o prazo de validade, considerar-se-á vencidas quando emitidas em prazo superior a 60 (sessenta) dias;

e) Certidão de Negativa de Suspensão e/ou Impedimento de Licitar ou Contratar com a Administração Pública, emitida pelo Sistema COMPRASNET.GO, nos termos do art. 5º, §4º, Decreto nº 7.425, de 16 de agosto de 2011;

f) Apresentar documentos de identificação do representante legal da empresa;

g) Comprovação de qualificação técnica através de atestado de capacidade técnica (art. 30 da Lei nº 8.666/1993), contendo as informações de contato para sua verificação, se for o caso.

h) Comprovação de regularidade perante o Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais - CADIN Estadual, nos termos do art. 6º, inciso I, da Lei nº 19.754, de 17 de julho de 2017.

i) Certidão de Negativa de Suspensão e/ou Impedimento de Licitar ou Contratar com a Administração Pública, emitida pelo Sistema COMPRASNET.GO, nos termos do art. 5º, §4º, Decreto nº 7.425, de 16 de agosto de 2011.

9.3. Os documentos extraídos via INTERNET terão seus dados conferidos pela Equipe de Apoio perante o site correspondente.

9.4. Não serão aceitos protocolos de entrega ou solicitação de documento em substituição aos documentos requeridos no presente Edital e seus Anexos.

9.5. Se a documentação de habilitação não atender às exigências deste Edital, o Pregoeiro considerará a licitante inabilitada, estando a licitante sujeita às penalidades cabíveis.

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

9.5.2. A existência de registro no CADIN estadual constituirá impedimento à contratação do licitante, nos termos o art. 6º, I e § 1º da Lei Estadual nº 19.754/2017.

9.6. Para as microempresas e empresas de pequeno porte, em cumprimento ao Artigo 5º da Lei Estadual nº 17.928/2012, havendo alguma restrição na comprovação da regularidade fiscal das microempresas e empresas de pequeno porte, será assegurado o prazo de 5 (cinco) dias úteis para a regularização da documentação, contados do momento em que o proponente for declarado o vencedor do certame, prorrogável por igual período, a critério da administração.

9.6.1. O tratamento favorecido previsto no item 9.6 somente será concedido se as microempresas e empresas de pequeno porte apresentarem no certame toda a documentação fiscal exigida, mesmo que esta contenha alguma restrição.

9.6.2. O motivo da irregularidade fiscal pendente será registrado pelo Pregoeiro em ata, com a indicação do documento necessário para comprovar a regularização.

9.6.3. A não-regularização da documentação no prazo estabelecido, implicará decadência do direito à contratação, sem prejuízo das sanções previstas no art. 81 da Lei n. 8.666, de 21 de junho de 1993, sendo facultado à Administração convocar os licitantes remanescentes, na ordem de classificação, para a assinatura do contrato, ou revogar a licitação.

10. DOS RECURSOS

10.1. Declarado o vencedor, qualquer licitante poderá, no prazo de 10 (dez) minutos, em campo próprio do sistema, manifestar sua intenção de recorrer, hipótese adstrita ao pregão eletrônico.

10.2. As razões do recurso deverão ser apresentadas no prazo de 3 (três) dias e em local próprio no sistema eletrônico.

10.3. Os demais licitantes ficarão intimados para, se desejar, apresentar suas contrarrazões no prazo de 3 (três) dias, contados da data final do prazo do recorrente, assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses.

10.4. A ausência de manifestação imediata e motivada do licitante quanto à intenção de recorrer, importará na decadência desse direito, e o pregoeiro estará autorizado a adjudicar o objeto ao licitante declarado vencedor.

10.5. Não serão conhecidos os recursos interpostos após os respectivos prazos legais, bem como os que forem enviados pelo *chat*, e-mail, correios ou entregue pessoalmente.

10.6. O acolhimento do recurso importará na invalidação apenas dos atos que não podem ser aproveitados.

10.7. A decisão do recurso será postada no *site* www.comprasnet.go.gov.br .

11. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

11.1. Inexistindo manifestação recursal, o Pregoeiro adjudicará o objeto à licitante vencedora. Decididos os recursos, a autoridade superior fará a adjudicação do objeto da licitação;

11.2. A homologação da presente licitação compete ao Secretário(a) de Estado da SEMAD ou a pessoa cuja esta competência tenha sido delegada.

12. DAS CONDIÇÕES PARA CONTRATAÇÃO

12.1. Homologada a licitação, a licitante vencedora será convocada por contato telefônico ou e-mail para, no prazo de 10 (dez) dias a partir da notificação, retirar a Nota de Empenho em substituição ao Contrato.

12.2. A recusa injustificada da adjudicatária, caracteriza o descumprimento total da obrigação assumida, sujeitando-a às penalidades previstas em lei, exceção feita às licitantes que se negarem a aceitar a contratação, fora da validade de suas propostas (art. 73 da Lei nº 8.666/1993).

12.3. A rescisão das obrigações decorrentes do presente Pregão se processará de acordo com o que estabelecem os artigos 77 a 80 da Lei nº 8.666/93.

12.3.1. Reconhecimento dos direitos da Administração, em caso de rescisão administrativa prevista no art. 77 da Lei Federal nº 8.666/93.

12.4. As exigências do fornecimento, as quantidades, os prazos, bem como as demais condições constam no Termo de Referência, Anexo I deste Edital.

12.5. Caberá à CONTRATANTE indicar o gestor do contrato, que deverá observar as disposições do Art. 67 da Lei Federal nº 8.666/93.

12.5.1. A Contratada deverá nomear preposto para representa-la na execução dos serviços, na forma do art. 68 da Lei Federal nº 8.666/1993.

12.6. Como condição para celebração do contrato, o licitante vencedor deverá manter as condições de habilitação.

a) Se o licitante vencedor não celebrar o contrato ou não apresentar situação regular, é facultado à Administração examinar e verificar a aceitabilidade das propostas subsequentes, na ordem de classificação, procedendo à contratação, sem prejuízo da aplicação das sanções previstas neste edital.

b) Quando da contratação com autor de proposta subsequente àquela melhor classificada, deverá a Administração negociar o valor, procurando aproximá-lo daquele ofertado inicialmente.

12.7. A contratada é obrigada a aceitar, nas mesmas condições da licitação, os acréscimos ou supressões, nos termos do parágrafo 1º do art. 65 da lei Federal nº 8.666/1993.

12.8. - No ato da entrega, não será permitida a substituição da marca do produto adjudicado. Com exceção de fato superveniente, não imputável à Contratada, e autorizada por esta Pasta, quanto à inviabilidade de fornecer o objeto na marca inicialmente cotada, observando os seguintes requisitos:

12.8.1. - A Contratada deverá apresentar justificativa para a substituição da marca indicada na proposta, assim como a indicação da nova marca e modelo do produto;

12.8.2. - Sendo a justificativa plausível, a nova marca e modelo serão analisados, a fim de verificar se atende às exigências técnicas formuladas no Anexo I – Termo de Referência;

12.8.3. - A nova marca ofertada deverá ser de qualidade igual ou superior à inicialmente cotada, de forma a atender todos os requisitos que foram solicitados no Anexo I – Termo de Referência.

12.8.4. - Caso falte alguns dos requisitos descritos anteriormente, a Administração não poderá aceitar a referida substituição, sob pena de rescisão contratual, conforme art. 78, I, da Lei Federal nº 8.666/93, e eventual penalidade, conforme art. 87 da Lei Federal nº 8.666/93.

12.9. - Como condição para contratação, na forma do Acórdão n. 2688/2019 - Plenário TCE, os bancos de dados CEIS e CNEP serão consultados, assim como a certidão do Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa – CNJ, da empresa melhor classificada.

12.10. - Como condição para contratação, deverá apresentar Prova de regularidade perante o Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais - CADIN Estadual, nos termos do art. 6º, inciso I, da Lei nº 19.754, de 17 de julho de 2017;

12.11. - Ocorrerá a retenção ou glosa no pagamento, sem prejuízo das sanções cabíveis, nas hipóteses em que a CONTRATADA:

a) Não produzir os resultados esperados, deixar de executar ou não executar as atividades contratadas com a qualidade mínima exigida;

b) Deixar de utilizar os recursos exigidos para a execução dos serviços, ou utilizá-los com quantidade inferior à demandada;

13. **DAS CONDIÇÕES DE RECEBIMENTO DO OBJETO**

13.1. O objeto será recebido, de acordo com o Art. 73 da Lei 8.666/93:

I - em se tratando de obras e serviços:

a) provisoriamente, pelo responsável por seu acompanhamento e fiscalização, mediante termo circunstanciado, assinado pelas partes em até 15 (quinze) dias da comunicação escrita do contratado;

b) definitivamente, por servidor ou comissão designada pela autoridade competente, mediante termo circunstanciado, assinado pelas partes, após o decurso do prazo de observação, ou vistoria que comprove a adequação do objeto aos termos contratuais, observado o disposto no art. 69 desta Lei;

II - em se tratando de compras ou de locação de equipamentos:

a) provisoriamente, para efeito de posterior verificação da conformidade do material com a especificação;

b) definitivamente, após a verificação da qualidade e quantidade do material e conseqüente aceitação.

14. **DO PAGAMENTO, DO FATURAMENTO E DO REAJUSTE**

14.1. Homologada a licitação, será emitida Nota de Empenho a favor da Adjudicatária, que deverá protocolizar, perante a SEMAD, na GERÊNCIA DE TECNOLOGIA a Nota Fiscal/Fatura para ser atestada pelo gestor do contrato.

14.2. Executado o contrato, o seu objeto será recebido:

a) provisoriamente, pelo responsável por seu acompanhamento e fiscalização, mediante termo circunstanciado, assinado pelas partes em até 15 (quinze) dias da comunicação escrita do contratado;

b) definitivamente, por servidor ou comissão designada pela autoridade competente, mediante termo circunstanciado, assinado pelas partes, após o decurso do prazo de observação, ou vistoria que comprove a adequação do objeto aos termos contratuais, observado o disposto no art. 69 desta Lei Federal nº 8.666/1993;

14.3. O pagamento será efetuado em até 30 (trinta) dias após a protocolização e atesto da Nota Fiscal/Fatura. Em atenção ao disposto no Art. 4º da Lei nº 18.364, de 10 de janeiro de 2014, o pagamento será efetivado por meio de crédito em conta-corrente do favorecido aberta exclusivamente em Instituição Bancária contratada para centralizar movimentação financeira dos Órgãos da Administração Direta (Caixa Econômica Federal).

14.4. Para efetivação do pagamento, a regularidade fiscal deverá ser comprovada pelos documentos hábeis ou por meio do Certificado de Registro Cadastral – CRC, e outros documentos que possam ser considerados pertinentes pelo setor responsável pelo pagamento da SEMAD, devendo a CONTRATADA manter todas as condições de habilitação exigidas pela Lei.

14.5. Na ocorrência de rejeição da Nota Fiscal/Fatura, motivada por erro ou incorreções, o prazo para pagamento estipulado no item 14.3, passará a ser contado a partir da data da sua reapresentação.

14.6. Ocorrendo atraso no pagamento em que a contratada não tenha concorrido de alguma forma para o mesmo, a CONTRATADA fará jus a compensação financeira devida, desde a data limite fixada para pagamento até a data correspondente ao efetivo pagamento da parcela. Os encargos moratórios pelo atraso no pagamento serão calculados pela seguinte fórmula:

EM = N x Vp x (I / 365) onde:

EM = Encargos moratórios a serem pagos pelo atraso de pagamento;
N = Números de dias em atraso, contados da data limite fixada para pagamento e a data do efetivo pagamento;
Vp = Valor da parcela em atraso;
I = IPCA anual acumulado (Índice de Preços ao Consumidor Ampliado do IBGE)/100.

15. **DOS RECURSOS FINANCEIROS E DA DOTAÇÃO ORÇAMENTÁRIA**

15.1. A despesa decorrente da presente licitação correrá à conta da Dotação Orçamentária nº 2021.21.53.04.122.4200.4243.03, Natureza de despesa 3.3.90.40.84 e 4.4.90.40.82, Fonte 162 - FUNDO ESTADUAL DO MEIO AMBIENTE - FEMA.

16. **DAS PENALIDADES**

16.1. Sem prejuízo das demais sanções legais cabíveis, pelo não cumprimento dos compromissos acordados poderão ser aplicadas, a critério da SEMAD, as seguintes penalidades, conforme disposto nos arts. 86 a 88 da Lei n° 8.666/93, bem como arts. 77 a 83 da Lei Estadual nº 17.928/12:

a) Aquele que, convocado dentro do prazo de validade de sua proposta, não celebrar o contrato ou instrumento equivalente, deixar de entregar ou apresentar documentação falsa exigida para o certame, declarar informações falsas, ensejar o retardamento da execução do seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato ou instrumento equivalente, comportar-se de modo inidôneo ou cometer fraude fiscal, garantido o direito à ampla defesa, ficará impedido de licitar e de contratar com a Administração e será descredenciado

do CADFOR, pelo prazo de até 05 (cinco) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade sem prejuízo das multas previstas nesse Edital e das demais cominações legais;

b) A inexecução contratual, inclusive por atraso injustificado na execução do contrato ou instrumento equivalente, sujeitará a contratada, além das penalidades referidas nesse item, a multa de mora, graduada de acordo com a gravidade da infração, obedecidos aos seguintes limites máximos:

I - 10% (dez por cento) sobre o valor do contrato ou instrumento equivalente, em caso de descumprimento total da obrigação, inclusive no caso de recusa do adjudicatário em firmar o contrato ou retirar a nota de empenho, dentro de 10 (dez) dias contados da data de sua convocação;

II - 0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso, sobre o valor da parte do fornecimento não realizado;

III - 0,7% (sete décimos por cento) sobre o valor da parte do fornecimento não realizado, por dia subsequente ao trigésimo.

c) Advertência;
d) Suspensão temporária de participação em licitação e impedimento de contratar com a Administração
e) Declaração de inidoneidade para licitar e contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação, na forma da lei, perante a SEMAD;
f) As sanções previstas nas alíneas a), c), d) e e) poderão ser aplicadas junto a da alínea b).
g)Não será aplicada multa se o atraso na prestação do serviço resultar de caso fortuito ou de força maior devidamente comprovada.

16.2. Antes da aplicação de qualquer penalidade será garantido à contratada direito ao contraditório e a ampla defesa. A multa poderá ser descontada dos pagamentos eventualmente devidos pela SEMAD ou ainda, quando for o caso, cobrada judicialmente.

17. **DA CONCILIAÇÃO, MEDIAÇÃO E ARBITRAGEM**

17.1. As controvérsias eventualmente surgidas quanto à formalização, execução ou encerramento do ajuste decorrentes desta licitação, chamamento público ou procedimentos congênere, serão submetidas à tentativa de conciliação ou mediação no âmbito da **CÂMARA DE CONCILIAÇÃO, MEDIAÇÃO E ARBITRAGEM DA ADMINISTRAÇÃO PÚBLICA ESTADUAL(CCMA),** na forma da Lei n. 9.307, de 23 de setembro de 1996, e da Lei Complementar Estadual n. 144, de 24 de julho de 2018.

17.2. Os conflitos que possam surgir relativamente ao ajuste decorrente desta licitação, acaso não puderem ser equacionados de forma amigável, serão, no tocante aos direitos patrimoniais disponíveis, submetidos à arbitragem, na forma da Lei nº 9.307, de 23 de setembro de 1996 e da Lei Complementar Estadual nº 144, de 24 de julho de 2018, elegendo-se desde já para o seu julgamento a **CÂMARA DE CONCILIAÇÃO, MEDIAÇÃO E ARBITRAGEM DA ADMINISTRAÇÃO ESTADUAL (CCMA)**, outorgando a esta os poderes para indicar os árbitros e renunciando expressamente à jurisdição e tutela do Poder Judiciário para julgamento desses conflitos, consoante instrumento em Anexo."

a) Qualquer disputa ou controvérsia relativa à interpretação ou execução deste ajuste, ou de qualquer forma oriunda ou associada a ele, no tocante a direitos patrimoniais disponíveis, e que não seja dirimida amigavelmente entre as partes (precedida da realização de tentativa de conciliação ou mediação), deverá ser resolvida de forma definitiva por arbitragem, nos termos das normas de regência da **CÂMARA DE CONCILIAÇÃO, MEDIAÇÃO E ARBITRAGEM DA ADMINISTRAÇÃO ESTADUAL (CCMA)**.
A CÂMARA DE CONCILIAÇÃO, MEDIAÇÃO E ARBITRAGEM DA ADMINISTRAÇÃO ESTADUAL (CCMA) será composta por Procuradores do Estado, Procuradores da Assembleia Legislativa e por advogados regularmente inscritos na OAB/GO, podendo funcionar em Comissões compostas sempre em número ímpar maior ou igual a 3 (três) integrantes (árbitros), cujo sorteio se dará na forma do art. 14 da Lei Complementar Estadual nº 114, de 24 de julho de 2018, sem prejuízo da aplicação das normas de seu Regimento Interno, onde cabível.
b) A sede da arbitragem e da prolação da sentença será preferencialmente a cidade de Goiânia.
c) O idioma da Arbitragem será a Língua Portuguesa.
d) A arbitragem será exclusivamente de direito, aplicando-se as normas integrantes do ordenamento jurídico ao mérito do litígio.
e) Aplicar-se-á ao processo arbitral o rito previsto nas normas de regência (incluso o seu Regimento Interno) da **CÂMARA DE CONCILIAÇÃO, MEDIAÇÃO E ARBITRAGEM DA ADMINISTRAÇÃO ESTADUAL (CCMA)**, na Lei nº 9.307, de 23 de setembro de 1996, na Lei nº 13.140, de 26 de junho de 2015, na Lei Complementar Estadual nº 144, de 24 de julho de 2018 e na Lei Estadual nº 13.800, de 18 de janeiro de 2001, constituindo a sentença título executivo vinculante entre as partes.
f) A sentença arbitral será de acesso público, a ser disponibilizado no sítio eletrônico oficial da Procuradoria-Geral do Estado, ressalvadas as hipóteses de sigilo previstas em lei.
g) As partes elegem o Foro da Comarca de Goiânia para quaisquer medidas judiciais necessárias, incluindo a execução da sentença arbitral. A eventual propositura de medidas judiciais pelas partes deverá ser imediatamente comunicada à **CÂMARA DE CONCILIAÇÃO, MEDIAÇÃO E ARBITRAGEM DA ADMINISTRAÇÃO ESTADUAL (CCMA)**, e não implica e nem deverá ser interpretada como renúncia à arbitragem, nem afetará a existência, validade e eficácia da presente cláusula arbitral."

18. **DAS DISPOSIÇÕES GERAIS**

18.1. Este Edital deverá ser lido e interpretado na íntegra. Após o registro da proposta no sistema, não serão aceitas alegações de desconhecimento.

18.2. A autoridade competente para determinar a contratação poderá revogar a licitação em face de razões de interesse público, derivadas de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-la por ilegalidade, de ofício ou por provocação de qualquer pessoa, mediante. ato escrito e fundamentado, conforme determinação do art. 49 da Lei Federal nº 8.666/1993.

18.2.1. A anulação do procedimento licitatório por motivo de ilegalidade não gera obrigação de indenizar, ressalvado o disposto no parágrafo único do art. 59 da Lei Federal nº 8.666/1993. Por sua vez, em caso de revogação, há possibilidade de indenizar por perdas e danos, desde que devidamente comprovados os prejuízos efetivos que tenha tido em razão da antecipação de providências realizadas em função da classificação (1º lugar).

18.2.2. A nulidade do procedimento licitatório induz à do contrato, neste caso, ressalvado o disposto no parágrafo único do artigo 59 da Lei Federal nº 8.666/93.

18.2.3. A Administração poderá, até a assinatura do contrato ou instrumento equivalente, inabilitar o licitante, por despacho fundamentado, sem direito a indenização ou ressarcimento e sem prejuízo de outras sanções cabíveis, se vier a ter conhecimento de fato ou circunstância anterior ou posterior ao julgamento da licitação que desabone a habilitação jurídica, as qualificações técnica e econômico-financeiro e regularidade fiscal do licitante. Neste caso, o(a) Pregoeiro(a) deverá restabelecer a etapa competitiva de lances entre os licitante, nos termos do art. 20-A, da lei Estadual nº 17.928/2012**.**

18.3. As licitantes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.

18.4. Na contagem dos prazos previstos neste Edital excluir-se-á o dia do início e incluir-se-á o do vencimento, considerando-se os dias consecutivos, exceto quando houver disposição em contrário. Somente se iniciam e vencem os prazos em dia de expediente regular e integral na SEMAD.

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

18.6. A contratada é obrigada a aceitar, nas mesmas condições da licitação, os acréscimos ou supressões, nos termos do § 1º do Artigo 65 da Lei Federal nº 8.666/93.

18.7. As informações e/ou esclarecimentos serão prestados pelo Pregoeiro através do site www.comprasnet.go.gov.br ficando todos os Licitantes obrigados a acessá-los para obtenção das informações prestadas pelo Pregoeiro.

18.8. Caberá também à licitante acompanhar as operações no sistema eletrônico durante a sessão pública do pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

18.9. **Havendo divergências entre a descrição do objeto constante no Edital e a descrição do objeto constante no *site* www.comprasnet.go.gov.br e nota de empenho, prevalecerá, sempre, a descrição deste Edital.**

18.10. Em qualquer fase da licitação, o Pregoeiro poderá promover diligência destinada a esclarecer ou complementar a instrução do processo, bem como sanear os erros de pequena relevância, mediante ato devidamente motivado.

18.11. Para dirimir as questões relativas ao presente Edital elege-se como foro competente o de Goiânia – GO, com exclusão de qualquer outro.

19. **DOS ANEXOS**

Constituem Anexos do Edital e dele fazem parte integrante:
ANEXO I – Termo de Referência
ANEXO II – Relação de Documentos que poderão ser substituídos pela apresentação do Certificado de Registro Cadastral – CRC
ANEXO III – Modelo de Proposta Comercial
ANEXO IV – Modelo de Declaração de Enquadramento na Lei Complementar nº 123/06
ANEXO V – Modelo de Declaração dos Fatos Impeditivos e Ciência das Cláusulas do Edital
ANEXO VI – Modelo de Declaração Que Não Emprega Menor (art. 7º, XXXIII, CF/88 c/c art. 27, V, Lei 8.666/93)

Goiânia, 21 de outubro de 2021

Morian Scussel Malburg
Pregoeiro

ANEXO I
TERMO DE REFERÊNCIA

1. **OBJETO**

A presente aquisição tem por objeto o a aquisição de solução de segurança de endpoints (antivírus), conforme especificações técnicas, quantidades e demais condições constantes neste Termo de Referência.

2. **JUSTIFICATIVA**

A utilização de solução de segurança de endpoints possibilita a redução dos riscos de fraude, vazamento de informações, inconsistências de informações, indisponibilidade das aplicações corporativas e, ate mesmo, sabotagens que podem gerar falso repúdio.
A solução de segurança de endpoints atualmente em uso na SEMAD foi disponibilizada em 2016 pela então Superintendência Central de Tecnologia da Informação da extinta Secretaria de Gestão e Planejamento - SEGPLAN. Entretanto, o período de assinatura expirou e não foi renovado, deixando a solução sem suporte e bastante desfasada, sem fornecer a devida e mínima segurança exigida para os padrões deste tipo de solução que existem atualmente no mercado, visto que as ameaças virtuais se aperfeiçoam cada vez mais.
Diante do exposto, a aquisição em tela se faz necessária como forma de contribuir para a segurança das informações estratégicas e para a continuidade dos serviços prestados pela SEMAD. É irrefutável a necessidade de proteção de quaisquer equipamentos conectados à rede de dados do Estado contra códigos maliciosos que possam colocar em risco os dados contidos, não só no equipamento originário, mas também nos demais equipamentos conectados à rede corporativa.
A solução de segurança de endpoints é uma parte fundamental dentro de um conjunto de ações que visam a segurança das informações corporativas da SEMAD.

3. **ESPECIFICAÇÃO DE OBJETO E VALORES ESTIMADOS**

			COMPARATIVO DE PREÇOS			
Item	**Descrição do Produto**	**Qtd.**	**Conselho Regional de Engenharia e Agronomia da Bahia**	**Universidade Federal do Rio Grande do Sul**	**Universidade Federal de Ciências da Saúde de Porto Alegre**	**ARP TRT 13ª Região**
1	Solução de segurança de endpoint	415 und	R$ 170,00	R$ 134,34	R$ 135,00	R$ 125,60
2	Serviço de instalação e implantação	Svc	-	-	-	R$ 16.000,00
				VALOR TOTAL		

4. **ESPECIFICAÇÕES TÉCNICAS DO OBJETO**

Item 1 - Solução de segurança de endpoint

4.1.1.0 - Servidor de Administração e Console Administrativa:

4.1.1.1 - Compatibilidade:

1. Microsoft Windows Server 2012 Standard / Core / Foundation / Essentials / Datacenter x64;
2. Microsoft Storage Server 2012 e 2012 R2 x64;
3. Microsoft Windows Server 2012 R2 Standard / Core / Foundation / Essentials / Datacenter x64;
4. Microsoft Windows Server 2016 Standard / Core / Datacenter x64;
5. Microsoft Windows Server 2019 Standard / Core / Datacenter x64;
6. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;
7. Microsoft Windows 8 SP1 Professional / Enterprise x32/x64;
8. Microsoft Windows 8 Professional / Enterprise x64;
9. Microsoft Windows 8.1 Professional / Enterprise x32;

10. Microsoft Windows 8.1 Professional / Enterprise x64;
11. Microsoft Windows 10 x32;
12. Microsoft Windows 10 x64;

4.1.1.2 - Suportar as seguintes plataformas virtuais:

1. Vmware: Workstation 15.x Pro, vSphere 6.7, vSphere 7.1;
2. Microsoft Hyper-V: 2012, 2012 R2, 2016, 2019 x64;
3. Parallels Desktop 16;
4. Citrix XenServer 7.1 LTSR;

4.1.1.3 - A console deve ser acessada via WEB (HTTPS) ou MMC;

4.1.1.4 - Console deve ser baseada no modelo cliente/servidor;

4.1.1.5 - Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;

4.1.1.6 - Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;

4.1.1.7 - Deve permitir incluir usuários do AD para logarem na console de administração

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

4.1.1.9 - As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;

4.1.1.10 - Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;

4.1.1.11 - Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;

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

4.1.1.13 - Deve armazenar histórico das alterações feitas em políticas;

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

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

4.1.1.16 - A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

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

4.1.1.18 - Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS e Android;

4.1.1.19 - A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

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

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

4.1.1.22 - Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;

4.1.1.23 - Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;

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

4.1.1.25 - Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

4.1.1.26 - Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

4.1.1.27 - A comunicação entre o cliente e o servidor de administração deve ser criptografada;

4.1.1.28 - Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

4.1.1.29 - Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

1. Nome do computador;
2. Nome do domínio;
3. Range de IP;
4. Sistema Operacional;
5. Máquina virtual.

4.1.1.30 - Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

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

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

4.1.1.33 - 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;

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

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

4.1.1.36 - 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;

4.1.1.37 - Deve fornecer as seguintes informações dos computadores:

1. Se o antivírus está instalado;
2. Se o antivírus está iniciado;
3. Se o antivírus está atualizado;
4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
5. Minutos/horas desde a última atualização de vacinas;
6. Data e horário da última verificação executada na máquina;
7. Versão do antivírus instalado na máquina;
8. Se é necessário reiniciar o computador para aplicar mudanças;
9. Data e horário de quando a máquina foi ligada;
10. Quantidade de vírus encontrados (contador) na máquina;
11. Nome do computador;
12. Domínio ou grupo de trabalho do computador;
13. Data e horário da última atualização de vacinas;
14. Sistema operacional com Service Pack;
15. Quantidade de processadores;
16. Quantidade de memória RAM;
17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
18. Endereço IP;
19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
20. Atualizações do Windows Updates instaladas;
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;
22. Vulnerabilidades de aplicativos instalados na máquina;

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

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

1. Alteração de Gateway Padrão;
2. Alteração de subrede;
3. Alteração de domínio;
4. Alteração de servidor DHCP;
5. Alteração de servidor DNS;
6. Alteração de servidor WINS;
7. Alteração de subrede;
8. Resolução de Nome;
9. Disponibilidade de endereço de conexão SSL;

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

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

4.1.1.42 - Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;

4.1.1.43 - Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

4.1.1.44 - 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;

4.1.1.45 - 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;

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

4.1.1.47 - Capacidade de gerar traps SNMP para monitoramento de eventos;

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

4.1.1.49 - Listar em um único local, todos os computadores não gerenciados na rede;

4.1.1.50 - Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;

4.1.1.51 - Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;

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

4.1.1.53 - 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;

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

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

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

4.1.1.57 - 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;

4.1.1.58 - Deve 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;

4.1.1.59 - Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

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

1. Nome do vírus;
2. Nome do arquivo infectado;
3. Data e hora da detecção;
4. Nome da máquina ou endereço IP;
5. Ação realizada.

4.1.1.61 - Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

4.1.1.62 - Capacidade de listar updates nas máquinas com o respectivo link para download

4.1.1.63 - Deve criar um backup de todos arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;

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

4.1.1.65 - Capacidade de realizar resumo de hardware de cada máquina cliente;

4.1.1.66 - Capacidade de diferenciar máquinas virtuais de máquinas físicas.

4.1.2.0 - Estações Windows:

4.1.2.1 - Compatibilidade:

1. Microsoft Windows 7 Professional/Enterprise/Home SP1 x86 / x64;
2. Microsoft Windows 8 Professional/Enterprise x86 / x64;
3. Microsoft Windows 8.1 Professional / Enterprise x86 / x64;
4. Microsoft Windows 10 Pro / Enterprise / Home / Education x86 / x64;
5. Microsoft Windows Server 2019 Essentials / Standard / Datacenter;
6. Microsoft Windows Server 2016 Essentials / Standard / Datacenter;
7. Microsoft Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
8. Microsoft Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
9. Microsoft Windows Server 2008 R2 Foundation / Essentials / Standard / Datacenter SP1;
10. Microsoft Windows Small Business Server 2011 Standard / Standard x64;
11. Microsoft Windows MultiPoint Server 2011 x64;

4.1.2.2 - Deve prover as seguintes proteções:

1. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
3. Antivírus de e-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
5. Firewall com IDS;
6. Autoproteção (contra-ataques aos serviços/processos do antivírus);
7. Controle de dispositivos externos;
8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;
9. Controle de acesso a sites por horário;
10. Controle de acesso a sites por usuários;
11. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;
12. Controle de execução de aplicativos;
13. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

4.1.2.3 - Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

4.1.2.4 - 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);

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

4.1.2.6 - 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;

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

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

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

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

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

4.1.2.12 - Capacidade de verificar somente arquivos novos e alterados;

4.1.2.13 - Capacidade de verificar objetos usando heurística;

4.1.2.14 - Capacidade de agendar uma pausa na verificação;

4.1.2.15 - Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;

4.1.2.16 - Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

4.1.2.17 - O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador);

1. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
2. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;
3. Capacidade de verificar links inseridos em e-mails contra phishings;
4. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera;
5. Capacidade de verificação de corpo e anexos de e-mails usando heurística;

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

4.1.2.19 - Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;

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

4.1.2.21 - Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;

4.1.2.22 - Deve ter suporte total ao protocolo Ipv6;

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

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

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

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

4.1.2.26 - 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;

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

4.1.2.28 - 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;

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

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

4.1.2.31 - Deve possuir módulo IDS (*Intrusion Detection System*) para proteção contra *port scans* e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;

4.1.2.32 - O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
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 a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

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

1. Discos de armazenamento locais;
2. Armazenamento removível;
3. Impressoras;
4. CD/DVD;
5. Drives de disquete;
6. Modems;
7. Dispositivos de fita;
8. Dispositivos multifuncionais;
9. Leitores de smart card;
10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
11. Wi-Fi;
12. Adaptadores de rede externos;
13. Dispositivos MP3 ou smartphones;
14. Dispositivos Bluetooth;
15. Câmeras e Scanners.

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

4.1.2.35 - Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;

4.1.2.36 - Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;

4.1.2.37 - Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.

4.1.2.38 - Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

4.1.2.39 - 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);

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

4.1.2.41 - Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

4.1.2.42 - White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

4.1.2.43 - Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

4.1.2.44 - 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;

4.1.2.45 - 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;

4.1.2.46 - 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;

4.1.2.47 - Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware;

4.1.2.48 - Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros;

4.1.2.49 - Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (*machine learning*);

4.1.2.50 - Capacidade de integração com o Windows Defender Security Center;

4.1.2.51 - Capacidade de integração com a *Antimalware Scan Interface* (AMSI);

4.1.2.52 - Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).

4.1.3.0 - Estações Mac OS X

4.1.3.1 - Compatibilidade:

1. macOS Catalina 10.15
2. macOS Mojave 10.14
3. masOS High Sierra 10.13
4. macOS Sierra 10.12

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

4.1.3.3 - Possuir módulo de web antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https;

4.1.3.4 - Possuir módulo de bloqueio á ataques na rede;

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

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

4.1.3.7 - Possibilidade de importar uma chave no pacote de instalação;

4.1.3.8 - Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

4.1.3.9 - 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);

4.1.3.10 - Capacidade de voltar para a base de dados de vacina anterior;

4.1.3.11 - Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;

4.1.3.12 - 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;

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

4.1.3.14 - 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;

4.1.3.15 - Capacidade de verificar somente arquivos novos e alterados;

4.1.3.16 - Capacidade de verificar objetos usando heurística;

4.1.3.17 - Capacidade de agendar uma pausa na verificação;

4.1.3.18 - O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

1. Perguntar o que fazer, ou;
2. Bloquear acesso ao objeto;
    1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador);
    2. Caso positivo de desinfecção:
        1. Restaurar o objeto para uso;
    3. Caso negativo de desinfecção:
        1. Mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador);

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

4.1.3.20 - Capacidade de verificar arquivos de formato de email;

4.1.3.21 - Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;

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

4.1.4.0 - Estações de trabalho Linux

4.1.4.1 - Compatibilidade:

1. **Plataforma 32 bits:**

1. Ubuntu 16.04 LTS;
2. Red Hat® Enterprise Linux® 6.7 Server;
3. CentOS 6.7;
4. Debian GNU / Linux 9.4 ;
5. Debian GNU / Linux 10;
6. Linux Mint 18.2;
7. Linux Mint 19;
8. GosLinux 6.6;
9. Mageia 4;
10. OS Lotos.

2. **Plataforma 64 bits:**

1. Ubuntu 16.04 LTS;
2. Ubuntu 18.04 LTS;
3. Red Hat Enterprise Linux 6.7;
4. Red Hat Enterprise Linux 7.2;
5. Red Hat Enterprise Linux 8.0;
6. CentOS 6.7;
7. CentOS 7.2;
8. CentOS 8.0;
9. Debian GNU / Linux 9.4
10. Debian GNU / Linux 10.1;
11. OracleLinux 7.3;
12. OracleLinux 8;
13. SUSE® Linux Enterprise Server 15;
14. openSUSE® Leap 15;
15. Amazon Linux AMI
16. Linux Mint 18.2;
17. Linux Mint 19;
18. GosLinux 6.6;
19. GosLinux 7.2.

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

4.1.4.3 - As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

4.1.4.4 - Capacidade de criar exclusões por local, máscara e nome da ameaça;

4.1.4.5 - Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

4.1.4.6 - 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;

4.1.4.7 - Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers;

4.1.4.8 - Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

1. Alta;
2. Média;
3. Baixa;
4. Recomendado;

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

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

4.1.4.11 - Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;

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

4.1.4.13 - 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;

4.1.4.14 - Capacidade de verificar objetos usando heurística;

4.1.4.15 - Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

4.1.4.16 - Possibilidade de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

4.1.4.17 - Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

4.1.5.0 - Servidores Windows

4.1.5.1 - Compatibilidade:

1. **Plataforma 32 bits:**

1. Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;
2. Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;
3. Windows Server 2008 Standard/Enterprise/Datacenter SP1 e posterior;
4. Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 e posterior;

2. **Plataforma 64 bits:**

1. Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;
2. Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;
3. Microsoft Windows Server 2008 Standard / Enterprise / DataCenter SP1 ou posterior;
4. Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter SP1 ou posterior.
5. Microsoft Windows Server 2008 R2 Foundation / Standard / Enterprise / DataCenter SP1 ou posterior;
6. Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter SP1 ou posterior;
7. Microsoft Small Business Server 2008 Standard / Premium
8. Microsoft Windows Hyper-V Server 2008 R2 SP1 e posterior;
9. Microsoft Microsoft Small Business Server 2011 Essentials / Standard
10. Microsoft Windows MultiPoint Server 2011
11. Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter / MultiPoint;
12. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
13. Microsoft Windows Server 2012 Core Standard / Datacenter;
14. Microsoft Windows Server 2012 R2 Core Standard / Datacenter;
15. Microsoft Windows Storage Server 2012;
16. Microsoft Windows Storage Server 2012 R2;
17. Microsoft Windows Hyper-V Server 2012;
18. Microsoft Windows Hyper-V Server 2012 R2;
19. Windows Server 2016 Essentials /Standard / Datacenter / MultiPoint Premium Server;
20. Windows Server 2016 Core Standard / Datacenter;
21. Windows Storage Server 2016;
22. Windows Hyper-V Server 2016;
23. Microsoft Windows Server 2019 Core / Terminal / Hyper-V
24. Windows Server IoT 2019 for Storage

4.1.5.2 - Deve prover as seguintes proteções:

1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
2. Autoproteção contra-ataques aos serviços/processos do antivírus;
3. Firewall com IDS;
4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
5. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
6. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

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

1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
3. Leitura de configurações;
4. Modificação de configurações;
5. Gerenciamento de Backup e Quarentena;
6. Visualização de relatórios;
7. Gerenciamento de relatórios;
8. Gerenciamento de chaves de licença;
9. Gerenciamento de permissões (adicionar/excluir permissões acima);

4.1.5.4 - O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
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 a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

4.1.5.5 - 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;

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

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

4.1.5.8 - Em caso de erros, deve ter capacidade de criar *logs* e *traces* automaticamente, sem necessidade de outros softwares;

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

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

4.1.5.11 - Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;

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

4.1.5.13 - 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 antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

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

4.1.5.15 - 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;

4.1.5.16 - Capacidade de verificar somente arquivos novos e alterados;

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

4.1.5.18 - Capacidade de verificar objetos usando heurística;

4.1.5.19 - Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

4.1.5.20 - Capacidade de agendar uma pausa na verificação;

4.1.5.21 - Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

4.1.5.22 - O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador);

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

4.1.5.24 - Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

4.1.5.25 - Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

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

4.1.5.27 - Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros

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

4.1.5.29 - Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

4.1.6.0 - Servidores Linux

4.1.6.1 - Compatibilidade:

1. **Plataforma 32 bits:**

1. CentOS 6.7 and later;
2. Debian GNU / Linux 9.4 and later;
3. Debian GNU / Linux 10.1 and later;
4. Linux Mint 19 and later;
5. Mageia 4;
6. Red Hat Enterprise Linux 6.7 and later;
7. ALT Education 9;
8. ALT Workstation 9;
9. ALT Server 9;

2. **Plataforma 64 bits:**

1. Ubuntu 16.04 LTS;
2. Ubuntu 18.04 LTS;
3. Red Hat Enterprise Linux 6.7;
4. Red Hat Enterprise Linux 7.2;
5. Red Hat Enterprise Linux 8.0;
6. CentOS 6.7;
7. CentOS 7.2;
8. CentOS 8.0;
9. Debian GNU / Linux 9.4
10. Debian GNU / Linux 10.1;
11. OracleLinux 7.3;
12. OracleLinux 8;
13. SUSE® Linux Enterprise Server 15;
14. openSUSE® Leap 15;
15. Amazon Linux AMI
16. Linux Mint 18.2;
17. Linux Mint 19;

18. GosLinux 7.2.

4.1.6.2 - Deve prover as seguintes proteções:

1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

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

1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
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;
3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;

4.1.6.4 - Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;

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

4.1.6.6 - 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;

4.1.6.7 - Capacidade de verificar objetos usando heurística;

4.1.6.8 - Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

4.1.6.9 - Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

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

4.1.7.0 - Smartphones e tablets

4.1.7.1 - Compatibilidade:

1. Android 5.0 – 5.1.1
2. Android 6.0 – 6.0.1
3. Android 7.0 – 7.12
4. Android 8.0 – 8.1
5. Android 9.0
6. Android 10.0
7. Android 11.0
8. iOS 10.0 – 10.3.3
9. iOS 11.0 – 11.3
10. iOS 12.0
11. iOS 13.0

4.1.7.2 - Deve prover as seguintes proteções (Android):

1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:
2. Proteção contra *adware* e *autodialers*;
3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;
4. Arquivos abertos no smartphone;
5. Programas instalados usando a interface do smartphone
6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;

4.1.7.3 - Deverá isolar em área de quarentena os arquivos infectados;

4.1.7.4 - Deverá atualizar as bases de vacinas de modo agendado;

4.1.7.5 - Capacidade de desativar por política:

- Wi-fi;
- Câmera;
- Bluetooth.

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

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

4.1.7.8 - Deverá ter firewall pessoal (Android);

4.1.7.9 - Capacidade de tirar fotos quando a senha for inserida incorretamente;

4.1.7.10 - Capacidade de enviar comandos remotamente de:

- Localizar;
- Bloquear.

4.1.7.11 - Capacidade de detectar Root em dispositivos Android;

4.1.7.12 - Capacidade de bloquear o acesso a site por categoria em dispositivos;

4.1.7.13 - Capacidade de bloquear o acesso a sites phishing ou malicioso;

4.1.7.14 - Capacidade de bloquear o dispositivo quando o cartão “SIM” for substituído;

4.1.7.15 - Capacidade de configurar White e blacklist de aplicativos;

4.1.7.16 - Capacidade de localizar o dispositivo quando necessário;

4.1.7.17 - Permitir atualização das definições quando estiver em “roaming”;

4.1.7.18 - Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

4.1.7.19 - Deve permitir verificar somente arquivos executáveis;

4.1.7.20 - Capacidade de agendar uma verificação (Android);

4.1.7.21 - Capacidade de enviar URL de instalação por e-mail;

4.1.7.22 - Capacidade de fazer a instalação através de um link QRCode;

4.1.7.23 - Capacidade de executar as seguintes ações caso a desinfecção falhe (Android):

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

4.1.8.0 - Gerenciamento de dispositivos móveis (MDM)

4.1.8.1 - Compatibilidade:

1. **Dispositivos com os sistemas operacionais:**

1. Android 5.0 – 5.1.1
2. Android 6.0 – 6.0.1
3. Android 7.0 – 7.12
4. Android 8.0 – 8.1
5. Android 9.0
6. Android 10.0
7. Android 11.0
8. iOS 10.0 – 10.3.3
9. iOS 11.0 – 11.3
10. iOS 12.0
11. iOS 13.0

2. **Software de gerência de dispositivos:**

1. VMWare AirWatch 9.3;
2. MobileIron 10.0;
3. IBM Maas360 10.68;
4. Microsoft Intune 1908;
5. SOTI MobiControl 14.1.4 (1693);

4.1.8.2 - Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

4.1.8.3 - Capacidade de ajustar as configurações de:

1. Sincronização de e-mail;
2. Uso de aplicativos;
3. Senha do usuário;
4. Criptografia de dados;
5. Conexão de mídia removível.

4.1.8.4 - Capacidade de instalar certificados digitais em dispositivos móveis;

4.1.8.5 - Capacidade de, remotamente, resetar a senha de dispositivos iOS;

4.1.8.6 - Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;

4.1.8.7 - Capacidade de, remotamente, bloquear um dispositivo iOS;

4.1.8.8 - Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;

4.1.8.9 - Capacidade de desinstalar remotamente o antivírus do dispositivo;

4.1.8.10 - Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;

4.1.8.11 - Capacidade de sincronizar com Samsung Knox;

4.1.9.0 - Criptografia

4.1.9.1 - Compatibilidade:

1. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;

2. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;
3. Microsoft Windows 7 Professional SP1 ou superior x86/x64;
4. Microsoft Windows 8 Enterprise x86/x64;
5. Microsoft Windows 8 Pro x86/x64;
6. Microsoft Windows 8.1 Pro x86/x64;
7. Microsoft Windows 8.1 Enterprise x86/x64;
8. Microsoft Windows 10 Enterprise x86/x64;
9. Microsoft Windows 10 Pro x86/x64;

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

4.1.9.3 - Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

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

4.1.9.5 - Capacidade de utilizar *Single Sign-On* para a autenticação de pré-boot;

4.1.9.6 - Permitir criar vários usuários de autenticação pré-boot;

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

4.1.9.8 - Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
2. Criptografar todos os arquivos individualmente;
3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

4.1.9.9 - 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;

4.1.9.10 - Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

4.1.9.11 - Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

4.1.9.12 - Verifica compatibilidade de hardware antes de aplicar a criptografia;

4.1.9.13 - Possibilita estabelecer parâmetros para a senha de criptografia;

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

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

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

4.1.9.17 - Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

4.1.9.18 - Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, arquivos de áudio, etc;

4.1.9.19 - Permite criar um grupo de extensões de arquivos a serem criptografados;

4.1.9.20 - Capacidade de criar regra de criptografia para arquivos gerados por aplicações;

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

4.1.9.22 - Capacidade de deletar arquivos de forma segura após a criptografia;

4.1.9.23 - Capacidade de criptografar somente o espaço em disco utilizado;

4.1.9.24 - Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;

4.1.9.25 - Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;

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

4.1.9.27 - Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;

4.1.9.28 - Deve ter a opção de utilização de TPM para criptografia através do BitLocker;

4.1.9.29 - Capacidade de fazer “Hardware encryption”;

4.1.10.0 - Gerenciamento de Sistemas

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

4.1.10.2 - Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;

4.1.10.3 - Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;

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

4.1.10.5 - Capacidade de gerenciar licenças de softwares de terceiros;

4.1.10.6 - Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;

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

4.1.10.8 - Possibilita fazer distribuição de software de forma manual e agendada;

4.1.10.9 - Suporta modo de instalação silenciosa;

4.1.10.10 - Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;

4.1.10.11 - Possibilita fazer a distribuição através de agentes de atualização;

4.1.10.12 - Utiliza tecnologia multicast para evitar tráfego na rede;

4.1.10.13 - Possibilita criar um inventário centralizado de imagens;

4.1.10.14 - Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;

4.1.10.15 - Suporte a WakeOnLan para deploy de imagens;

4.1.10.16 - Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;

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

4.1.10.18 - Capacidade de gerar relatórios de vulnerabilidades e patches;

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

4.1.10.20 - Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;

4.1.10.21 - Permite baixar atualizações para o computador sem efetuar a instalação

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

4.1.10.23 - Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;

4.1.10.24 - Permite selecionar produtos a serem atualizados pela console de gerenciamento;

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

4.1.10.26 - Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;

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

4.1.10.28 - Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades;

4.1.10.29 - Deve permitir selecionar o idioma das aplicações que serão atualizadas;

4.1.10.30 - Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;

4.1.11.0 - Detecção e Resposta

4.1.11.1 - Compatibilidade:

1. Windows 7 SP1 Home / Professional / Enterprise 32-bit / 64-bit;
2. Windows 8.1.1 Professional / Enterprise 32-bit / 64-bit;
3. Windows 10 RS3 (version 1703) Home / Professional / Education / Enterprise 32-bit / 64-bit;
4. Windows 10 RS4 (version 1803) Home / Professional / Education / Enterprise 32-bit / 64-bit;
5. Windows 10 RS5 (version 1809) Home / Professional / Education / Enterprise 32-bit / 64-bit;
6. Windows 10 RS6 (version 1903) Home / Professional / Education / Enterprise 32-bit / 64-bit;
7. Windows 10 19H2 (version 1909) Home / Professional / Education / Enterprise 32-bit / 64-bit;
8. Windows 10 20H1 (version 2004) Home / Professional / Education / Enterprise 32-bit / 64-bit;
9. Windows Server 2008 R2 Foundation / Standard / Enterprise 64-bit;
10. Windows Server 2012 Foundation / Standard / Enterprise 64-bit;
11. Windows Server 2012 R2 Foundation / Standard / Enterprise 64-bit;
12. Windows Server 2016 Essentials / Standard / Datacenter 64-bit;
13. Windows Server 2019 Essentials / Standard / Datacenter 64-bit.

4.1.11.2 - As funcionalidades relacionadas a detecção e resposta solicitadas nesse item, devem ser operadas na mesma console de gerenciamento da solução de endpoint;

4.1.11.3 - A solução deve oferecer módulo focado em capacidades de EDR “Endpoint Detection and Response”, incluindo no mínimo as seguintes capacidades:

4.1.11.4 - O agente deve ter capacidade de coletar e processar dados relacionadas ao veredito e ao contexto da ameaça;

4.1.11.5 - Deve fornecer graficamente a visualização da cadeia do ataque;

4.1.11.6 - Deve possuir a capacidade de varredura, para identificar a presença de um artefato detectado em outros dispositivos na rede, através de indicadores de comprometimento (IoC).

1. A varredura deve oferecer opções de resposta automatizada (sem intervenção do administrador), para serem executadas caso o IoC seja encontrado em outro dispositivo, com no mínimo as seguintes opções:
    1. Isolar o host;
    2. Iniciar uma varredura nas áreas críticas;
    3. Quarentenar o objeto;

4.1.11.7 - Capacidade de integração com a solução de sandbox;

4.1.11.8 - A solução deve criar um report detalhado sobre o incidente, tendo a capacidade de incluir no mínimo os seguintes dados:

1. Detecções provenientes da solução de endpoint;
2. Alterações de registro;
3. Conexões remotas;
4. Criação de arquivos;
5. Varredura por todos os dispositivos executada a partir de indicador de comprometimento (IoC) gerado através da solução e importado pelo administrador.
6. Possibilidade de exportar os indicadores de comprometimento (IoC) gerados a partir da solução.

4.1.11.9 - A solução deve oferecer no mínimo as seguintes opções de resposta:

1. Prevenir a execução de um arquivo;
2. Quarentenar um arquivo;
3. Iniciar uma varredura por IoC;
4. Parar um processo;
5. Executar um processo;

4.1.11.10 - Ferramenta que possibilite o isolamento do host infectado com no mínimo as características abaixo:

4.1.11.11 - A opção de isolamento deve estar disponível junto a visualização do incidente;

4.1.11.12 - Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra;

4.1.12 - Licenciamento

4.1.12.1 - O período de vigência do licenciamento da solução ofertada deverá ser, no mínimo, 36 (trinta e seis) meses.

Item 2 - Serviço de instalação e implantação

4.2.1 - A Licitante vencedora será inteiramente responsável pela instalação, atualização ou migração da solução antivírus atualmente em uso pela CONTRATANTE, bem como às despesas diretas ou indiretas para execução das atividades pela sua equipe técnica;

4.2.2 - A instalação, atualização ou migração dos softwares em estações de trabalho poderá ser realizada remotamente, sem causar indisponibilidade do ambiente, devendo ser realizada em horários a serem definidos pela CONTRATANTE;

4.2.3 - A instalação, atualização ou migração dos softwares em servidores de rede poderá ser realizada remotamente, devendo ser realizada em horários a serem definidos pela CONTRATANTE;

4.2.4 - A CONTRATANTE poderá autorizar a instalação, atualização ou migração durante o horário de expediente se, ao seu exclusivo critério, entender que não oferece risco ao funcionamento de sua rede de computadores e serviços em produção;

4.2.5 - Para garantir que a instalação, atualização ou migração não afetará o ambiente da CONTRATANTE, os procedimentos e atividades deverão ser realizados por técnicos certificados pelo fabricante;

4.2.6 - A CONTRATADA deverá realizar a criação de todas as políticas, regras funcionalidades, e customizações apontadas pela CONTRATANTE;

4.2.7 - A CONTRATANTE acompanhará todo o processo de instalação e configuração da solução junto a CONTRATADA.

5. CONDIÇÕES DE FORNECIMENTO

Para comprovação das características mínimas relativas ao presente Termo de Referência, a proposta deverá vir acompanhada de manuais técnicos, carta/declaração do fabricante ou publicações originais do fabricante, fazendo constar no documento técnico a identificação e página do documento onde se encontra descrita cada uma das características ofertadas;

5.1.1 - Os documentos técnicos deverão ser apresentados junto com a proposta, por planilha contendo item, a descrição do item, e a comprovação técnica (de acordo com o item anterior);

5.1.2 - As especificações das características técnicas da solução de segurança ofertada deverão estar descritas de forma clara e detalhada;

5.1.3 - Será permitido o uso de expressões técnicas de uso comum na língua inglesa.

A empresa declarada vencedora deverá informar a marca e o modelo referência do objeto ofertado;

A SEMAD, a seu exclusivo critério, poderá solicitar amostra da solução completa ofertada pelo licitante vencedor para realização de testes que venham demonstrar a efetiva conformidade com a especificação técnica constante deste Termo de Referência.

5.2.1 - A adjudicação da solução vencedora dependerá da aprovação dos testes de funcionalidade da solução de segurança, a serem realizados na demonstração. Deverá fornecer declaração de revenda autorizada da solução ofertada e declaração que possuirá, pelo menos, 1 (um) profissional com certificação do fabricante da solução ofertada no momento da entrega dos serviços.

O não atendimento das exigência acima acarretará na desclassificação do licitante vencedor.

6. METODOLOGIA DE CÁLCULO

A quantidade de licenças foi calculada de acordo com a quantidade de equipamentos existentes na rede de dados da SEMAD, sendo que, 10% será alocado para reserva técnica, para uso em equipamentos que sejam adquiridos posteriormente.

7. DISTRIBUIÇÃO E ARMAZENAMENTO DOS EQUIPAMENTOS

Todas as licenças serão utilizadas de forma imediata, com exceção das alocadas para reserva técnica.

8. GARANTIA DOS MATERIAIS E SERVIÇOS

O período de garantia das licenças deverá ser de 36 (trinta e seis) meses e 3 (três) meses para o serviço de instalação, contados a partir da data de emissão do comprovante de recebimento definitivo**.** O período de garantia superior a 12 meses é necessário por se tratar de licenças de uso;

No período de garantia deverá ser prestada assistência técnica/manutenção ou substituição corretiva a fim de manter a solução em perfeitas condições de uso, sem ônus adicionais para a SEMAD**;**

A assistência técnica deverá solucionar a ocorrência, após sua abertura pelo SEMAD, entre 8h e 17h, de segunda a sexta-feira, em até 7 (sete) dias, ao final dos quais, caso não tenha sido solucionado, deverá ser substituído por solução idêntica ou superior.

9. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

1. Entregar os produtos no prazo de 30 (trinta) dias corridos a contar da emissão do empenho;
2. Entregar oficialmente os itens do objeto contratados e/ou executados, juntamente com a apresentação da Nota Fiscal ou Fatura correspondente;
3. Substituir, arcando com as despesas decorrentes, os produtos que apresentarem defeitos, imperfeições, alterações, irregularidades ou quaisquer características discordante às exigidas pelo setor solicitante, ainda que constatados depois do recebimento e/ou pagamento;
4. Manter sempre atualizado o seu endereço, número do telefone fixo e/ou celular, fax, e-mail ou outro meio de contato, junto à CONTRATANTE;
5. informar na Nota Fiscal e/ou Fatura a descrição dos itens do objeto contratados e/ou executados, de acordo com as especificações constantes da Nota de Empenho;
6. Pagar pontualmente os fornecedores e obrigações fiscais, em relação à entrega dos itens do objeto;
7. Pagar todos os tributos e contribuições fiscais ou parafiscais que incidam ou venham a incidir de forma direta ou indireta sobre a execução dos itens do objeto contratados, bem como as despesas eventuais de frete;

10. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

1. Emitir Nota de Empenho a crédito da CONTRATADA, no valor correspondente ao valor total dos itens do objeto contratados, executados e entregues em caráter definitivo;
2. Enviar por e-mail Nota de Empenho, digitalizada, emitida em favor da CONTRATADA, ou, na indisponibilidade desta tecnologia, enviá-la por outros meios (fax, postal etc.);
3. Permitir o acesso do pessoal da CONTRATADA às dependências da CONTRATANTE, para execução dos itens do objeto contratado;
4. Impedir que pessoas não autorizadas pela CONTRATADA executem quaisquer itens do objeto contratado;
5. Fornecer todas as condições e informações necessárias, para que a CONTRATADA possa executar os itens do objeto contratados conforme exigências do presente edital e respectivos anexos;
6. Acompanhar e fiscalizar o cumprimento das obrigações assumidas pela CONTRATADA;
7. Solicitar à CONTRATADA retificação da entrega de itens do objeto contratados cujos padrões de qualidade estejam aquém das exigências contidas no presente edital e respectivos anexos;
8. Informar das irregularidades, defeitos, vícios ou incorreções detectados durante a entrega de itens do objeto contratados, para que a CONTRATADA adote as medidas indispensáveis à adequação às especificações e regras constantes do presente edital e respectivos anexos;
9. Exigir que a CONTRATADA entregue os itens do objeto contratados consoante as exigências estabelecidas no presente edital e respectivos anexos;
10. Rejeitar total ou parcialmente itens do objeto contratados, executados em desacordo com as exigências contidas no presente edital e respectivos anexos;
11. Notificar por escrito a CONTRATADA, quando ocorrer eventuais imperfeições na execução de itens do objeto contratados, fixando prazo para sua correção;
12. A fiscalização exercida pela CONTRATANTE não excluirá ou reduzirá a responsabilidade da CONTRATADA pela perfeita execução do item do objeto.

11. PRAZO DE EXECUÇÃO E CRITÉRIOS DE ACEITAÇÃO DO SERVIÇO

1. A entrega dos objetos deverá ser realizada de uma única vez, no prazo de 30 (trinta) dias corridos a contar da emissão do empenho, respeitando todas especificações e condições previstas neste Termo;
2. A entrega deverá ser feita na Secretaria do Meio Ambiente e Desenvolvimento Sustentável, na 11ª Avenida, nº 1.272 - Setor Leste Universitário - CEP: 74.605-060 - Goiânia - GO;
3. A Gerência de Tecnologia - GETEC é a unidade responsável pelo recebimento dos produtos, através do servidor Edjalma Queiroz da Silva. A entrega deverá ser realizada em dia e horário agendados, através do e-mail: getec.meioambiente@goias.gov.br;
4. A entrega dos serviços deverá ser realizada de forma definitiva;

12. SANÇÕES

1. Sem prejuízo das demais sanções legais cabíveis, pelo não cumprimento dos compromissos acordados poderão ser aplicadas, a critério da CONTRATANTE, as seguintes penalidades à CONTRATADA:
2. Ficará impedido de licitar e de contratar com o Estado e será descredenciado no CADFOR, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em edital e no contrato, além das demais cominações legais, garantido o direito à ampla defesa, o licitante que, convocado dentro do prazo de validade de sua proposta:

a) não assinar o contrato ou a ata de registro de preços;

b) não entregar a documentação exigida no edital;

c) apresentar documentação falsa;

d) causar o atraso na execução do objeto;

e) não mantiver a proposta;

f) falhar na execução do contrato;

g) fraudar a execução do contrato;

h) comportar-se de modo inidôneo;

i) declarar informações falsas; e

j) cometer fraude fiscal.

§ 1º A inexecução contratual, inclusive por atraso injustificado na execução do contrato ou instrumento equivalente, sujeitará a contratada, além das cominações legais cabíveis, à multa de mora, graduada de acordo com a gravidade da infração, obedecidos os seguintes limites máximos:
10% (dez por cento) sobre o valor do contrato ou instrumento equivalente, em caso de descumprimento total da obrigação, inclusive no caso de recusa do adjudicatário em firmar o contrato ou retirar a nota de empenho, dentro de 10 (dez) dias contados da data de sua convocação;
0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso, sobre o valor da parte do fornecimento não realizado;
0,7% (sete décimos por cento) sobre o valor da parte do fornecimento não realizado, por cada dia subsequente ao trigésimo.

3. Antes da aplicação de qualquer penalidade será garantido ao licitante o direito ao contraditório e à ampla defesa.
4. As sanções serão registradas e publicadas no CADFOR.
5. A multa poderá ser descontada dos pagamentos eventualmente devidos ou ainda, quando for o caso, cobrada judicialmente.

13. CONTRATO E RESCISÃO

1. O Contrato será substituído pela Nota de Empenho;
2. Constituem motivos para rescisão, caso houver, por parte do licitante:

- Atraso injustificado na entrega do serviço;
- Não atender ou atender de forma parcial as especificações técnicas do objeto;
- O cometimento reiterado de faltas no fornecimento do serviço;
- A ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da execução do contrato.

3. Constituem motivos para rescisão, caso houver, por parte do contratante:

- A não liberação, por parte da Administração, de local para fornecimento, nos prazos estipulados;
- Razões de interesse público, de alta relevância e amplo conhecimento, justificadas e determinadas pela máxima autoridade da esfera administrativa a que está subordinado o contratante e exaradas no processo administrativo a que se refere o contrato.

14. PAGAMENTO

1. O pagamento será no prazo de 30 (trinta) dias após a entrega da nota fiscal na Gerência de Gestão e Finanças, devidamente atestada pelo Gestor (a);
2. Em atenção ao disposto no Art. 4º da Lei nº 18.364, de 10 de janeiro de 2014, o pagamento será efetivado por meio de crédito em conta-corrente do favorecido aberta exclusivamente em Instituição Bancária contratada para centralizar movimentação financeira dos Órgãos da Administração Direta (Caixa Econômica Federal);
3. **A contratada deverá emitir a Nota Fiscal em nome do Fundo Estadual do Meio Ambiente – FEMA, CNPJ nº. 01.037.124/0001-04.**

15. **SERVIDOR RESPONSÁVEL PELO ACOMPANHAMENTO/GESTOR DO CONTRATO**

1. A responsabilidade pelo acompanhamento, recebimento, aceite e fiscalização dos equipamentos ficará por conta do servidor Edjalma Queiroz da Silva, Gerente de Tecnologia, fone: (62) 3201-5270. São suas atribuições:

- Acompanhar a execução e fiscalizar o fiel cumprimento das obrigações pactuadas no referido instrumento;
- Observar e fazer cumprir os prazos de sua vigência;
- Verificar se os prazos foram atendidos, e se as demais especificações estão de acordo com o contrato;
- Observar a regularidade das despesas empenhadas, de conformidade com a previsão de pagamento quando for o caso;
- Atestar a execução total ou parcial do objeto contratado, encaminhando as notas fiscais ao setor competente;

EDJALMA QUEIROZ DA SILVA, **Gerente**, em 18/10/2021

ANEXO II

RELAÇÃO DE DOCUMENTOS QUE PODERÃO SER SUBSTITUÍDOS PELA APRESENTAÇÃO DO CERTIFICADO DE REGISTRO CADASTRAL -CRC

A licitante poderá apresentar o CRC em substituição aos documentos relativos à habilitação jurídica, regularidade fiscal e qualificação econômico-financeira, conforme listados abaixo:

16. **Habilitação Jurídica**

a) Registro comercial, no caso de empresa individual;

b) Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, que poderá ser substituído por documento consolidado das alterações, devidamente comprovado o último registro no órgão próprio e, no caso de sociedades por ações, acompanhado dos documentos de eleição de seus administradores;

c) Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova da diretoria em exercício;

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

e) Cédula de identidade do sócio ou representante legal da empresa, na forma do inciso I do art. 28 da Lei 8.666/93

17. **Regularidade Fiscal**

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ) do Ministério da Fazenda ou prova de inscrição no Cadastro de Pessoas Físicas (CPF), conforme art. 29, inc. I, da Lei Federal nº 8.666/1993

b) Prova de inscrição no Cadastro de Contribuintes estadual ou municipal, relativo ao domicílio ou sede da licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) Cópias das certidões negativas de débitos ou equivalentes na forma da lei, relativas:

I - à Seguridade Social – INSS(CERTIDÃO CONJUNTA DA PGFN/RFB/INSS/DIVIDA ATIVA DA UNIÃO, EMITIDA PELA RFB)

II - ao Fundo de Garantia por Tempo de Serviço (FGTS);

III - Comprovação de regularidade perante ao CADIN Estadual;

IV - CND de Suspensão e/ou impedimento de Licitar ou Contratar com Administração Pública emitida pelo Sistema COMPRASNET.GO,

V - à Fazenda Pública do Estado do domicílio ou sede da licitante (Certidão de Débito em Dívida Ativa);

VI - à Fazenda Pública do Município do domicílio ou sede da licitante (Tributos Mobiliários);

VII - à Fazenda Pública do Estado de Goiás (Certidão de Débito em Dívida Ativa).

VIII - à Débitos Trabalhistas - **Certidão Negativa de Débitos Trabalhistas (CNDT)**

2.1 Caso a participação no certame se dê através da matriz, com possibilidade de que a execução contratual se dê por filial, ou vice-versa, a prova de regularidade fiscal, mediante apresentação do CRC, deverá ser de ambas (deliberação da Procuradoria Geral do Estado através de seu Despacho "AG" nº 001930/2008).

18. **Qualificação Econômico-Financeira**

a) Certidão negativa de falência e recuperação judicial, emitida pelo distribuidor da sede da pessoa jurídica.

b) Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados, através de índices oficiais, quando encerrado há mais de três meses da data da apresentação da proposta;

c) Comprovação da boa situação financeira da empresa através de no mínimo um dos seguintes índices contábeis, o qual deverá ser maior ou igual a 1:

d) -ILC: Índice de Liquidez Corrente ou,

-ILG: Índice de Liquidez Geral ou,
- GS: Grau de Solvência

ILC =	AC / PC	=	Ativo Circulante / Passivo Circulante
ILG =	AC + RLP / PC + PNC	=	Ativo Circulante + Realizável a Longo Prazo / Passivo Circulante + Passivo Não Circulante
GS =	AT	=	Ativo

	PC + PNC		Total Passivo Circulante + Passivo Não Circulante

e) Nos termos do art. 32, § 1º da Lei Federal 8.666/1993, fica dispensada a documentação exigida no item 3, subitem 2) e 3), no caso do fornecimento de bens para pronta entrega com valor inferior a R$ 80.000,00 (oitenta mil reais);

f) Nos termos do art. 2º A do Decreto Estadual nº 7.466, de 18/10/2011, não será exigido das microempresas e empresas de pequeno porte a apresentação do balanço patrimonial do último exercício social, no caso do fornecimento de bens para pronta entrega;

19. **Qualificação técnica**

- Apresentar para fins de qualificação técnica, no mínimo 01 (um) atestado/declaração fornecido por pessoa jurídica de direito público ou privado, comprovando que a licitante já forneceu, satisfatoriamente, o objeto deste edital ou outro semelhante, bem como prova de atendimento de requisitos previstos em lei especial, quando for o caso. O atestado/declaração deverá conter, no mínimo, o nome da empresa/órgão contratante, telefone de contato e o nome do responsável pelo mesmo.

Notas:

- O Certificado de Regularidade de Registro Cadastral - CRC, deverá estar dentro do prazo de validade com status homologado. Caso o CRC apresente *"status irregular"*, será assegurado a licitante o direito de apresentar a documentação atualizada e regular na própria sessão.
  As certidões sem prazo de validade deverão ter sido expedidas com prazo não superior a 60 dias de antecedência da data de abertura da licitação.

ANEXO III
MODELO DE PROPOSTA COMERCIAL
PREGÃO ELETRÔNICO Nº 19/2021

Nome da Empresa:
CNPJ:
Endereço:
Fone: : E-mail:
Conta-Corrente nº: Banco: **CAIXA ECONOMICA FEDERAL** Nº da Agência:
À SEMAD:

Prezados Senhores:

Apresentamos a nossa proposta para o fornecimento do objeto do Pregão Eletrônico nº 19/2021. A validade de nossa proposta é de *** (**********) dias corridos, a contar da data de abertura da licitação.

7.1 Detalhamento	7.2 Quantidade	7.3 Prazo para sua Realização	7.4 Estimativa de Custo Unitário	7.5 Estimativa de Custo
7.1.1 Solução de segurança de endpoint	415		R$	**R$**
7.1.2 Serviço de instalação e implantação	1	30 dias	R$	**R$** **TOTAL: R$**

Finalmente, declaramos que temos pleno conhecimento de todos os aspectos relativos à licitação em causa e nossa plena concordância com as condições estabelecidas no Edital da licitação e seus Anexos, conforme demonstrativo abaixo.

Local, __ , de _____, de 2021.

Assinatura

ANEXO IV
MODELO DE DECLARAÇÃO DE ENQUADRAMENTO NA
LEI COMPLEMENTAR Nº 123/06
(deverá ser entregue, após a fase de lances, junto com a proposta comercial)
PREGÃO ELETRÔNICO Nº 19/2021

A (nome/razão social) _____, inscrita no CNPJ nº _____, por intermédio de seu representante legal o(a) Sr.(a) _____, portador(a) da Carteira de Identidade nº _____ e do CPF nº _____, DECLARA, sob as penas da lei, que cumpre os requisitos legais para a qualificação como microempresa ou empresa de pequeno porte, e atesta a aptidão para usufruir do tratamento favorecido estabelecido nos arts. 42 a 49 da Lei Complementar federal n. 123/06, não possuindo nenhum dos impedimentos previstos no § 4º do artigo 3º da referida Lei.

Local e data.

_____

Representante legal

Nota: A falsidade desta DECLARAÇÃO, objetivando os benefícios da Lei Complementar nº 123/06, caracterizará crime de que trata o Art. 299 do Código Penal, sem prejuízo do enquadramento em outras figuras penais e das penalidades previstas neste Edital.

ANEXO V
MODELO DE DECLARAÇÃO DOS FATOS IMPEDITIVOS E CIÊNCIA DAS CLÁUSULAS DO EDITAL
(deverá ser entregue, após a fase de lances, junto com a proposta comercial)

PREGÃO ELETRÔNICO Nº 19/2021

À
Secretaria de Estado de Meio Ambiente e Desenvolvimento Sustentável - SEMAD

Palácio Pedro Ludovico Teixeira nº 400 – 2º andar, Setor Central – CEP 74.015-908 – Goiânia-GO

Assunto: Declaração

A Empresa _____, CNPJ nº _____, DECLARA:

- Sob as penas da lei, que, até a presente data, inexistem fatos impeditivos para sua habilitação no presente processo licitatório, ciente da obrigação de declarar ocorrências posteriores.
- Ter ciência de todas as cláusulas do Edital, sendo que o descumprimento de qualquer dessas cláusulas acarretará a aplicação das penalidades conforme art. 87 da Lei nº 8.666/93, principalmente a declaração de inidoneidade para licitar ou contratar com a Administração Pública.
- inexistem quaisquer dos fatos impeditivos à participação na licitação, diante das vedações constantes no art. 9º da Lei nº 8.666/1993

Local e data:___ / ___ / 2021

_____
(carimbo, razão social e assinatura do responsável)

ANEXO VI

MODELO DE DECLARAÇÃO QUE NÃO EMPREGA MENOR
(ART. 7º, XXXIII, CF/88 C/C ART. 27, V, LEI 8.666/93)
(deverá ser entregue, após a fase de lances, junto com a proposta comercial)
PREGÃO ELETRÔNICO Nº 19/2021

_____, inscrito no CNPJ nº __.___.___.____/__ por intermédio de seu representante legal o(a) Sr(a)_____, portador(a) da Carteira de Identidade nº _____ e do CPF nº ___.___.___-__DECLARA, em atendimento ao disposto no inciso XXXIII, do art. 7º da Constituição Federal, combinado com o inciso V, do art. 27, da Lei n. 8666/93, que não possui, em seu quadro de pessoal, empregados menores de 18 anos em trabalho noturno, insalubre ou perigoso e qualquer trabalho por menor de 16 anos, salvo, na condição de aprendizes, a partir de 14 anos.

Local e data:___ / ___ / 2021

ANEXO VII
EDITAL PREGÃO ELETRÔNICO Nº 19/2021

COMPROMISSO ARBITRAL

1) Qualquer disputa ou controvérsia relativa à interpretação ou execução deste ajuste, ou de qualquer forma oriunda ou associada a ele, no tocante a direitos patrimoniais disponíveis, e que não seja dirimida amigavelmente entre as partes (precedida da realização de tentativa de conciliação ou mediação), deverá ser resolvida de forma definitiva por arbitragem, nos termos das normas de regência da CÂMARA DE CONCILIAÇÃO, MEDIAÇÃO E ARBITRAGEM DA ADMINISTRAÇÃO ESTADUAL (CCMA).
2) A CÂMARA DE CONCILIAÇÃO, MEDIAÇÃO E ARBITRAGEM DA ADMINISTRAÇÃO ESTADUAL (CCMA) será composta por Procuradores do Estado, Procuradores da Assembleia Legislativa e por advogados regularmente inscritos na OAB/GO, podendo funcionar em Comissões compostas sempre em número ímpar maior ou igual a 3 (três) integrantes (árbitros), cujo sorteio se dará na forma do art. 14 da Lei Complementar Estadual nº 114, de 24 de julho de 2018, sem prejuízo da aplicação das normas de seu Regimento Interno, onde cabível.
3) A sede da arbitragem e da prolação da sentença será preferencialmente a cidade de Goiânia.
4) O idioma da Arbitragem será a Língua Portuguesa.
5) A arbitragem será exclusivamente de direito, aplicando-se as normas integrantes do ordenamento jurídico ao mérito do litígio.
6) Aplicar-se-á ao processo arbitral o rito previsto nas normas de regência (incluso o seu Regimento Interno) da CÂMARA DE CONCILIAÇÃO, MEDIAÇÃO E ARBITRAGEM DA ADMINISTRAÇÃO ESTADUAL (CCMA), na Lei nº 9.307, de 23 de setembro de 1996, na Lei nº 13.140, de 26 de junho de 2015, na Lei Complementar Estadual nº 144, de 24 de julho de 2018 e na Lei Estadual nº 13.800, de 18 de janeiro de 2001, constituindo a sentença título executivo vinculante entre as partes.
7) A sentença arbitral será de acesso público, a ser disponibilizado no sítio eletrônico oficial da Procuradoria-Geral do Estado, ressalvadas as hipóteses de sigilo previstas em lei.
8) As partes elegem o Foro da Comarca de Goiânia para quaisquer medidas judiciais necessárias, incluindo a execução da sentença arbitral. A eventual propositura de medidas judiciais pelas partes deverá ser imediatamente comunicada à CÂMARA DE CONCILIAÇÃO, MEDIAÇÃO E ARBITRAGEM DA ADMINISTRAÇÃO ESTADUAL (CCMA), e não implica e nem deverá ser interpretada como renúncia à arbitragem, nem afetará a existência, validade e eficácia da presente cláusula arbitral."

Local e data.

GOIANIA, 21 de outubro de 2021.

Documento assinado eletronicamente por **MORIAN SCUSSEL MALBURG**, **Pregoeiro (a)**, em 21/10/2021, às 10:20, conforme art. 2º, § 2º, III, "b", da Lei 17.039/2010 e art. 3ºB, I, do Decreto nº 8.808/2016.

A autenticidade do documento pode ser conferida no site **http://sei.go.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=1** informando o código verificador **000024609901** e o código CRC **DE1EE5FE**.

RUA 82 Nº 400, PALÁCIO PEDRO LUDOVICO TEIXEIRA, 2º ANDAR, ALA LESTE - Bairro SETOR SUL - GOIANIA - GO - CEP 74015-908 - (62)3201-5210.