gov.br

Compras.gov.br

COLÉGIO MILITAR DE BRASÍLIA - CMB
Fls. 461
Rub:

PREGÃO ELETRÔNICO
01/2024

CONTRATANTE (UASG)
160064 – Colégio Militar de Brasília, Unidade Gestora Gerenciadora;

UNIDADE GESTORA PARTICIPANTE
158314 – Intituto Federal do Ceará – Campus Limeiro do Norte. participantes dos itens 18, 19, 20 e 25.

OBJETO
Registro de preços para aquisição de pontos de acesso e equipamentos complementares para rede sem fio

VALOR TOTAL DA CONTRATAÇÃO
R$ 5.390.580,47 (cinco milhões trezentos e noventa mil, quinhentos e oitenta reais e quarenta e sete centavos)

DATA DA SESSÃO PÚBLICA
Dia 25/06/2024 às 10h (horário de Brasília)

CRITÉRIO DE JULGAMENTO:
menor preço

MODO DE DISPUTA:
aberto e fechado

PREFERÊNCIA ME/EPP/EQUIPARADAS
SIM (Itens 5, 11, 17 a 20, 22 a 25)

Sumário

Aprovado pelo DESPACHO n. 00148/2024/CGAO/SCGP/CCU/AGU, de 16 de abril de 2024

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
COLÉGIO MILITAR DE BRASÍLIA

PREGÃO ELETRÔNICO nº 01/2024

(Processo Administrativo n° 64250.011956/2023-72)

Torna-se público que o Colégio Militar de Brasília, por meio da Seção de Aquisições, Licitações e Contratos (SALC), sediado no SGAN 902, Conjunto "A", Asa Norte, CEP 70.790-020, na cidade de Brasília-DF, realizará licitação, para registro de preços, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 1º de abril de 2021, do Decreto nº 11.462, de 31 de março de 2023, e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

1. DO OBJETO

1.1. O objeto da presente licitação é a aquisição de pontos de acesso e equipamentos complementares para rede sem fio, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será dividida em itens (1 ao 11 e 15 ao 26) como também grupo único, formado pelos itens 12 a 14, conforme tabela constante do Termo de Referência, facultando-se ao licitante a participação em quantos itens e grupo único de interesse.

2. DO REGISTRO DE PREÇOS

2.1. As regras referentes aos órgãos gerenciador e participantes, bem como a eventuais adesões são as que constam da minuta de Ata de Registro de Preços.

3. DA PARTICIPAÇÃO NA LICITAÇÃO

3.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

3.1.1. Os interessados deverão atender às condições exigidas no cadastramento no Sicaf até o terceiro dia útil anterior à data prevista para recebimento das propostas.

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

3.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação,

Aprovado pelo DESPACHO n. 00148/2024/CGAO/SCGP/CCU/AGU, de 16 de abril de 2024

devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

3.4. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

3.5. Para os itens 5, 11, 17 ao 20, 22 ao 25, a participação é exclusiva a microempresas e empresas de pequeno porte, nos termos do art. 48 da Lei Complementar nº 123, de 14 de dezembro de 2006.

3.5.1. A obtenção do benefício a que se refere o item anterior fica limitada às microempresas e às empresas de pequeno porte que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

3.6. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133, de 2021, pessoa física e para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006 e do Decreto n.º 8.538, de 2015.

3.7. Não poderão disputar esta licitação:

3.7.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);

3.7.2. autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;

3.7.3. empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

3.7.4. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

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

3.7.6. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

3.7.7. pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

3.7.8. agente público do órgão ou entidade licitante;

3.7.9. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

3.7.10. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei nº 14.133, de 2021.

3.8. O impedimento de que trata o item 3.7.4 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

3.9. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 3.7.2 e 3.7.3 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

3.10. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

3.11. O disposto nos itens 3.7.2 e 3.7.3 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

3.12. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei nº 14.133/2021.

3.13. A vedação de que trata o item 3.7.8 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

4. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

4.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

4.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento "MENOR PREÇO"adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

4.3. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto nos itens 8.1.1 e 8.12.1 deste Edital.

4.4. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

4.4.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

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

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

4.4.4. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

4.5. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.

4.6. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

4.6.1. no item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo "não" impedirá o prosseguimento no certame, para aquele item;

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

4.7. A falsidade da declaração de que trata os itens 4.4 ou 4.6 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

4.8. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

4.9. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

4.10. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

4.11. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:

4.11.1. a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

4.11.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.

4.12. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

4.12.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e

4.12.2. percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto.

4.13. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 4.11 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

4.14. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

4.15. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

Aprovado pelo DESPACHO n. 00148/2024/CGAO/SCGP/CCU/AGU, de 16 de abril de 2024

5. DO PREENCHIMENTO DA PROPOSTA

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

5.1.1. valor unitário e total do item;

5.1.2. Marca;

5.1.3. Fabricante;

5.1.4. Quantidade cotada, devendo respeitar o máximo previsto.

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

5.2.1. O licitante NÃO poderá oferecer proposta em quantitativo inferior ao máximo previsto para contratação.

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

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

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

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

5.7. Na presente licitação, a Microempresa e a Empresa de Pequeno Porte poderão se beneficiar do regime de tributação pelo Simples Nacional.

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

5.8.1. O prazo de validade da proposta não será inferior a 60 (sessenta) dias, a contar da data de sua apresentação.

5.8.2. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;

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

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

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

Aprovado pelo DESPACHO n. 00148/2024/CGAO/SCGP/CCU/AGU, de 16 de abril de 2024

6.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

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

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

6.5. O lance deverá ser ofertado pelo valor unitário do item para os itens 1 ao 11 e 15 ao 26, e para os itens 12 a 14 do grupo único deverá ser ofertado pelo valor global.

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

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

6.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de 0,01 (um) centavo.

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

6.10. Será adotado para o envio de lances no pregão eletrônico o modo de disputa "aberto e fechado", os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

6.10.1. A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

6.10.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

6.10.3. No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

6.10.4. Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

6.10.5. Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

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

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

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

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

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

Aprovado pelo DESPACHO n. 00148/2024/CGAO/SCGP/CCU/AGU, de 16 de abril de 2024

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

6.17. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

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

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

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

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

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

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

6.18.1.1. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

6.18.1.2. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

6.18.1.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

6.18.1.4. desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

6.18.2. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

6.18.2.1. empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

6.18.2.2. empresas brasileiras;

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

6.18.2.4. empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

Aprovado pelo DESPACHO n. 00148/2024/CGAO/SCGP/CCU/AGU, de 16 de abril de 2024

6.19. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

6.19.1. Tratando-se de licitação em grupo, a contratação posterior de item específico do grupo exigirá prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou a entidade e serão observados os seguintes preços unitários máximos homologados como critério de aceitabilidade.

~~6.19.1.1. ...~~

~~6.19.1.2. ...~~

6.19.2. ~~[Não será admitida a previsão de preços diferentes em razão do local de entrega ou de acondicionamento, tamanho de lote ou qualquer outro motivo] / [Será admitida a previsão de preços diferentes conforme os critérios abaixo]:~~

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

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

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

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

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

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

7. DA FASE DE JULGAMENTO

7.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 3.7 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

7.1.1. SICAF;

7.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis); e

7.1.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep).

7.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei nº 8.429, de 1992.

7.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. (IN nº 3/2018, art. 29, *caput*)

7.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (IN nº 3/2018, art. 29, §1º).

7.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação. (IN nº 3/2018, art. 29, §2º).

7.3.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

7.4. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com os itens 3.5.1 e 4.6 deste edital.

7.5. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no artigo 29 a 35 da IN SEGES nº 73, de 30 de setembro de 2022.

7.6. Será desclassificada a proposta vencedora que:

7.6.1. contiver vícios insanáveis;

7.6.2. não obedecer às especificações técnicas contidas no Termo de Referência;

7.6.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

7.6.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

7.6.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

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

7.7.1. A inexequibilidade, na hipótese de que trata o caput, só será considerada após diligência do pregoeiro, que comprove:

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

7.7.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

7.8. Em contratação de serviços de engenharia, além das disposições acima, a análise de exequibilidade e sobrepreço considerará o seguinte:

7.8.1. Nos regimes de execução por tarefa, empreitada por preço global ou empreitada integral, semi-integrada ou integrada, a caracterização do sobrepreço se dará pela superação do valor global estimado;

7.8.2. No regime de empreitada por preço unitário, a caracterização do sobrepreço se dará pela superação do valor global estimado e pela superação de custo unitário;

7.8.3. Será exigida garantia adicional do licitante vencedor cuja proposta for inferior a 85% (oitenta e cinco por cento) do valor orçado pela Administração, equivalente à diferença entre este último e o valor da proposta, sem prejuízo das demais garantias exigíveis de acordo com a Lei.

7.9. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

7.10. Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de Planilha de Custos e Formação de Preços elaborada pela Administração, o licitante classificado em primeiro lugar será convocado para apresentar Planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

Aprovado pelo DESPACHO n. 00148/2024/CGAO/SCGP/CCU/AGU, de 16 de abril de 2024

7.11. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação;

7.11.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;

7.11.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

7.12. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.

8. DA FASE DE HABILITAÇÃO

8.1. Os documentos previstos no Termo de Referência, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

8.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

8.2. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

8.3. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

8.4. Quando permitida a participação de consórcio de empresas, a habilitação técnica, quando exigida, será feita por meio do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado.

8.4.1. Se o consórcio não for formado integralmente por microempresas ou empresas de pequeno porte e o termo de referência exigir requisitos de habilitação econômico-financeira, haverá um acréscimo de 30%, para o consórcio em relação ao valor exigido para os licitantes individuais.

8.5. Os documentos exigidos para fins de habilitação poderão ser apresentados em original, por cópia ou por qualquer outro meio expressamente admitido pela administração.

8.6. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133/2021.

8.7. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021).

8.8. Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

8.9. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

Aprovado pelo DESPACHO n. 00148/2024/CGAO/SCGP/CCU/AGU, de 16 de abril de 2024

8.10. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

8.10.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. (IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º).

8.11. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. (IN nº 3/2018, art. 7º, *caput*).

8.11.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação. (IN nº 3/2018, art. 7º, parágrafo único).

8.12. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

8.12.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de duas horas, prorrogável por igual período, contado da solicitação do pregoeiro.

8.13. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

8.13.1. Os documentos relativos à regularidade fiscal que constem do Termo de Referência somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

8.13.2. Respeitada a exceção do subitem anterior, relativa à regularidade fiscal, quando a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, a verificação ou exigência do presente subitem ocorrerá em relação a todos os licitantes.

8.14. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64, e IN 73/2022, art. 39, §4º):

8.14.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

8.14.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

8.15. Na análise dos documentos de habilitação, a comissão de contratação poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

8.16. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no subitem 8.12.1.

8.17. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

8.18. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação (art. 4º do Decreto nº 8.538/2015).

8.19. Quando a fase de habilitação anteceder a de julgamento e já tiver sido encerrada, não caberá exclusão de licitante por motivo relacionado à habilitação, salvo em razão de fatos supervenientes ou só conhecidos após o julgamento.

Aprovado pelo DESPACHO n. 00148/2024/CGAO/SCGP/CCU/AGU, de 16 de abril de 2024

9. DA ATA DE REGISTRO DE PREÇOS

9.1. Homologado o resultado da licitação, o licitante mais bem classificado terá o prazo de 05 (cinco) dias, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, cujo prazo de validade encontra-se nela fixado, sob pena de decadência do direito à contratação, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

9.2. O prazo de convocação poderá ser prorrogado uma vez, por igual período, mediante solicitação do licitante mais bem classificado ou do fornecedor convocado, desde que:

(a) a solicitação seja devidamente justificada e apresentada dentro do prazo; e

(b) a justificativa apresentada seja aceita pela Administração.

9.3. A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no sistema de registro de preços.

9.4. Serão formalizadas tantas Atas de Registro de Preços quantas forem necessárias para o registro de todos os itens constantes no Termo de Referência, com a indicação do licitante vencedor, a descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais condições.

9.5. O preço registrado, com a indicação dos fornecedores, será divulgado no PNCP e disponibilizado durante a vigência da ata de registro de preços.

9.6. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente justificada.

9.7. Na hipótese de o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidas, fica facultado à Administração convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

10. DA FORMAÇÃO DO CADASTRO DE RESERVA

10.1. Após a homologação da licitação, será incluído na ata, na forma de anexo, o registro:.

10.1.1. dos licitantes que aceitarem cotar o objeto com preço igual ao do adjudicatário, observada a classificação na licitação; e

10.1.2. dos licitantes que mantiverem sua proposta original

10.2. Será respeitada, nas contratações, a ordem de classificação dos licitantes ou fornecedores registrados na ata.

10.2.1. A apresentação de novas propostas na forma deste item não prejudicará o resultado do certame em relação ao licitante mais bem classificado.

10.2.2. Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem cotar o objeto com preço igual ao do adjudicatário antecederão aqueles que mantiverem sua proposta original.

10.3. A habilitação dos licitantes que comporão o cadastro de reserva será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

10.3.1. quando o licitante vencedor não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital; ou

10.3.2. quando houver o cancelamento do registro do fornecedor ou do registro de preços, nas hipóteses previstas nos art. 28 e art. 29 do Decreto nº 11.462/23.

10.4. Na hipótese de nenhum dos licitantes que aceitaram cotar o objeto com preço igual ao do adjudicatário concordar com a contratação nos termos em igual prazo e nas condições propostas pelo primeiro classificado, a Administração, observados o valor estimado e a sua eventual atualização na forma prevista no edital, poderá:

10.4.1. convocar os licitantes que mantiveram sua proposta original para negociação, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

10.4.2. adjudicar e firmar o contrato nas condições ofertadas pelos licitantes remanescentes, observada a ordem de classificação, quando frustrada a negociação de melhor condição.

11. DOS RECURSOS

11.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

11.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

11.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

11.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

11.3.2. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.

11.3.3. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

11.3.4. na hipótese de adoção da inversão de fases prevista no § 1º do art. 17 da Lei nº 14.133, de 2021, o prazo para apresentação das razões recursais será iniciado na data de intimação da ata de julgamento.

11.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

11.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

11.6. Os recursos interpostos fora do prazo não serão conhecidos.

11.7. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

11.8. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

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

11.10. Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico https://www.cmb.eb.mil.br/index.php/licitacoes.

12. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

12.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

12.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;

12.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

12.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

12.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;

12.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou

12.1.2.4. deixar de apresentar amostra;

12.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

12.1.3. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

12.1.3.1. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

12.1.4. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação

12.1.5. fraudar a licitação

12.1.6. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

12.1.6.1. agir em conluio ou em desconformidade com a lei;

12.1.6.2. induzir deliberadamente a erro no julgamento;

12.1.6.3. apresentar amostra falsificada ou deteriorada;

12.1.7. praticar atos ilícitos com vistas a frustrar os objetivos da licitação

12.1.8. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

12.2. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

12.2.1. advertência;

12.2.2. multa;

12.2.3. impedimento de licitar e contratar e

12.2.4. declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

12.3. Na aplicação das sanções serão considerados:

12.3.1. a natureza e a gravidade da infração cometida.

12.3.2. as peculiaridades do caso concreto

12.3.3. as circunstâncias agravantes ou atenuantes

12.3.4. os danos que dela provierem para a Administração Pública

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

12.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de 30 (trinta) dias úteis, a contar da comunicação oficial.

12.4.1. Para as infrações previstas nos itens 12.1.1, 12.1.2 e 12.1.3, a multa será de 0,5% a 15% do valor do contrato licitado.

12.4.2. Para as infrações previstas nos itens 12.1.4, 12.1.5, 12.1.6, 12.1.7 e 12.1.8, a multa será de 15% a 30% do valor do contrato licitado.

12.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

12.6. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

12.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 12.1.1, 12.1.2 e 12.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

12.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 12.1.4, 12.1.5, 12.1.6, 12.1.7 e 12.1.8, bem como pelas infrações administrativas previstas nos itens 12.1.1, 12.1.2 e 12.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

12.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 12.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.

12.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

12.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

12.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

12.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

12.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

13. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

13.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

13.2. A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

13.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, pelo seguinte meio: pregoeiro@cmb.eb.mil.br.

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

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

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

14. DAS DISPOSIÇÕES GERAIS

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

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

14.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.

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

14.5. 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, o princípio da isonomia, a finalidade e a segurança da contratação.

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

14.7. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

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

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

14.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico http://www.cmb.eb.mil.br/index.php/licitacoes.

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

14.11.1. ANEXO I - Termo de Referência

14.11.1.1. Apêndice do Anexo I – Estudo Técnico Preliminar

14.11.2. ANEXO II – Minuta de Termo de Contrato

14.11.3. ANEXO III – Minuta de Ata de Registro de Preços

14.11.4. ANEXO IV – Modelo de Proposta de Preço

Aprovado pelo DESPACHO n. 00148/2024/CGAO/SCGP/CCU/AGU, de 16 de abril de 2024

COLÉGIO MILITAR DE BRASÍLIA
Fls. 470
Rub:

Brasília-DF, 10 de junho de 2024.

Confeccionado por:

ADELSON PEDRO DA SILVA – 1º Ten
Chefe da SALC

Aprovado por:

THALES MOTA DE ALENCAR – Cel
Ordenador de Despesas

EM BRANCO

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
COLÉGIO MILITAR DE BRASÍLIA
PREGÃO ELETRÔNICO SRP nº XX/2023

(Processo Administrativo nº 64250.011956/2023-72)

ANEXO I - TERMO DE REFERÊNCIA

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Registro de preços visando aquisição pontos de acesso e equipamentos complementares para rede sem fio, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste Instrumento.

GRUPO	ITEM	DESCRIÇÃO/ ESPECIFICAÇÃO	CATMAT	UND.	QTD.	VALOR UNITÁRIO	VALOR TOTAL
-	1	PONTOS DE ACESSO PARA REDE SEM FIO (INDOOR)	484745	UND.	60	R$ 23.371,20	R$ 1.402.272,00
-	2	PONTOS DE ACESSO PARA REDE SEM FIO (OUTDOOR)	484745	UND.	06	R$ 25.011,00	R$ 150.066,00
-	3	FIREWALL PARA ALTA DISPONIBILIDADE	481646	UND	01	R$ 121.489,29	R$ 121.489,29
-	4	SISTEMA DE ENERGIA ININTERRUPTA (UPS/NOBREAK) 2000VA	481193	UND	30	R$ 7.469,68	R$ 224.090,40
-	5	SISTEMA DE ENERGIA ININTERRUPTA (UPS/NOBREAK) 20KVA	458567	UND.	01	R$ 56.070,45	R$ 56.070,45
-	6	SWITCH DE ACESSO L2+L3 48 PORTAS 10/100/1000BASE-T	485141	UND.	10	R$ 54.155,96	R$ 541.559,60
-	7	SWITCH 48 PORTAS FIBER COM 2 PORTAS UPLINK/STACK QSFP28	481771	UND.	02	R$ 178.622,40	R$ 357.244,80
-	8	ESTAÇÃO DE TRABALHO DO TIPO DESKTOP COMPACTO TIPO 1	601761	UND.	50	R$ 8.985,00	R$ 449.250,00
-	9	ESTAÇÃO DE TRABALHO DO TIPO DESKTOP COMPACTO TIPO 2	601761	UND.	30	R$ 12.152,00	R$ 364.560,00
-	10	NOTEBOOK	613702	UND.	30	R$ 12.535,68	R$ 376.070,40
--	11	CÂMERE DE VIDEOCONFERENCIA	300634	UND.	05	R$ 11.873,33	R$ 59.366,67

Aprovado pelo DESPACHO n. 00148/2024/CGAO/SCGP/CCU/AGU, de 16 de abril de 2024

GRUPO	ITEM	DESCRIÇÃO/ ESPECIFICAÇÃO	CATMAT	UND.	QTD.	VALOR UNITÁRIO	VALOR TOTAL
		CORPORATIVA					
GRUPO 1	12	PROCESSADOR / GERENCIADOR PARA MONITORES DE VIDEOWALL	606303	UND.	01	R$ 24.670,00	R$ 24.670,00
	13	MONITOR PROFISSIONAL PARA VIDEOWALL	604256	UND.	08	R$ 17.413,33	R$ 139.306,64
	14	SUPORTE PARA MONITOR PROFISSIONAL PARA VIDEOWALL	608412	UND.	08	R$ 1.577,50	R$ 12.620,00
-	15	PROJETOR DATASHOW 4600 LUMENS	613277	UND.	60	R$ 8.939,80	R$ 536.388,00
-	16	PROJETOR 12000 4K UHD LASER	613277	UND.	02	R$ 119.929,67	R$ 239.859,34
-	17	ADAPTADOR DISPLAY PORT/HDMI	453465	UND.	100	R$ 52,46	R$ 5.246,00
-	18	ALICATE DE CRIMPAR	291168	UND.	8	R$ 319,25	R$ 2.554,00
-	19	UNIDADE DE DISCO EXTERNO 2TB	426009	UND.	32	R$ 1.137,07	R$ 36.386,24
-	20	MONITOR 24"	464064	UND.	56	R$ 1.159,23	R$ 64.916,88
-	21	PLACA DE VIDEO 1GB HDMI	426940	UND.	50	R$ 1.684,31	R$ 84.215,50
-	22	PLACA DE REDE PADRÃO PCI-EXPRESS	462602	UND.	30	R$ 180,60	R$ 5.418,00
-	23	MEMÓRIA RAM DDR3 8GB	473420	UND.	30	R$ 229,67	R$ 6.890,00
-	24	MEMÓIRA RAM DDR4 8GBPO	604331	UND.	30	R$ 324,94	R$ 9.748,30
-	25	ÁLCOOL ISOPROPÍLICO	475009	UND.	12	R$ 20,29	R$ 243,48
-	26	LICENÇA OFFICE	27472	UND.	50	R$ 2.401,57	R$ 120.078,50
Valor Total estimado é de: R$ 5.390.580,47 (cinco milhões trezentos e noventa mil, quinhentos e oitenta reais e quarenta e sete centavos)							

1.2. Os bens objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar.

1.3. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

1.4. O prazo de vigência da contratação é de 12 (doze) meses contados da data da assinatura da Ata de Registro de Preços, na forma do artigo 105 da Lei n° 14.133, de 2021.

1.5. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. O objeto da contratação está previsto no Plano de Contratações Anual 2024, conforme consta das informações básicas deste Termo de Referência.

2.2.O objeto da contratação também está alinhado com a Estratégia de Governo Digital 2024 e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2024 do CMB, conforme demonstrado abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS (PLANO DE GESTÃO 2024 do CMB)	
ID	Objetivos Estratégicos
OE06	Manter, expandir e aprimorar a infrestrutura de TIC do CMB.
OE07	Aumentar a eficiência da estrutura de comunicação (dados, voz e video) do CMB

ALINHAMENTO AO PDTIC 2024	
ID	Ação do PDTIC
IE-15	Expandir a estrutura de comunicação de dados sem fio - *Wireless – no CMB.*

2.3.Por tratar de oferta de serviços públicos digitais, o objeto da contratação será integrado à Plataforma Gov.br, nos termos do Decreto nº 8.936, de 19 de dezembro de 2016, e suas atualizações, de acordo com as especificações deste Termo de Referência.

I) ID PCA no PNCP: 00394452000103-0-000049/2024;

II) Data de publicação no PNCP: 20/5/2023;

III) Id do item no PCA: 84 a 89;

IV) Classe/Grupo: 7010, 7030, 7050, 7060 e 7080; e

V) Identificador da Futura Contratação: 160064-90013/2023.

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

3.1 A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

4. REQUISITOS DA CONTRATAÇÃO

Sustentabilidade:

4.1.Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

4.2.que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares;

4.3.que os materiais utilizados não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como

mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenilpolibromados (PBBs), éteres difenil-polibromados (PBDEs);

4.4.priorizar os bens que sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2.

4.5.os bens deverão ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.

Indicação de marcas ou modelos (Art. 41, inciso I, da Lei nº 14.133, de 2021):

4.6.Na presente contratação será admitida a indicação da(s) seguinte(s) marca(s), característica(s) ou modelo(s), de acordo com as justificativas contidas nos Estudos Técnicos Preliminares:

4.6.1. SonicWall para os itens 1, 2 e 3;

4.6.2. Ruckus para os itens 6 e 7

Subcontratação

4.7. Não é admitida a subcontratação do objeto contratual.

Garantia da contratação

4.8.Não haverá exigência da garantia da contratação dos artigos 96 e seguintes da Lei nº 14.133, de 2021, pelas razões constantes do Estudo Técnico Preliminar.

5. MODELO DE EXECUÇÃO DO OBJETO

Condições de Entrega

5.1.O prazo de entrega dos bens é de 60 (sessenta) dias, contados do(a) recebimento do contrato/empenho, pela contratada, em remessa única.

5.2.Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 05 (cinco) dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

5.3.Os bens deverão ser entregues no seguinte endereço: SGAN 902/904 - Asa Norte CEP 70790-020 Brasília-DF.

Garantia, manutenção e assistência técnica

5.4.O prazo de garantia contratual dos bens, complementar à garantia legal, é de, no mínimo 36 (trinta e seis)) meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

5.5.A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.

Aprovado pelo DESPACHO n. 00148/2024/CGAO/SCGP/CCU/AGU, de 16 de abril de 2024

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

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

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

6.5 Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

Fiscalização

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

Fiscalização Técnica

6.7.O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

6.7.1. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º, e Decreto nº 11.246, de 2022, art. 22, II);

6.7.2. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

6.7.3. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que

5.6. A garantia abrange a realização da manutenção corretiva dos bens pelo próprio Contratado, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

5.7. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.

5.8. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

5.9. Uma vez notificado, o Contratado realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 05 (cinco) dias úteis, contados a partir da data de retirada do equipamento das dependências da Administração pelo Contratado ou pela assistência técnica autorizada.

5.10. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada do Contratado, aceita pelo Contratante.

5.11. Na hipótese do subitem acima, o Contratado deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo Contratante, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos.

5.12. Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do Contratante ou a apresentação de justificativas pelo Contratado, fica o Contratante autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir do Contratado o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.

5.13. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade do Contratado.

5.14. A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

6. MODELO DE GESTÃO DO CONTRATO

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

Aprovado pelo DESPACHO n. 00148/2024/CGAO/SCGP/CCU/AGU, de 16 de abril de 2024

adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV).

6.7.4. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V).

6.7.5. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

Fiscalização Administrativa

6.8.O fiscal administrativo do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

6.8.1. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

Gestor do Contrato

6.9.O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

6.10. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

6.11. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem

o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

6.12. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

6.13. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

6.14. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

6.15. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

7. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Recebimento

7.1. Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

7.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 10 (dez) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

7.3. O recebimento definitivo ocorrerá no prazo de 05(cinco) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

7.4. Para as contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021, o prazo máximo para o recebimento definitivo será de até 05(cinco) dias úteis.

7.5.O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

7.6.No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

7.7.O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

7.8.O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança dos bens nem a responsabilidade ético-profissional pela perfeita execução do contrato.

Liquidação

7.9.Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §3º da Instrução Normativa SEGES/ME nº 77/2022.

7.9.1. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

7.10. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

7.10.1. o prazo de validade;

7.10.2. a data da emissão;

7.10.3. os dados do contrato e do órgão contratante;

7.10.4. o período respectivo de execução do contrato;

7.10.5. o valor a pagar; e

7.10.6. eventual destaque do valor de retenções tributárias cabíveis.

7.11. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

7.12. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

7.13. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).

7.14. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

7.15. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

7.16. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

7.17. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

Prazo de pagamento

7.18. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

7.19. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice Geral de Preços do Mercado (IGP-M) de correção monetária.

Forma de pagamento

7.20. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

7.21. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

7.22. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

7.22.1. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

7.23. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

Cessão de crédito

7.24. É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020, conforme as regras deste presente tópico.

7.25. A eficácia da cessão de crédito, de qualquer natureza, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

7.26. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, nos termos do Parecer JL-01, de 18 de maio de 2020.

7.27. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração. (INSTRUÇÃO NORMATIVA Nº 53, DE 8 DE JULHO DE 2020 e Anexos)

7.28. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do contratado.

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E FORMA DE FORNECIMENTO

Forma de seleção e critério de julgamento da proposta

8.1.O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO.

Forma de fornecimento

Aprovado pelo DESPACHO n. 00148/2024/CGAO/SCGP/CCU/AGU, de 16 de abril de 2024

8.2.O fornecimento do objeto será integral

Exigências de habilitação

8.3.Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

Habilitação jurídica

8.4.**Pessoa física:** cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

8.5.Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

8.6.Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

8.7.Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

8.8.Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.° 77, de 18 de março de 2020.

8.9.Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

8.10. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

8.11. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

8.12. Agricultor familiar: Declaração de Aptidão ao Pronaf – DAP ou DAP-P válida, ou, ainda, outros documentos definidos pela Secretaria Especial de Agricultura Familiar e do Desenvolvimento Agrário, nos termos do art. 4º, §2º do Decreto nº 10.880, de 2 de dezembro de 2021.

8.13. Produtor Rural: matrícula no Cadastro Específico do INSS – CEI, que comprove a qualificação como produtor rural pessoa física, nos termos da Instrução Normativa RFB n. 971, de 13 de novembro de 2009 (arts. 17 a 19 e 165).

8.14. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

8.15. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

8.16. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

8.17. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

8.18. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

8.19. Prova de inscrição no cadastro de contribuintes [Estadual/Distrital] ou [Municipal/Distrital] relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

8.20. Prova de regularidade com a Fazenda [Estadual/Distrital] ou [Municipal/Distrital] do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

8.21. Caso o fornecedor seja considerado isento dos tributos [Estadual/Distrital] ou [Municipal/Distrital] relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

8.22. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

8.23. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea "c", da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;

8.24. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

8.25. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, com relação aos itens 1, 4, 6, 7, 8, 9, 10, 15 e 16, comprovando;

8.25.1. índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

8.25.2. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

8.25.3. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;

8.25.4. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

8.26. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação patrimônio líquido mínimo de 10% (dez por cento) do valor total estimado da parcela pertinente.

8.27. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

Qualificação Técnica

8.28. Comprovação de aptidão para o fornecimento de bens similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

8.28.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

8.28.1.1. Fornecimento de solução de rede sem fio (itens 1 e 2), com quantitativo mínimo de 05 (cinco) e pelo menos 1 (um) equipamento de firewall para o item 3, comprovando a instalação;

8.28.1.2. Fornecimento de nobreaks (itens 4 e 5);

8.28.1.3. Fornecimento de switches de rede (itens 6 e 7), comprovando instalação;

8.29. Em caso de participação de cooperativas, será exigida a seguinte documentação complementar:

8.29.1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971;

8.29.2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

8.29.3. A comprovação do capital social proporcional ao número de cooperados necessários à execução contratual;

8.29.4. O registro previsto na Lei n. 5.764, de 1971, art. 107;

8.29.5. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato; e

8.29.6. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa: a) ata de fundação; b) estatuto social com a ata da assembleia que o aprovou; c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia; d) editais de convocação das três últimas assembleias gerais extraordinárias; e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

8.29.7. A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

9.1 O custo estimado total da contratação é de R$ 5.390.580,47 (cinco milhões trezentos e noventa mil, quinhentos e oitenta reais e quarenta e sete centavos), conforme custos unitários apostos na tabela acima.

9.2 A estimativa de custo levou em consideração o risco envovido na contratação e sua alocação entre contratante e contratado, cnofomre especificado na matriz de risco constante do contrato.

9.3 Em caso de licitação para Registro de Preços, os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações (art. 25 do Decreto nº 11.462/2023):

9.3.1. em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos do disposto na alínea "d" do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;

9.3.2. em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

9.3.3. serão reajustados os preços registrados, respeitada a contagem da anualidade e o índice previsto para a contratação; ou

9.3.4. poderão ser repactuados, a pedido do interessado, conforme critérios definidos para a contratação.

10. ADEQUAÇÃO ORÇAMENTÁRIA

10.1 As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

10.2 A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

COLÉGIO MILITAR DE BRASÍLIA
Fls. 478
Rub.

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
COLÉGIO MILITAR DE BRASÍLIA

ESTUDO TÉCNICO PRELIMINAR

Processo Administrativo nº 64250.011956/2023-72

Aquisição de pontos de acesso e equipamentos complementares para continuidade do projeto da rede sem fio do CMB

Brasília, 31 de outubro de 2023.

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
COLÉGIO MILITAR DE BRASÍLIA

Histórico de Revisões

Data	Versão	Descrição	Autor
28/05/2023	1.0	Finalização da primeira versão do documento	TEN SANTOS
12/09/2023	1.1	Inserção das soluções viáveis para os grupos de equipamentos	TEN SANTOS
14/06/2023	1.2	Inserção dos custos do projeto	TEN SANTOS
16/06/2023	1.3	Adequação do Custos Totais de Propriedade	TEN SANTOS
26/09/2023	1.4	Revisão de quantitativos e especificações	TEN SANTOS
28/05/2024	1.5	Revisão Após parecer da AGU	TEN SANTOS

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
COLÉGIO MILITAR DE BRASÍLIA

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

INTRODUÇÃO

O presente documento tem por objetivo analisar a viabilidade técnica e econômica para aquisição de novos pontos de acesso e equipamentos complementares para rede sem fio do CMB, com prestação de garantia e suporte técnico.

O ETP tem por objetivo identificar e analisar os cenários para o atendimento de demanda registrada no Documento de Formalização da Demanda – DFD, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar a tomada de decisão e o prosseguimento do respectivo processo de contratação.

Referência: Inciso XI, do art. 2º e art. 11 da IN SGD/ME nº 94/2022.

1. INFORMAÇÕES BÁSICAS

Processo administrativo n.º 64250.011956/2023-72

Contratação de Tecnologia de Informação e Comunicação - TIC

2. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

2.1 Motivação / Justificativa

2.1.1 A missão do Colégio Militar de Brasília - CMB não difere de outros colégios militares que é ministrar a educação básica, nos anos finais do ensino fundamental (do 6º ao 9º ano) e no ensino médio. O ensino no CMB é realizado em consonância com a legislação federal de educação e obedece às leis e aos regulamentos em vigor no Exército, em especial às normas e diretrizes do Departamento de Ensino e Cultura do Exército Brasileiro, órgão gestor da linha de ensino do Exército

2.1.2 Diante de dessa missão de ensino, o CMB está se adequando a nova realidade que é promover a conectividade de internet, por meio de uma rede sem fio, para alunos e professores, visando uma melhor qualidade de ensino. A rede sem fio em espaços educacionais se tornou algo básico hoje em dia. Em uma sociedade conectada e sob demanda, as instituições de ensino têm uma quantidade imensa de pressão para atender às demandas de WiFi dos ambientes de aprendizado do século XXI.

2.1.3 Em 2022 o CMB adquiriu uma solução composta de FIREWALL e PONTOS DE ACESSO para atender os espaços educacionais e tornou-se nada menos que um recurso crítico. Seja na sala de aula, seja em apoio direto à missão acadêmica, seja em cargos de apoio para manter as instalações funcionando, a rede sem fio só se torna mais importante a cada bimestre de 2022.

2.1.4 Essa aquisição possibilitou as seguintes vantagens:

2.1.4.1 Possibilitou que os alunos do CMB tivessem acesso a uma ampla variedade de conhecimentos, conteúdos educativos, sendo complementares à sua educação formal;

2.1.4.2 Alunos e professores conquistam um ambiente de aprendizado mais inteligente e interativo, tornando as experiências com os conteúdos muito mais relevantes, induzindo a uma melhor aprendizagem;

2.1.4.3 Beneficiou as metas de gestão escolar;

2.1.4.4 Contribuiu para despertar maior interesse nos alunos;

2.1.4.5 Possibilitou compartilhamento das informações, facilitando a organização dos alunos e professores;

2.1.5 No intuito de dar continuidade a esses benefícios e proteger o recurso que já foi aplicado no projeto de rede sem fio, o CMB necessita aumentar o número de pontos de acesso. Conforme já levantado e estudado pela Seção de Informática seriam necessários no mínimo 30 pontos de acesso.

2.1.6 Além dos pontos de acesso e para que a solução de rede sem fio fique o mais completa possível, será necessário a aquisição de nobreaks para proteção e continuidade dos serviços após possíveis falhas na rede elétrica. Também será necessária a aquisição de novos switches com tecnologia POE e principalmente switches core, para que a nova demanda de tráfego de dados não tenha gargalos que atualmente já são visíveis. Não menos importante é necessária a aquisição de novos notebooks e desktops que possuam placas e antenas capazes de suportar o WIFI6 e seus novos protocolos de segurança.

2.1.7 Pretende-se alcançar com essa aquisição a continuidade dos serviços de rede sem fio, permitindo que os usuários acessem os recursos da rede educacional praticamente de qualquer local conveniente, proporcionar que o aluno possa ser potencialmente mais produtivo, podendo realizar suas atividades em qualquer espaço conveniente nas dependências do CMB e diminuir a complexidade dos cabos físicos reais sendo executados em vários locais dentro do CMB;

2.1.8 Desse modo, considera-se indispensável a aquisição de novos pontos de acesso e equipamentos complementares para rede sem fio do CMB.

3. ÁREA REQUISITANTE

Identificação da Área requisitante	Nome do responsável
SEÇÃO DE INFORMÁTICA	Alex Julio Favela dos Santos – 1º Ten

4. NECESSIDADES TECNOLÓGICA

4.1 Para os pontos de acesso o CMB necessita de equipamentos compatíveis com os Access Point SonicWave 231c da marca Sonicwall. Isso porque, nesse ano de 2022 foram adquiridos 11 (onze) access point e 01 (um) firewall do mesmo fabricante, e todos estão em garantia e suporte até 2025.

4.2 Esses pontos de acesso atualmente geram três SSIDs. a) SSID ALUNO; b) SSID ADM; e c) SSID VISITANTE. Estão em teste até a data deste documento outros dois SSID, SSID PROFESSOR e SSID JE (jogos escolares).

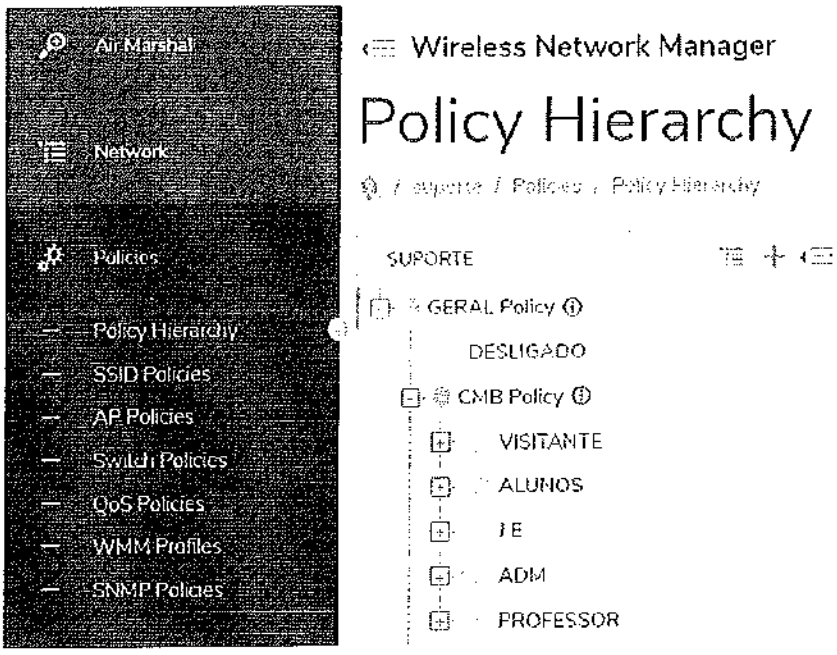

Figura 1: SSDIs na hierarquia do CMB

4.3 Essa contextualização é válida para que seja possível justificar a necessidade tecnológica pretendida. Conforme figura 1 as redes JE e PROFESSOR estão off-line visto que estão sendo realizados testes para essas redes.

4.4 Para que os pontos de acesso a rede sem fio estejam de acordo com as normas estabelecidas pelo CITEX / 7º CTA os equipamentos devem possuir funcionalidades NATIVAS, que possibilitem a segurança e não permitam a comunicação com a rede EBNet. Algumas funcionalidades são praticadas atualmente no CMB em relação a tecnologia para rede sem fio. São elas:

TECNOLOGIA	APLICABILIDADE	REDES (SSIDs)	STATUS
Capture ATP: analisa o comportamento em uma plataforma *sandbox multimotor* que inclui emulação completa do sistema, análise no nível de	Arquivos PDF e EXECUTÁVEIS devem ser negados ou verificados antes da sua execução, na rede sem fio do CMB. Dentro desta característica predispor o	ALUNOS VISITANTES JE	Executando (para rede JE alguns parâmetros estão em

hipervisor, sandbox virtualizado e RTDMI™, que usa técnicas de inspeção baseadas em memória em tempo real para forçar o malware a revelar seu armamento na memória.	tamanho do arquivo para não prejudicar a memória do ponto de acesso. Deverá ser possível gerar veredito (avisos) para o administrador da rede, em casos de documentos Microsoft Office. Para os casos de protocolos, possibilitar o bloqueio do tráfego FTP e desejável que tenha lista de exclusão MD5 (verificação da assinatura digital), esse último em teste pelo CMB. Todas essas funcionalidades também para arquivos em nuvem.		teste)
Serviço de Filtragem de Conteúdo: que compara websites requisitados com um enorme banco de dados na nuvem, que contém milhões de classificações de URLs, endereços IP e websites. Fornece ferramentas aos administradores para criar e aplicar políticas que permitam ou impeçam o acesso a sites, baseadas na identidade individual ou de grupo, ou por horário, para mais de 50 categorias predefinidas.	Os pontos de acesso para rede sem fio atualmente dispõem de 93 categorias e são filtradas aproximadamente 30 categorias, sendo as mais importantes: 1. Violência/Ódio/Racismo 2. Roupa íntima 3. Nudismo 4. Pornografia 5. Armas 6. Conteúdo adulto/maduro 7. Culto/Oculto 8. Drogas/Drogas Ilícitas 9.Habilidades ilegais/habilidades questionáveis 10. Educação Sexual 11. Jogos de azar 12. Álcool/Tabaco 13. Malware 14. Radicalização e Extremismo 15. Questionável 16. Prevenção de proxy e anonimizadores 17. Spyware e Adware 18. Proxies HTTP abertos 19. Maconha 20. Traição 21. Ataque de força Bruta 22. Phishing e outras fraudes	TODAS AS REDES	Executando (em teste questões de *schedule*)

	23. Redes de bots 24. URLs de SPAM Possibilite ainda, filtrar por níveis de reputação e o mais importante, enseje campos para Whitelist e Black list, sendo a primeira para liberar sites que são confiáveis, porém bloqueados pela lista predefinida e, para o último caso, o bloqueio de sites que não estão na lista pré-definida, porém são danosos para o CMB.		
Política de Segurança por ACL: permita definir regras de classificação ou estabelecer critérios para fornecer segurança na rede, bloqueando usuários não autorizados e permitindo que usuários autorizados acessem áreas ou recursos específicos. Fornece segurança básica para acesso à rede, controlando se os pacotes são encaminhados ou bloqueados nas portas do pontos de acesso.	Criação de filtros que permitem classificar pacotes de dados de acordo com um conteúdo específico no cabeçalho do pacote, como endereço de origem, endereço de destino, número da porta de origem, número da porta de destino e muito mais. Além da segmentação lógica e as regras de Firewall, atualmente foi criada a regra com destino a rede EBNet (10.0.0.0), que bloqueia todos os usuários da rede sem fio tanto na origem e no destino conteúdos HTTP, HTTPS, Terminal Service TCP/UDP, SSH, Telnet, TFTP, DNS TCP/UDP, DHCP, FTP Control/Data, Kerberos TCP/UDP, NetBios NS/DGM/SSN tanto TCP/UDP, SMB, RPC Services e IPSec. Existem outros níveis de serviço e o ponto de acesso é capaz de fazer grupos desses serviços para minimizar o número de ACLs. Além disso permitir o gerenciamento de banda tanto em upload como download e o direcionamento dos pacotes para esses serviços.	TODAS AS REDES	Executando (em teste outros níveis de serviço)

	A política de segurança de ACLs estão sendo muito bem usadas e fornecem um excelente controle de fluxo de tráfego.		
Geo-IP Filter: permita que os administradores bloqueiem as conexões de ou para uma localização geográfica para resolver o endereço IP público para um determinado país. Esse recurso pode ser usado em dois modos, bloqueio geral ou bloqueio por meio de regras de acesso do firewall.	Atualmente regra criada para monitorar os IPs de áreas denominadas perigosas em distribuição de ransoware como México, Colômbia, Costa Rica e Peru. Nada foi bloqueado e somente testado. Geração de relatório para análise de tráfego. Os atuais pontos de acesso permitem que sejam criadas listas específicas de IPs e que não bloquei ou caiam e monitoramento todo o range de um país.	JE	Testado (regra desabilitada)
Controle de Aplicativos: forneça uma solução para definir regras de política para assinaturas de aplicativos.	Foram realizadas as políticas de controle de aplicativos que incluem políticas globais de controle de aplicativos e políticas de regras de aplicativos que são mais direcionadas, tais como os grupos de transferencia de arquivos (Depositfiles, Divshare, Mediafire, Mega, Torrentz.eu, ZippyShare, Rapidgator, Filefactory, Hugefiles, Box.net, Files.cx e Xunlei), messaging (DingTalk, WeChat, WhasApp, Skype, Facebook-menssager, Google_Duo e YiXin), midia social (facebook, Instagram, Linkdin, Xing, Twitter e Snapchat) media-streaming (Hulu, Netflix, Grooveshark, Shoutcast e Tunein) e outras categorias PornHub e bing. O controle de aplicação oferece controle granular sobre o tráfego de rede no nível de usuários, endereços de e-mail, agendamentos e sub-redes IP. A principal funcionalidade desse	Transferência de arquivos TODAS AS REDES (Regra de Diminuição da taxa de Uplink) Media-streaming e PornHub TODAS AS REDES (Regra para bloquear) Messaging e midia social TODAS AS REDES (Regra para alertar)	

	recurso de controle de acesso da camada de aplicativo é regular a navegação na Web, transferência de arquivos, e-mail e anexos de e-mail.		

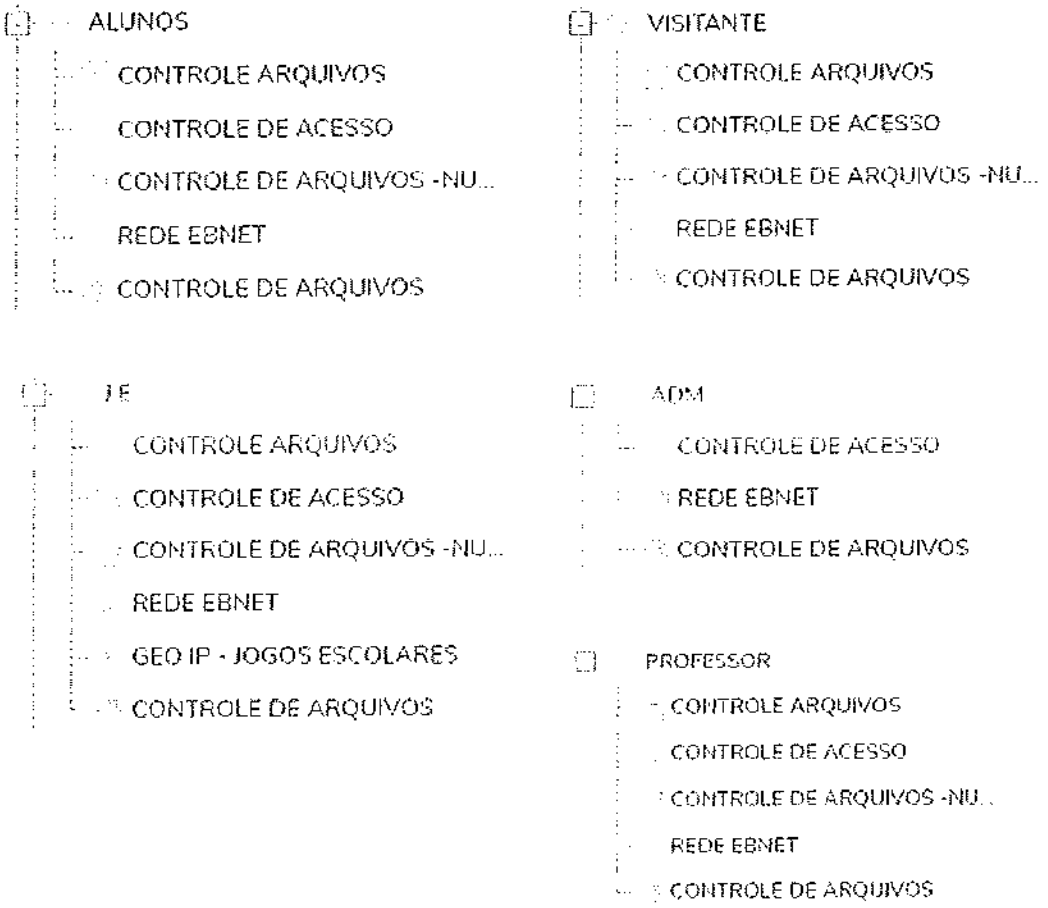

Figura 2: SSIDs e as regras de segurança criadas

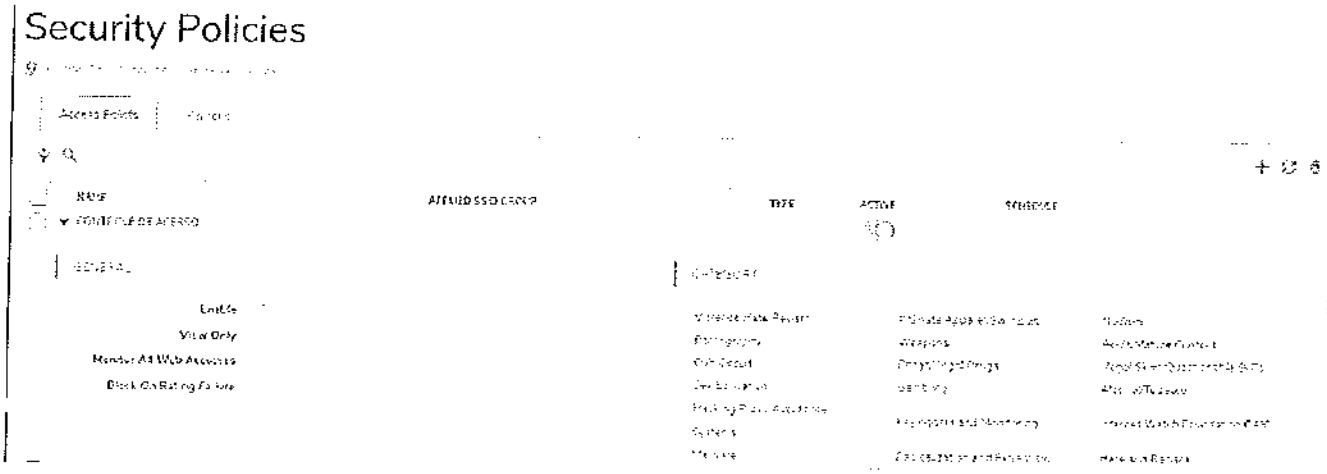

Figura 3: Detalhes da regra de segurança para controle de acesso.

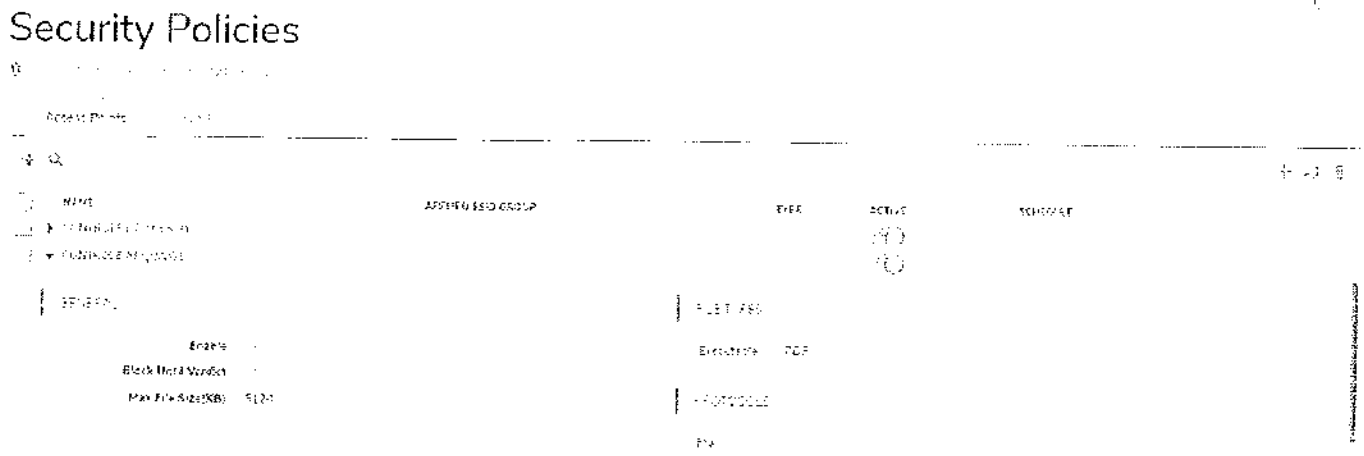

Figura 4: Detalhes da regra de segurança para controle de arquivos.

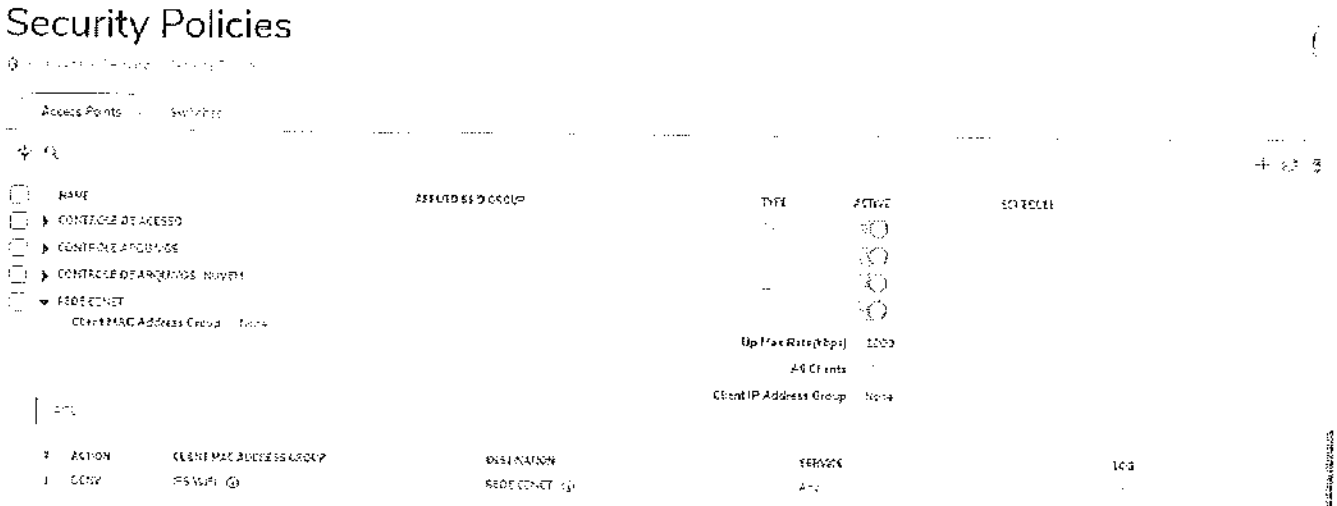

Figura 5: Detalhes da regra de segurança para política de segurança por ACL.

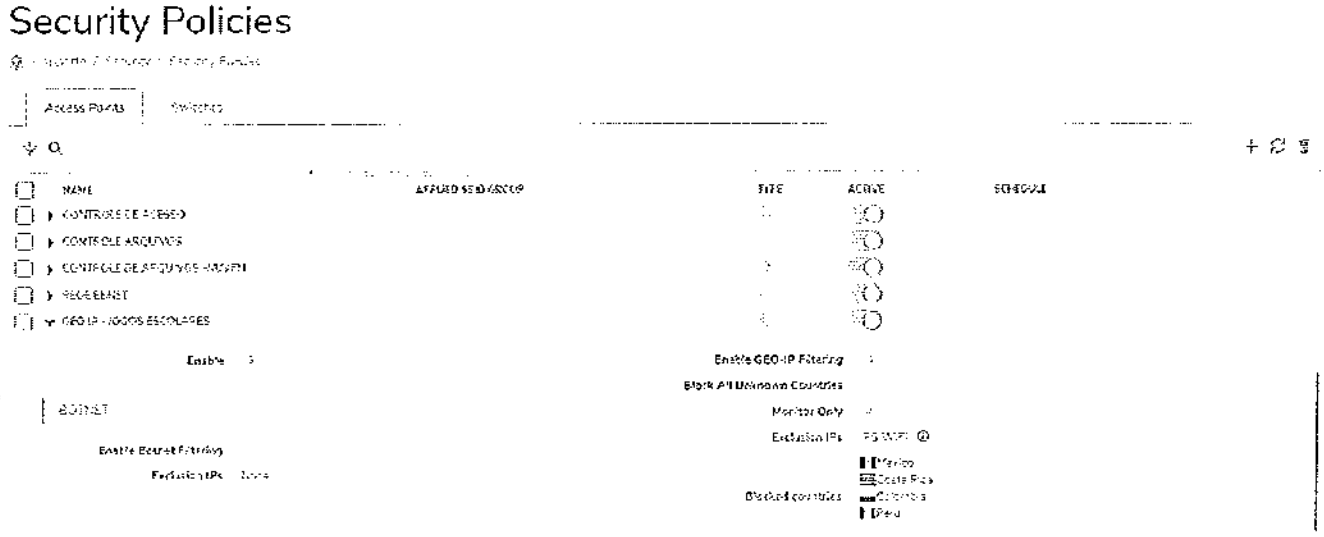

Figura 6: Detalhes da regra de segurança para GEO-IP.

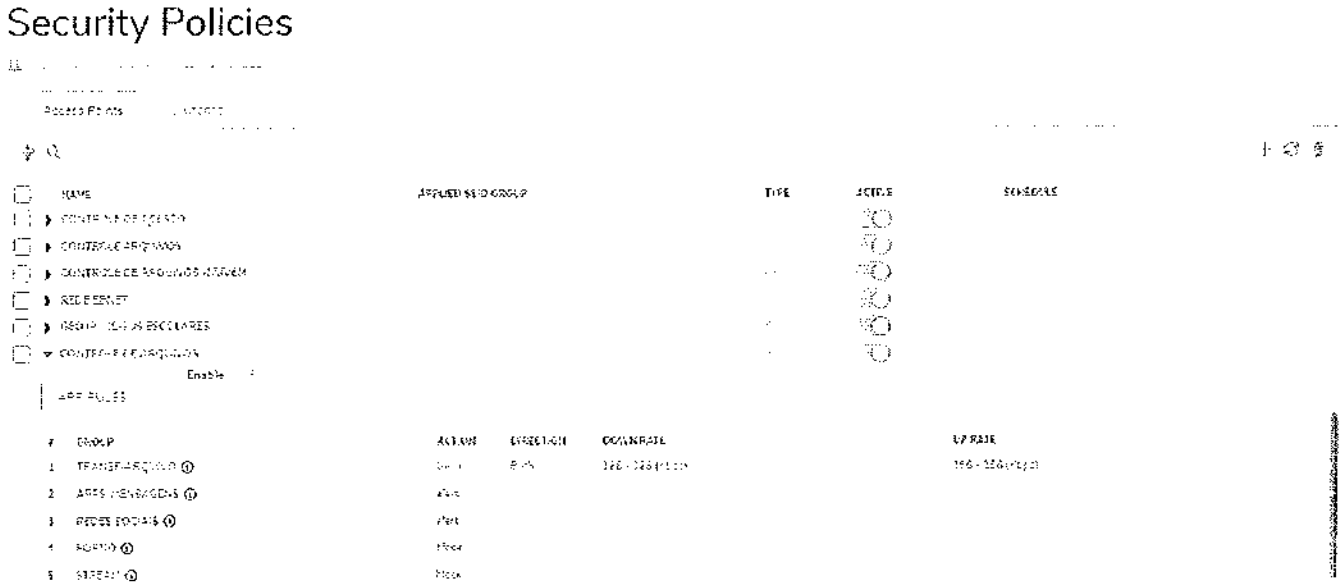

Figura 7: Detalhes da regra de segurança para controle de aplicativos.

4.5 Os pontos de acesso deverão ainda ter compatibilidade com a gerência centralizada em nuvem que possibilita um serviço de configuração e atualização de forma simples para fornecer conectividade de nuvem híbrida e de site a site com o Zero-Trust Security e o Least Privilege Security como uma oferta integrada.

4.6 Em complemento aos pontos de acesso, é necessário adquiri sistema de proteção elétrica para ligar os switches, que por sua vez, ligarão dos pontos de acesso por meio de tecnologia POE. Por esta motivação, devem ser adquiridos nobreaks entre 1.0 Kva e 2.0 Kva.

4.7 Além disso os nobreaks devem prover energia estabilizada, mantendo a tensão de alimentação da carga o dentro da faixa nominal de Brasília (220 v), evitando danos aos equipamentos e a perda de tarefas, trabalhos e relatórios com a súbita interrupção no fornecimento de energia ou variação de tensão, que já ocorreram e ocorrem no CMB.

4.8 Ainda na tratativa de falhas elétricas, outro equipamento a ser adquirido, para esse projeto de rede sem fio é um nobreak de maior capacidade. Esse nobreak deve sustentar o CPD do CMB. Sem um nobreak central não há como manter o mínimo de segurança em caso de falhas de energia. Desta forma, é importante a aquisição de um nobreak entre 15 Kva e 20 Kva.

4.9 É necessário também a aquisição de novos switches de acesso com tecnologia POE para ligar os pontos de acesso a rede e permitir um tráfego de dados mais robusto após a liberação da rede sem fio para alunos, professores e para administração do CMB. Nesse ponto deve-se atentar para duas configurações de switch. A primeira configuração será para os switches de acesso, que ligam diretamente os pontos de acesso sem fio e que geram a ponte com a rede cabeada. A segunda configuração será para switches que deverão estar no core de rede e que vão receber a ligação dos switches de acesso como também os servidores de serviços do CMB que proporcionam a entrega dos serviços de rede.

4.10 Para utilização da nova rede sem fio que já possibilita maior velocidade com WIFI 6 e protocolos de segurança como WPA3 é relevante a compra de novos computadores. Para maior aproveitamento se faz necessário a aquisição de desktops e notebooks que tenham placas de rede, processadores, memória e armazenamento atualizados e garantam um melhor aproveitamento da solução que será adquirida.

4.11 O CMB adquiriu somente um firewall para segurança da rede. Com esse firewall foi possível analisar o tráfego da rede e se estava adequado para suportar a nova carga. É possível alegar que com a chegada da rede sem fio para os alunos e colaboradores do colégio o tráfego vai duplicar. Ainda assim o firewall comprado pelo colégio consegue suportar.

4.12 Atualmente esse equipamento tem sido o CORE da rede, centralizando a maior parte do tráfego de dados, porém não se tem redundância desse equipamento o que torna um ponto de falha para entrada e saída para internet como para EBnet.

4.13 Desta forma, vamos aproveitar esse processo de compra e solicitar um firewall para fazer alta disponibilidade (H.A – high availability) que vai garantir a continuidade de serviços utilizados, mesmo em ocasiões de falhas por exemplo, de hardware, software, interrupção de energia etc.

4.14 Com o surgimento da pandemia e o crescimento do uso de tecnologias de comunicação, surge a necessidade de uma solução de vídeo conferência moderna, onde pode-se compartilhar conteúdo de telas e, assim, realizar aulas, palestras, entrevistas, reuniões e comunicados de forma controlada (acesso restrito/amplo).

4.15 Além do cenário atual da pandemia, o Colégio Militar de Brasília vinha adotando esta tecnologia para as salas de aula, com o objetivo de manter uma comunicação e colaboração eficaz. Além disso esse projeto vai proporcionar os seguintes benefícios pós pandemia:

a. Permite que diferentes escolas se conectem e colaborem facilmente;

b. Facilita viagens de campo virtuais;

c. Torna o aprendizado fora da sala de aula mais conveniente e fácil;

d. Permite que os alunos gravem as aulas para revisão posterior.

4.16 O intuito é modernizar a tecnologia de videoconferência atual, possibilitando a realização de aulas, reuniões e chamadas pelos militares do CMB com qualquer pessoa conectada à internet (em estação de trabalho compacta e câmera com microfone e som que proporcione mobilidade), de forma segura e protegida. Porém, para a utilização plena da solução pelos militares, além do uso já disponível de videoconferências em estações de trabalho e smartphones, há a necessidade de aquisição de equipamentos de videoconferência adequados para esse propósito.

4.17 Desta forma há um projeto de promover a modernização e ampliação da solução de videoconferência que apresenta em seu escopo a intenção de contratar equipamentos de videoconferência para uso compartilhado em salas de aula, reunião, assim como aparelhos individuais destinados a uso específico do Comandante.

4.18 Com a modernização da tecnologia, verificou-se a necessidade de aquisição de videowall que juntamente com a tecnologia da videoconferência teria uma melhor interatividade nas salas de aulas e conteúdos com mais qualidade e mais bem aproveitados.

4.19 Seria importante também para propagar as informações primordiais do colégio para um número maior de pessoas, proporcionando melhor interatividade e conhecimento em relação ao conteúdo que deverá ser repassado pelo CMB.

4.20 A solução de videowall poderá proporcione experiências interativas entre seus participantes uma vez que reuniões dessa natureza são corriqueiramente pautadas por apresentações que demandam tais recursos, além da necessidade de interação remota com outros comandos do Exército.

4.21 Somando-se aos equipamentos audiovisuais (videowall e videoconferência) o CMB precisa renovar seus projetores de sala de aula. Essa demanda é necessária para atender as necessidades relativas à realização e transmissão de eventos, aulas, treinamentos oferecidos pelo CMB para seus alunos, professores e colaboradores.

4.22 Por fim, e no intuito de aproveitar o processo de renovação de tecnologias, serão ainda solicitados nesse processo periféricos e ferramentas para manutenção de computadores, rede e outros equipamentos que podem ser aproveitados pelo CMB, e prover a diminuição de custos na aquisição de novos equipamentos.

4.23 Todos os detalhes da solução tecnológica estarão no item 7 desse documento.

5. REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO

5.1 A aquisição para esse projeto de rede sem fio deve prever serviços de instalação, reinstalação e configuração de pontos de acesso espalhados dentro das dependências do CMB.

5.2 A tabela abaixo ilustra como os requisitos tecnológicos da solução escolhida estão alinhados à necessidade do negócio.

Requisito tecnológico	Alinhamento com a necessidade do negócio
Os pontos de acesso devem ter compatibilidade com toda solução de rede sem fio já adquirida em 2022.	Aproveitar a estrutura física e lógica já adquirida, possibilitando a expansão da rede sem fio de acordo com os recursos financeiros disponíveis.

Os pontos de acesso devem ser utilizados para atender prioritariamente professores e alunos. De forma secundária atender as demandas administrativas do CMB, que atualmente é atendida também pela rede cabeada.	Uma solução dedicada para promover o aprimoramento da aprendizagem, facilitar a interação entre alunos e professores e atender às crescentes demandas do ensino contemporâneo.
Proteção de distúrbios elétricos por meio de nobreaks que atrapalham a continuidade de atividades.	Proteger os equipamentos da rede de dados como um todo e principalmente que assegurar o não corrompimento de dados do CMB.
Desktop e notebooks atualizados para atender professores e a administração do CMB.	Renovação do parque tecnológico e substituição de equipamentos antigos e inutilizáveis.
Videoconferência, Videowall e Projetor multimídia.	Proporcionar melhor aproveitamento do conteúdo e permitir maior interação entre alunos, professores e integrantes do CMB
Deve ser uma solução com ampla adoção nas escolas e faculdades de instituições públicas e privadas.	Solução inovadora, com suporte e garantia.

6. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

6.1 Para a elaboração deste processo, os recursos necessários foram estruturados em serviços, conforme detalhado na tabela abaixo:

	ITEM	DESCRIÇÃO	QTDE
	01	PONTOS DE ACESSO PARA REDE SEM FIO (INDOOR)	60
	02	PONTOS DE ACESSO PARA REDE SEM FIO (OUTDOOR)	06
	03	FIREWALL PARA ALTA DISPONIBILIDADE	01
	04	SISTEMA DE ENERGIA ININTERRUPTA (UPS/NOBREAK) 2000VA	30
	05	SISTEMA DE ENERGIA ININTERRUPTA (UPS/NOBREAK) 20KVA	01
	06	SWITCH DE ACESSO L2+L3 48 PORTAS 10/100/1000BASE-T	10
	07	SWITCH 48 PORTAS FIBER COM 2 PORTAS UPLINK/STACK QSFP28	02
	08	ESTAÇÃO DE TRABALHO DO TIPO DESKTOP COMPACTO TIPO 1	30
	09	ESTAÇÃO DE TRABALHO DO TIPO DESKTOP COMPACTO TIPO 2	20
	10	NOTEBOOK	30
	11	CÂMERA DE VIDEOCONFERENCIA CORPORATIVA	05
GRUPO 1	12	PROCESSADOR / GERENCIADOR PARA MONITORES DE VIDEOWALL	01
	13	MONITOR PROFISSIONAL PARA VIDEOWALL	08
	14	SUPORTE PARA MONITOR PROFISSIONAL PARA VIDEOWALL	08
	15	PROJETOR 2800 LUMENS PADRÃO 21118	60
	16	PROJETOR 12000 LUMENS 4K UHD LASER	02
	17	ADAPTADOR DISPLAY PORT/HDMI	100

	18	ALICATE DE CRIMPAR	05
	19	UNIDADE DE DISCO EXTERNO 2TB	30
	20	MONITOR 24"	50
	21	PLACA DE VIDEO 1GB HDMI	50
	22	PLACA DE REDE PADRÃO PCI-EXPRESS	30
	23	MEMÓRIA RAM DDR3 8GB	30
	24	MEMÓIRA RAM DDR 4 8GBPO	30
	25	ÁLCOOL ISOPROPÍLICO	10
	26	LICENÇA OFFICE	50

7. LEVANTAMENTO DE SOLUÇÕES

7.1 Identificação das Soluções

7.1.1 A primeira tabela descreve soluções em relação a aquisição dos pontos de acesso e firewall (itens do grupo 1) visto que se trata de uma expansão e a mesma deve ser comparada a atuais tecnologias de mercado.

7.1.2 Para esse projeto foram consideradas quatro soluções para os equipamentos de pontos de acesso, são elas:

Nº	SOLUÇÃO
1	Adquirir novos pontos de acesso que não tenham as funcionalidades capture ATP, Serviço de Filtragem de Conteúdo, Política de Segurança por ACL, Geo-IP e Controle de Aplicativo. Neste caso todos os dados passam a ser centralizados e tratados no firewall central.
2	Adquirir novos pontos de acesso com a mesma compatibilidade dos pontos de acessos que estão instalados e que estão dentro da garantia e suporte. A compatibilidade relevante é que os novos pontos de acesso sejam integrados na controladora atual ou que a empresa contratada, para os novos pontos de acesso, tenha uma controladora que integre os pontos de acessos existentes.
3	Adquirir outros pontos de acesso que tenham as funcionalidades capture ATP, Serviço de Filtragem de Conteúdo, Política de Segurança por ACL, Geo-IP e Controle de Aplicativo, que possam substituir todos os pontos de acesso existentes dentro do custo previsto para esse projeto.
4	Ampliar os pontos de acesso atuais com as mesmas características já implantadas tentando manter a marca já comprada pelo CMB. Também ampliar os pontos de acesso com outra marca, porém prevendo o custo de troca de todos os pontos de acesso já instalados sem onerar para o CMB.

7.1.3 A próxima tabela descreve soluções em relação ao sistema de energia ininterrupta, switches, computadores, notebooks, solução de videowall e câmera de vídeo conferência (itens de 4 até 16).

Nº	SOLUÇÃO
1	Adquirir novos equipamentos
2	Realizar a manutenção dos equipamentos existentes.
3	Alugar os equipamentos solicitados.

8. ANÁLISE COMPARATIVA DAS SOLUÇÕES

8.1 Para os pontos de acesso e firewall (itens 1 e 2 da tabela 3 deste documento) segue tabela com análise comparativa.

Requisito	Solução	Sim	Não	Não se Aplic
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
	Solução 4	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
	Solução 4	X		
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1		X	
	Solução 2		X	
	Solução 3	X		
	Solução 4	X		
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X

8.2 Para os sistemas de energia ininterrupta, switches, computadores, notebooks, solução de videowall e câmera de vídeo conferência segue tabela abaixo:

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
	Solução 3		X	
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1	X		
	Solução 2		X	
	Solução 3		X	
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X

8.3 Os demais itens (do 17 ao 26) não necessitam de comparações de solução visto que serão aquisições e complemento da estrutura já instalada no CMB.

8.4 Análise Comparativa de Custos das Soluções Funcionalmente e Tecnicamente Viáveis (Art. 11, Inciso III da IN nº 94 de 23 de dezembro de 2022/SGD-ME)

8.4.1 O mapa comparativo de preços utilizou o critério aplicado do valor médio apurado, para obter o preço de referência, em conformidade com os critérios preconizados pelo Art. 20 da Instrução Normativa nº 94, de 23 de abril de 2022, da Secretaria de Governo Digital do Ministério da Economia (SEI nº 7879960), combinada com a IN nº 05/2014, alterada pela IN nº 03/2017.

8.4.2 Os preços médios obtidos para cada item foram baseados em informações prestadas por fornecedores, conforme o inciso IV, Art. 2º, IN nº 05/2014 e alterações IN nº 03/2017 (pesquisa com os fornecedores, desde que as datas das pesquisas não se diferenciem em mais de 180 (cento e oitenta) dias.

8.4.3 A pesquisa de preços empreendida obedece, portanto, os critérios priorizados tanto pela IN nº 94/2022 SGD/ME quanto pela IN nº 05/2014, alterada pela IN nº 03/2017, refletindo a realidade encontrada em contratações similares e o valor médio de mercado obtida através de pesquisa de preços dos fornecedores, devido que o tipo de serviços requerido não consta nos painéis de preços públicos.

9. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

9.1 Para os pontos de acesso e firewall (itens 1 e 2 da tabela 3 deste documento) segue tabela com soluções consideradas inadequadas para esse processo.

Nº	SOLUÇÃO	IMPACTO
1	Adquirir novos pontos de acesso que não tenham as funcionalidades capture ATP, Serviço de Filtragem de Conteúdo, Política de Segurança por ACL, Geo-IP e Controle de Aplicativo. Neste caso todos os dados passam a ser centralizados e tratados no firewall central.	Para essa solução o CMB vai **involuir** no que já realizou em relação a segurança. A proposta é que o acesso tenha três camadas de segurança. A primeira camada nas máquinas com a instalação de um EDR (Endpoint Detection & Response). A segunda camada, que já existe, seria no próprio ponto de acesso e os switches. Por fim a terceira camada no firewall. Adotando essa solução, todo tráfego deverá ser tratado no firewall ficando apenas uma camada de segurança e um gargalo central no firewall da rede. A rede também teria que sofrer uma segmentação para access point que não são Sonicwall.
2	Adquirir novos pontos de acesso com a mesma compatibilidade dos pontos de acessos que estão instalados e que estão dentro da garantia e suporte. A compatibilidade relevante é que os novos pontos de acesso sejam integrados na controladora atual ou que a empresa contratada, para os novos pontos de acesso, tenha uma controladora que integre os pontos de acessos existentes.	Em pesquisa de mercado e consultando representantes de fornecedores como a Fortinet, Sophos e Sonicwall, não existe a possibilidade de integração entre as marcas. Ou seja, o CMB teria que trabalhar com duas plataformas de gerência para configurar, visualizar e manter os pontos de acesso. Ressalta-se que além dos access point seria necessário também a controladora, software para prover a segurança dos pontos já levantados, migração e treinamento.
3	Adquirir outros pontos de acesso que tenham as funcionalidades capture ATP, Serviço de Filtragem de Conteúdo, Política de Segurança por ACL, Geo-IP e Controle de Aplicativo, que possam substituir todos os pontos de acesso existentes dentro do custo previsto para esse projeto.	Em análise de mercado o projeto não vai ficar mais barato, visto que ao valor considerado na proposta deve-se somar o custo que o CMB já teve para solução atual, no valor aproximado de 260.000,00. Ressalta-se que além dos access point seria necessário também a controladora, software para prover a segurança dos pontos já levantados, migração e treinamento.

9.2 Para os sistemas de energia ininterrupta, switches, computadores, notebooks, solução de videowall, projetores multimídia e câmera de vídeo conferência duas soluções são consideradas inadequadas.

Nº	SOLUÇÃO	IMPACTO
2	Realizar a manutenção dos equipamentos existentes.	• Sistemas de Energia: para os equipamentos existentes no CMB as peças são caras e a mão de obra especializada em Brasília é

		restrita fazendo com que não tenha propostas de preços para comparação de mercado. • Para os casos de switches não existe mão de obra especializada que realize os serviços. As peças dos switches em sua maioria são importadas. • Computadores, Notebooks e projetores multimídia a seção de manutenção do CMB já realizam o serviço, mas essa modalidade não amplia o número de computadores que atualmente o CMB necessita. • Solução de videwall não existe no CMB atualmente e por isso essa modalidade não é compatível. • Câmera de videoconferência para salas de médio porte o CMB também não possui equipamento e, portanto, essa modalidade não é compatível.
3	Alugar os equipamentos solicitados.	• Para ambos os equipamentos a modalidade aluguel do valor da locação excede o custo do equipamento em 1 ou 2 anos, e a pretensão do CMB é comprar os equipamentos com garantia mínima de 03 anos; • Em comunicação com outros órgãos que já realizaram essa modalidade muitos alegam a falta de compromisso da contratada em algumas questões de reparo, visto que empresas vencedoras do certame nem sempre tem corpo técnico e ferramentas para solucionar os problemas críticos de equipamentos como nobreaks e swiches.

9.3 Os demais materiais complementares a solução (do item 17 ao 26) não impactam em relação a custo ou aos pontos de acesso já instalados no CMB, e desta forma, não fazem parte da análise de possíveis soluções para pontos de acesso, restando somente a solução de aquisição.

10. ANÁLISE COMPARATIVA DE CUSTOS

10.1 CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

10.1.1 Conforme demonstrado no item anterior, o primeiro cenário que é constituído pelos itens 1, 2 e 3 apresentou 04 (quatro) soluções possíveis sendo que as três primeiras se tornam inviáveis pelos impactos apresentados no documento, restando apenas a solução 4 como totalmente viável. Porém, será feita uma análise comparativa entre o cenário 2 e 4 para melhorar as questões de inviabilidade das outras soluções.

10.1.2 Será considerado o valor do pregão CREA-SC 25/2022 para hardware AP indoor e serviços. Os demais preços serão calculados pelo investimento realizado pelo CMB como o custo total de propriedade (TCO) da solução 2.

Solução Viável 2 - Adquirir novos pontos de acesso com a mesma compatibilidade dos pontos de acessos	
Descrição	• Adquirir novos pontos de acesso com a mesma compatibilidade dos pontos de acessos que estão instalados e que estão dentro da garantia e suporte. A compatibilidade relevante é que os novos pontos de acesso sejam integrados na controladora atual ou que a empresa contratada, para os novos pontos de acesso, tenha uma controladora que integre os pontos de acessos existentes
Custo Total de Propriedade	Serão sintetizados os procedimentos empregados para cálculo dos custos totais de propriedade (TCOs) dos cenários viáveis e, em seguida, apresentar a análise comparativa de custos. A seção de informática computou os seguintes custos dos produtos: • hardware • software • suporte • Treinamento • Absorção dos equipamentos legados

TCO SOLUÇÃO 2				
Elemento de Custo	**Qtde**	**Descrição**	**Valor**	**Valor Total do Item**
Custo da Solução	60	Hardware (AP indoor)	R$ 11.505,85	R$ 1.049.113,14
	06	Hardware (AP outdoor)	R$ 14.977,00	
	01	Hardware (Firewall)	R$ 58.367,40	
	66	Licenças (AP's)	R$ 3.189,89	
	01	Licenças (Firewall)	-	
Serviços	01	Suporte	-	30.750,00
	01	Treinamento	R$ 30.750,00	
Absorção dos equipamentos legados.	01	Configurar, garantir e realizar o suporte em relação a aquisição de outra tecnologia.	R$ 173.141,40	173.141,40
			TOTAL	**R$ 1.253.004,54**

Solução Viável 4 - Ampliar os pontos de acesso atuais com as mesmas características implantadas	
Descrição	• Ampliar os pontos de acesso atuais com as mesmas características já implantadas tentando manter a marca já comprada pelo CMB. Também ampliar os pontos de acesso com outra marca, porém prevendo o custo de troca de todos os pontos de acesso já instalados sem onerar para o CMB.
Custo Total de Propriedade	Serão sintetizados os procedimentos empregados para cálculo dos custos totais de propriedade (TCOs) dos cenários viáveis e, em seguida, apresentar a análise comparativa de custos. A seção de informática computou os seguintes custos dos produtos: • hardware • software • suporte • treinamento • instalação • absorção dos equipamentos legados

TCO CENÁRIO 04

Elemento de Custo	**Qtde**	**Descrição**	**Valor**	**Valor Total do Item**
Custo da Solução	60	Hardware (AP indoor)	R$ 10.434,00	R$ 774.269,00
	06	Hardware (AP outdoor)	R$ 14.977,00	
	01	Hardware (Firewall)	R$ 58.367,40	
	66	Licenças (AP's)	-	
	01	Licenças (Firewall)	-	
Serviços	01	Suporte	-	R$ 38.000,00
	01	Treinamento	R$ 38.000,00	
	01	Instalação	R$ 160.000,00	R$ 160.000,00
Absorção dos equipamentos legados.	01	Configurar, garantir e realizar o suporte em relação a aquisição de outra tecnologia.	-	0,00
			TOTAL	**R$ 972.269,00**

10.1.3 Para os sistemas de energia ininterrupta, switches, computadores, notebooks, solução de videowall, projetores multimídia e câmera de vídeo conferência foram apresentadas 03 (três) soluções na qual duas soluções são consideradas inadequadas.

10.1.4 Desta forma, não há como fazer comparação de custos em relação a soluções visto que somente uma solução é adequada. Ainda sim no relatório de pesquisa de preços serão elencados valores que possibilitem comparar custos para essas soluções.

10.1.5 Para essa estimativa deve ser considerado que as aquisições serão realizadas com garantia de 03 (três) anos de garantia. Desta forma, esses custos representam apenas serviços que não estão cobertos pela garantia, como por exemplo mudança de localidade dos equipamentos, configurações básicas local entre outros.

10.1.6 Demais detalhes estarão demonstrados no mapa comparativo de preço e no relatório de pesquisa de preços.

10.2 CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

10.2.1 O cálculo foi realizado apenas para o primeiro cenário que é constituído pelos itens 1, 2 e 3 apresentou 04 (quatro) soluções possíveis sendo que as três primeiras se tornam inviáveis. Porém, será feita o cálculo do cenário 2 e 4 para ilustrar os custos totais de propriedade.

Descrição da solução	Estimativa de TCO ao longo dos anos			Total
	Ano 1	Ano 2	Ano 3	
Solução Viável 2	1.253.004,54	76.508,00	63.978,00	**1.393.490,00**
Solução Viável 4	972.269,00	14.584,03	4.861,34	**991.714,37**

10.2.2 Os valores foram alcançados com a soma de índices de 0,5% até 1,5% considerando fatores de novos treinamentos, problemas ocasionados não previstos na garantia, suporte de reconfiguração entre outros. Para solução 2 além dos índices foi somando o valor de aproximadamente R$ 58.000,00 referente a suporte e garantia do legado que para solução 4 não faz efeito visto que a proposta da solução é continuar com o legado com total interoperabilidade com a nova aquisição.

11. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

11.1. PONTOS DE ACESSO PARA REDE SEM FIO INDOOR

11.1.1 Deverá ser compatível com a solução wireless sonicwave 231c de forma que possa integrar com esta solução;

11.1.2 Possuir estrutura que permita a utilização do equipamento em locais internos, com fixação em teto;

11.1.3 Esse equipamento deve possuir total integração com o firewall TZ670, que está configurado e integrado com a controladora de rede Wireless dos Ap's, sendo gerenciado por uma única console de gerência;

11.1.4 Deverá acompanhar kit para fixação do Access point nas paredes ou teto;

11.1.5 Operar simultaneamente nas frequências de 2.4GHz e 5GHz, com rádios distintos;
11.1.6 Permitir a criação de – no mínimo – 8 SSID's – para cada rádio;
11.1.7 Permitir a configuração de Hidden SSID's (SSID's ocultos);
11.1.8 Suportar os padrões IEEE 802.11 a/b/g/n/ac/ac;
11.1.9 Deverá suportar os padrões IEEE 802.11r (fast transition), IEEE 802.11k, IEEE 802.11v;
11.1.10 Operar com tecnologia do tipo "MIMO (Multiple Input/Multiple Output)" do tipo "multi-user", MU-MIMO;
11.1.11 Deverá possuir mecanismo de rádio com suporte à MU-MIMO 4x4 em frequência 2.4Ghz e 8x8 em frequência 5.0Ghz;
11.1.12 Suportar no mínimo 128 usuários conectados por rádio;
11.1.13 Possuir antenas internas e integradas com padrão de irradiação omni-direcional;
11.1.14 Compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax;
11.1.15 Implementar, pelo menos, os seguintes padrões de segurança wireless:
11.1.15.1 Wi-Fi Protected Access (WPA) com algoritmo de criptografia TKIP (Temporal Key Integrity Protocol);
11.1.15.2 Suportar padrão de criptografia WPA2 Personal e WPA2 Enterprise;
11.1.15.3 Wi-Fi Protected Access 3 (WPA3) com os seguintes algoritmos, Advanced Encryption Standard (WPA3-AES) e IEEE 802.11i.
11.1.16 Deverá suportar Beamforming;
11.1.17 Possuir capacidade de selecionar automaticamente o canal de transmissão;
11.1.18 O equipamento deve ser capaz de implementar 802.11 Dynamic Frequency Selection (DFS);
11.1.19 A solução wireless deve implementar mecanismo que permita às estações se conectarem ao rádio com melhor throughput, ao invés do rádio com melhor sinal, através do padrão RRM (Radio Resource Management) IEEE 802.11k ou similar, evitando sobrecarga nos Pontos de Acesso;
11.1.20 Deverá ser fornecido com todas as licenças para funcionamento em MESH (WiFi Mesh);
11.1.21 Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5 GHz, deixando a banda de 2,4 GHz livre para dispositivos que trabalhem somente nesta frequência;
11.1.22 Possuir tecnologia "Airtime Fairness" permitindo melhor desempenho da rede wireless;
11.1.23 Permitir alimentação elétrica por meio de Power Over Ethernet (PoE), padrão 802.3at;
11.1.24 Alternativamente, a CONTRATADA poderá fornecer um switch com alimentação PoE e com quantidade de portas suficientes para conectar e alimentar eletricamente os equipamentos AP objeto deste Edital;
11.1.25 Possuir capacidade de selecionar dinamicamente a frequência de operação (DFS);
11.1.26 Permitir o controle da potência de transmissão (Transmit Power Control - TPC);
11.1.27 Possuir radio dedicado para detectar ataques do tipo "Rogue AP", ou seja, detectar a existência em funcionamento de outros equipamentos AP cuja instalação/operação/sinal de rádio não tenha sido autorizado para uso;
11.1.28 Deve, juntamente com a solução de Controladora Wireless, detectar e gerar alarmes de interferências WiFi provenientes de dispositivos padrão IEEE 802.11;
11.1.29 Possuir funcionalidade de visualização de dispositivos conectados e histórico das conexões;
11.1.30 Permitir atualização de firmware através da controladora centralizada;
11.1.31 Possuir, no mínimo, 01 (uma) interface IEEE 802.3 10/100/1000 Mbps Base-T Ethernet, autosensing, com conector RJ-45, para conexão à rede local fixa;

11.1.32 Implementar cliente DHCP, para configuração automática do seu endereço IP;
11.1.33 Deve suportar VLAN seguindo a norma IEEE 802.1q;
11.1.34 Deverá ser apresentado certificado válido de interoperabilidade fornecido pela Wi-Fi Alliance na categoria de Enterprise Access Point;
11.1.35 Possuir LEDs para a indicação do status: portas ethernets, rede wireless, e atividades do equipamento;
11.1.36 Deve suportar temperatura de operação entre 0°C a 40°C;
11.1.37 Deve ser gerenciado pela controladora em nuvem da SonicWall que está instalada e configurada no CMB, a qual é responsável pelas seguintes funções na rede sem fio:
11.1.37.1 administração, configuração e gerenciamento completo centralizado dos pontos de acesso WiFi especificados;
11.1.37.2 funções de segurança para acesso;
11.1.37.3 funções de segurança para tráfego de dados e controle;
11.1.37.4 funções de gerenciamento de RF (Rádio Frequência); e
11.1.37.5 funções de gerenciamento de dispositivos de usuários;
11.1.38 A solução de Controladora Wireless em Nuvem não deve ter restrição de licença que limite o número de Ponto de Acesso a ser controlado por ela;
11.1.39 Deve disponibilizar uma Console de Gerenciamento Web acessível através de protocolo Criptografado, compatível com os principais browsers do mercado (Internet Explorer, Firefox e Chrome);
11.1.40 Deve permitir habilitar e desabilitar os SSID's;
11.1.41 Deve permitir realizar procedimentos de configuração, correção e aperfeiçoamento da cobertura e disponibilidade nos pontos de acesso;
11.1.42 Deve realizar o upgrade de softwares dos pontos de acesso WiFi;
11.1.43 Deve realizar otimização de radiofrequência, monitoramento e alertas
11.1.44 Deve permitir a criação de múltiplas redes distintas e segregadas, mas administradas na mesma console, permitindo assim a segmentação e agrupamento de Access Points que tenham objetivos comuns, permitindo uma melhor organização do ambiente de equipamentos administrados.
11.1.45 Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado no Access Point ou fornecido modulo adicional para essa funcionalidade;
11.1.46 Possuir base contendo, no mínimo, 20 milhões de sites internet web já registrados e classificados com atualização automática;
11.1.47 Deve atuar como filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração de proxy dos browsers das máquinas clientes.
11.1.48 A plataforma deve possuir as seguintes funcionalidades de filtro de URL:
11.1.49 Permitir a criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra);
11.1.50 Deverá permitir criar política de controle de URL por SSID ou faixa de endereço IP ou usuário;
11.1.51 Possuir pelo menos 50 categorias de URLs;
11.1.52 Suporta a exclusão ou inclusão de URLs do bloqueio, por categoria;
11.1.53 Deverá possibilitar a categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente, utilizando-se ferramenta do proprio fabricante;
11.1.54 A solução deverá permitir um mecanismo que permita sobrescrever as categorias de URL;
11.1.55 Deve possibilitar a criação de ACLs para bloquear ou permitir que dispositivos indesejados acessem a rede WIFI;

11.1.56 Deve permitir a visualização de um conjunto de informações dos Access Points que fazem parte da rede wireless, disponibilizando pelo menos as seguintes informações:

11.1.57 Relação dos Access Points conectados, disponibilizando no mínimo as informações de Nome, MAC Address, Modelo de equipamento e endereço IP;

11.1.58 Tempo de disponibilidade do Access Point, versão de firmware do Acces Point e quantidade de clientes conectados na frequência 5Ghz e 2.4 Ghz.

11.1.59 Localização dos Access Points com visualização em mapa mundi real e online.

11.1.60 Deve permitir a visualização de um conjunto de informações dos dispositivos conectados à rede wireless, disponibilizando pelo menos os dados abaixo especificados:

11.1.61 Endereço IP, MAC Address, Status, SSID;

11.1.62 Sistema Operacional do dispositivo utilizado;

11.1.63 Informação da frequência de conexão com a rede WiFi e Access Point utilizados;

11.1.64 Deve disponibilizar um formato de relatório sintético, com o resumo das principais informações estatísticas de utilização dos Access Point, como por exemplo: SSIDs mais usados, clientes com maior consumo de dados, tipos de dispositivos usados (Sistema Operacional), Top Access Points mais utilizados com consumo de dados, inventario da configuração dos Access Points, localização dos Access Points. Tal relatório ainda deve possibilitar ser enviado por e-mail, para o Administrador;

11.1.65 Deve possibilitar o agrupamento dos Access Point suportando a criação e o gerenciamento de grupos de Access Point simultâneos, permitindo assim criar nomenclaturas de organização como "Prédio Central", "Primeiro Andar" entre outros.

11.1.66 O serviço deverá prover solução de autenticação e registro de usuários, considerando captive portal com autenticação através de redes sociais, usuário local, página customizável de confirmação das políticas da empresa;

11.1.67 Deverá suportar o direcionamento do usuário para captive portal externo;

11.1.68 A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos, Zero-Day, do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real e inspeção de tráfego de saída de callbacks;

11.1.69 Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

11.1.70 Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real;

11.1.71 Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF;

11.1.72 Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android;

11.1.73 Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware;

11.1.74 A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas;

11.1.75 A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliance através de assinaturas;

11.1.76 Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;

11.1.77 Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

11.1.78 Conter ameaças avançadas de dia zero;

11.1.79 Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;
11.1.80 Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;
11.1.81 Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;
11.1.82 Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado;
11.1.83 Implementar a análise de arquivos executáveis, DLLs, ZIP no ambiente controlado;
11.1.84 Conter ameaças de dia zero de forma transparente para o usuário final;
11.1.85 Conter ameaças de dia zero através de tecnologias em nível de emulação e código de registro;
11.1.86 Implementar mecanismo de pesquisa por diferentes intervalos de tempo;
11.1.87 Conter ameaças de dia zero via tráfego de internet;
11.1.88 Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança;
11.1.89 Conter ameaças de dia zero que possam burlar o sistema operacional emulado;
11.1.90 A solução deve permitir a criação de White list baseado no MD5 do arquivo;
11.1.91 Conter ameaças de dia zero antes da execução e evasão de qualquer código malicioso;
11.1.92 Conter exploits avançados.
11.1.93 A análise "In Cloud" ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Antispyware automaticamente e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede);
11.1.94 Suporte a submissão manual de arquivos para análise através do serviço de Sandbox
11.1.95 Caso a solução não entregue a funcionalidade de sandbox, será aceito a composição de soluções;
11.1.96 Deverá possuir base de Geo-IP, com pelo menos 130 países já cadastrados para configuração de políticas de operação (bloqueio ou detecção);
11.1.97 Deve ter integrado ferramenta de análise de malware conhecido com capacidade de validar se os arquivos baixados pelos usuários são maliciosos ou não, utilizando -se de base de conhecimento "in-cloud" para tais validações.

11.2. PONTOS DE ACESSO PARA REDE SEM FIO OUTDOOR

11.2.1 Deverá ser compatível com a solução wireless da SONICWALL de foram que possa integrar com esta;
11.2.2 Deve possuir certificação IP67 para operar em ambiente externo;
11.2.3 Possuir estrutura que permita a utilização do equipamento em locais externos, com fixação em teto;
11.2.4 Esse equipamento deve possuir total integração com o firewall TZ670, que está configurado e integrado com a controladora de rede Wireless dos Ap's, sendo gerenciado por uma única console de gerência;
11.2.5 Deverá acompanhar kit para fixação do Access point nas paredes ou teto;
11.2.6 Operar simultaneamente nas frequências de 2.4GHz e 5GHz, com rádios distintos;
11.2.7 Permitir a criação de – no mínimo – 8 SSID's – para cada rádio;
11.2.8 Permitir a configuração de Hidden SSID's (SSID's ocultos);

11.2.9 Suportar os padrões IEEE 802.11 a/b/g/n/ac/ac;
11.2.10 Deverá suportar os padrões IEEE 802.11r (fast transition), IEEE 802.11k, IEEE 802.11v;
11.2.11 Operar com tecnologia do tipo "MIMO (Multiple Input/Multiple Output)" do tipo "multi-user", MU-MIMO;
11.2.12 Deverá possuir mecanismo de rádio com suporte à MU-MIMO 4x4;
11.2.13 Suportar no mínimo 128 usuários conectados por rádio;
11.2.14 Possuir antenas internas e integradas com padrão de irradiação omni-direcional;
11.2.15 Compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax;"
11.2.16 Implementar, pelo menos, os seguintes padrões de segurança wireless:
11.2.16.1 Wi-Fi Protected Access (WPA) com algoritmo de criptografia TKIP (Temporal Key Integrity Protocol);
11.2.17 Deverá suportar Beamforming;
11.2.18 Possuir capacidade de selecionar automaticamente o canal de transmissão;
11.2.19 O equipamento deve ser capaz de implementar 802.11 Dynamic Frequency Selection (DFS);
11.2.20 A solução wireless deve implementar mecanismo que permita às estações se conectarem ao rádio com melhor throughput, ao invés do rádio com melhor sinal, através do padrão RRM (Radio Resource Management) IEEE 802.11k ou similar, evitando sobrecarga nos Pontos de Acesso;
11.2.21 Deverá ser fornecido com todas as licenças para funcionamento em MESH (WiFi Mesh);
11.2.22 Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5 GHz, deixando a banda de 2,4 GHz livre para dispositivos que trabalhem somente nesta frequência;
11.2.23 Possuir tecnologia "Airtime Fairness" permitindo melhor desempenho da rede wireless;
11.2.24 Permitir alimentação elétrica por meio de Power Over Ethernet (PoE), padrão 802.3at;
11.2.25 Alternativamente, a CONTRATADA poderá fornecer um switch com alimentação PoE e com quantidade de portas suficientes para conectar e alimentar eletricamente os equipamentos AP objeto deste Edital;
11.2.26 Possuir capacidade de selecionar dinamicamente a frequência de operação (DFS);
11.2.27 Permitir o controle da potência de transmissão (Transmit Power Control - TPC);
11.2.28 Suportar padrão de criptografia WPA2 Personal e WPA2 Enterprise;
11.2.29 Possuir radio dedicado para detectar ataques do tipo "Rogue AP", ou seja, detectar a existência em funcionamento de outros equipamentos AP cuja instalação/operação/sinal de rádio não tenha sido autorizado para uso;
11.2.30 Deve, juntamente com a solução de Controladora Wireless, detectar e gerar alarmes de interferências WiFi provenientes de dispositivos padrão IEEE 802.11;
11.2.31 Possuir funcionalidade de visualização de dispositivos conectados e histórico das conexões;
11.2.32 Permitir atualização de firmware através da controladora centralizada;
11.2.33 Possuir, no mínimo, 01 (uma) interface IEEE 802.3 10/100/1000 Mbps Base-T Ethernet, autosensing, com conector RJ-45, para conexão à rede local fixa;
11.2.34 Possuir, no mínimo, 01 (uma) interface IEEE 802.3 100/1000/2.500 Mbps Ethernet, autosensing, com conector RJ-45, para conexão à rede local fixa;
11.2.35 Possuir, no mínimo, 01 (uma) interface do tipo console;
11.2.36 Possuir interface USB dedicada para conexão de modens 3G/4G permitindo configurar uma saida de internet por esta conexão.
11.2.37 Implementar cliente DHCP, para configuração automática do seu endereço IP;

11.2.38 Deve suportar VLAN seguindo a norma IEEE 802.1q;
11.2.39 Deverá ser apresentado certificado válido de interoperabilidade fornecido pela Wi-Fi Alliance na categoria de Enterprise Access Point;
11.2.40 Possuir LEDs para a indicação do status: portas ethernets, rede wireless, e atividades do equipamento;
11.2.41 Deve suportar temperatura de operação entre 0°C a 40°C;
11.2.42 Deve ser gerenciado pela controladora em nuvem da SonicWall que está instalada e configurada no CMB, a qual é responsável pelas seguintes funções na rede sem fio:
11.2.42.1 administração, configuração e gerenciamento completo centralizado dos pontos de acesso WiFi especificados;
11.2.42.2 funções de segurança para acesso;
11.2.42.3 funções de segurança para tráfego de dados e controle;
11.2.42.4 funções de gerenciamento de RF (Rádio Frequência); e
11.2.42.5 funções de gerenciamento de dispositivos de usuários;
11.2.43 A solução de Controladora Wireless em Nuvem não deve ter restrição de licença que limite o número de Ponto de Acesso a ser controlado por ela;
11.2.44 Deve disponibilizar uma Console de Gerenciamento Web acessível através de protocolo Criptografado, compatível com os principais browsers do mercado (Internet Explorer, Firefox e Chrome);
11.2.45 Deve permitir habilitar e desabilitar os SSID's;
11.2.46 Deve permitir realizar procedimentos de configuração, correção e aperfeiçoamento da cobertura e disponibilidade nos pontos de acesso;
11.2.47 Deve realizar o upgrade de softwares dos pontos de acesso WiFi;
11.2.48 Deve realizar otimização de radiofrequência, monitoramento e alertas
11.2.49 Deve permitir a criação de múltiplas redes distintas e segregadas, mas administradas na mesma console, permitindo assim a segmentação e agrupamento de Access Points que tenham objetivos comuns, permitindo uma melhor organização do ambiente de equipamentos administrados.
11.2.50 Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado no Access Point ou fornecido modulo adicional para essa funcionalidade;
11.2.51 Possuir base contendo, no mínimo, 20 milhões de sites internet web já registrados e classificados com atualização automática;
11.2.52 Deve atuar como filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração de proxy dos browsers das máquinas clientes.
11.2.53 A plataforma deve possuir as seguintes funcionalidades de filtro de URL:
11.2.54 Permitir a criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra);
11.2.55 Deverá permitir criar política de controle de URL por SSID ou faixa de endereço IP ou usuário;
11.2.56 Possuir pelo menos 50 categorias de URLs;
11.2.57 Suporta a exclusão ou inclusão de URLs do bloqueio, por categoria;
11.2.58 Deverá possibilitar a categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente, utilizando-se ferramenta do próprio fabricante;
11.2.59 A solução deverá permitir um mecanismo que permita sobrescrever as categorias de URL;
11.2.60 Deve possibilitar a criação de ACLs para bloquear ou permitir que dispositivos indesejados acessem a rede WIFI;

11.2.61 Deve permitir a visualização de um conjunto de informações dos Access Points que fazem parte da rede wireless, disponibilizando pelo menos as seguintes informações:

11.2.62 Relação dos Access Points conectados, disponibilizando no mínimo as informações de Nome, MAC Address, Modelo de equipamento e endereço IP;

11.2.63 Tempo de disponibilidade do Access Point, versão de firmware do Acces Point e quantidade de clientes conectados na frequência 5Ghz e 2.4 Ghz.

11.2.64 Localização dos Access Points com visualização em mapa mundi real e online.

11.2.65 Deve permitir a visualização de um conjunto de informações dos dispositivos conectados à rede wireless, disponibilizando pelo menos os dados abaixo especificados:

11.2.66 Endereço IP, MAC Address, Status, SSID;

11.2.67 Sistema Operacional do dispositivo utilizado;

11.2.68 Informação da frequência de conexão com a rede WiFi e Access Point utilizados;

11.2.69 Deve disponibilizar um formato de relatório sintético, com o resumo das principais informações estatísticas de utilização dos Access Point, como por exemplo: SSIDs mais usados, clientes com maior consumo de dados, tipos de dispositivos usados (Sistema Operacional), Top Access Points mais utilizados com consumo de dados, inventario da configuração dos Access Points, localização dos Access Points. Tal relatório ainda deve possibilitar ser enviado por e-mail, para o Administrador;

11.2.70 Deve possibilitar o agrupamento dos Access Point suportando a criação e o gerenciamento de grupos de Access Point simultâneos, permitindo assim criar nomenclaturas de organização como "Prédio Central", "Primeiro Andar" entre outros.

11.2.71 O serviço deverá prover solução de autenticação e registro de usuários, considerando captive portal com autenticação através de redes sociais, usuário local, página customizável de confirmação das políticas da empresa.

11.2.72 Deverá suportar o direcionamento do usuário para captive portal externo;

11.2.73 A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos, Zero-Day, do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real e inspeção de tráfego de saída de callbacks;

11.2.74 Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

11.2.75 Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real;

11.2.76 Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF;

11.2.77 Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android;

11.2.78 Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware;

11.2.79 A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas;

11.2.80 A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliance através de assinaturas.

11.2.81 Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;

11.2.82 Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

11.2.83 Conter ameaças avançadas de dia zero;

11.2.84 Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;

11.2.85 Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;

11.2.86 Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

11.2.87 Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado;

11.2.88 Implementar a análise de arquivos executáveis, DLLs, ZIP no ambiente controlado;

11.2.89 Conter ameaças de dia zero de forma transparente para o usuário final;

11.2.90 Conter ameaças de dia zero através de tecnologias em nível de emulação e código de registro;

11.2.91 Implementar mecanismo de pesquisa por diferentes intervalos de tempo;

11.2.92 Conter ameaças de dia zero via tráfego de internet;

11.2.93 Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança;

11.2.94 Conter ameaças de dia zero que possam burlar o sistema operacional emulado;

11.2.95 A solução deve permitir a criação de White list baseado no MD5 do arquivo;

11.2.96 Conter ameaças de dia zero antes da execução e evasão de qualquer código malicioso;

11.2.97 Conter exploits avançados.

11.2.98 A análise "In Cloud" ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Antispyware automaticamente e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede);

11.2.99 Suporte a submissão manual de arquivos para análise através do serviço de Sandbox

11.2.100 Caso a solução não entregue a funcionalidade de sandbox, será aceito a composição de soluções;

11.2.101 Deverá possuir base de Geo-IP, com pelo menos 130 países já cadastrados para configuração de políticas de operação (bloqueio ou detecção).

11.2.102 Deve ter integrado ferramenta de análise de malware conhecido com capacidade de validar se os arquivos baixados pelos usuários são maliciosos ou não, utilizando -se de base de conhecimento "in-cloud" para tais validações.

11.3. FIREWALL PARA ALTA DISPONIBILIDADE

11.3.1 Deverá possuir as seguintes características:

11.3.2 Ser compatível com a solução de segurança existente e implementada no CMB da SonicWall de forma que a solução seja gerenciada por uma única console de gerenciamento e realize a redundância com o equipamento TZ670 adquirido;

11.3.3 A Performance de todos os serviços ativos de Threat Prevention, (Proteção Anti-Malware e Anti-virus, IDS, IPS e Controle de Aplicação) deverá ser de 1.5 Gbps ou superior. Caso o fornecedor não possa comprovar este item em documentações públicas, deve ser comprovado através de testes em bancada com gerador de pacotes (custos destes testes pagos pela CONTRATADA);

11.3.4 A Performance de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL) de no mínimo 290 Mbps;

11.3.5 Performance de IPS de 1.4 Gbps ou superior;

11.3.6 Suporte a, no mínimo, 1.000.000 de conexões do tipo SPI simultâneas;

11.3.7 Suporte a, no mínimo, 14.000 novas conexões por segundo;

11.3.8 Disco interno SSD para armazenamento de no mínimo 16 Gb;

11.3.9 Deve suportar fonte de alimentação interna redundante com chaveamento automático de 100-240 VAC;

11.3.10 Deverá possuir 4 interfaces de 1 GbE SFP;

11.3.11 Possuir 12 interfaces de rede 10/100/1000 base-TX. Todas as interfaces devem possuir mecanismo de autosense e seleção de modo half/full duplex. A seleção da velocidade e duplex deve ser realizada obrigatoriamente através da interface gráfica de gerenciamento. As interfaces devem suportar as seguintes atribuições:

11.3.11.1 Segmento WAN, ou externo;

11.3.11.2 Segmento WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação. O equipamento deverá suportar no mínimo balanceamento de 4 links utilizando diferentes métricas pré-definidas pelo sistema e configuráveis pelo administrador;

11.3.11.3 Segmento LAN ou rede interna;

11.3.11.4 Segmento LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada);

11.3.11.5 Segmento LAN ou rede interna ou Porta de sincronismo para funcionamento em alta disponibilidade;

11.3.11.6 Segmento ou Zona exclusiva para controle de dispositivos Wireless dedicado, com controle e configuração destes dispositivos;

11.3.12 01 (uma) interface do tipo console ou similar;

11.3.13 01 (uma) interface de rede dedicada para gerenciamento;

11.3.14 A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 50 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para no mínimo, 1000 usuários simultâneos, com aquisição de licença futura;

11.3.15 A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para no mínimo, 500 usuários simultâneos, com aquisição de licença futura;

11.3.16 Suportar 1000 túneis de VPN IPSEC simultâneos;

11.3.17 Suportar, no mínimo, 1.40 Gbps de throughput de VPN IPSEC;

11.3.18 Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e/ou end-of-sale ou situação semelhante;

11.3.19 Todas as funcionalidades descritas devem funcionar no mesmo appliance sem a necessidade de composição de um ou mais produtos;

11.3.20 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

11.3.21 O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

11.3.22 O equipamento deverá ser baseado em hardware desenvolvido com está finalidade, ou seja, não sendo aceita soluções baseadas em plataforma PC ou equivalente;

11.3.23 Não serão permitidas soluções baseadas em sistemas operacionais abertos (OpenSource) como Free BSD, Debian ou mesmo Linux;

11.3.24 Todo o ambiente deverá ser gerenciado através de uma única interface;

11.3.25 Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos;

11.3.26 A solução deverá suportar monitoramento através de SNMP v2 e v3;

11.3.27 Deve oferecer as funcionalidades de backup/restore tanto da configuração quanto do firmware/sistema operacional através da interface gráfica, assim como permitir ao administrador agendar procedimentos de backups da configuração em determinado dia e hora. O appliance deve armazenar no mínimo 02 (duas) versões distintas do sistema operacional, sendo possível escolher qual versão será inicializada, de backups da configuração em determinado dia e hora;

11.3.28 Suporte a definição de VLAN no firewall, conforme padrão IEEE 802.1q e ser possível criar sub-interfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas;

11.3.29 A solução deve suportar configuração de link-aggregation de interfaces suportando o protocolo 802.3ad para aumento de throughput;

11.3.30 A solução deve suportar configuração de port-redundacy de interfaces para a alta disponibilidade de interfaces;

11.3.31 Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea mediante o uso de suas interfaces físicas nos seguintes modos:

11.3.31.1 Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);

11.3.31.2 Modo sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

11.3.31.3 Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

11.3.31.4 Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;

11.3.31.5 Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

11.3.32 Possuir DHCP Server interno;

11.3.33 Suporte a encaminhamento de pacotes UDPs multicast/broadcast entre diferentes interfaces e zonas de segurança como DHCP Relay, suportando os protocolos e portas:

11.3.33.1 Time service—UDP porta 37;

11.3.33.2 DNS—UDP porta 53;

11.3.33.3 DHCP—UDP portas 67 e 68;

11.3.33.4 Net-Bios DNS—UDP porta 137;

11.3.33.5 Net-Bios Datagram—UDP porta 138;

11.3.33.6 Wake On LAN—UDP porta 7 e 9;

11.3.33.7 mDNS—UDP porta 5353;

11.3.33.8 Suporte a Jumbo Frames;

11.3.33.9 Implementar sub-interfaces ethernet lógicas;

11.3.34 Deve suportar os seguintes tipos de NAT:

11.3.34.1 Nat dinâmico (Many-to-1);

11.3.34.2 Nat dinâmico (Many-to-Many);

11.3.34.3 Nat estático (1-to-1);

11.3.34.4 NAT estático (Many-to-Many);

11.3.34.5 Nat estático bidirecional 1-to-1;

11.3.34.6 Tradução de porta (PAT);

11.3.34.7 NAT de origem;
11.3.34.8 NAT de destino;
11.3.34.9 Suportar NAT de origem e NAT de destino simultaneamente.
11.3.35 Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing);
11.3.36 Implementar mecanismo de sincronismo de horário através do protocolo NTP;
11.3.37 Para tanto o appliance deve realizar a pesquisa em pelo menos 03 servidores NTP distintos, com a configuração do tempo do intervalo de pesquisa;
11.3.38 Possuir gerenciamento de tráfego de entrada ou saída, por serviços, endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida em porcentagem (%) para cada regra definida;
11.3.39 Implementar 802.1p e classe de serviços CoS (Class of Service) de DSCP (Differentiated Services Code Points);
11.3.40 Permitir remarcação de pacotes utilizando TOS e/ou DSCP;
11.3.41 Suporte a policy based routing (PBR), com a capacidade de roteamento por endereço de origem, endereço de destino, serviço, interface ou todas as opções simultâneas;
11.3.42 Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP;
11.3.43 Suportar Equal Cost Multi-Path (ECMP);
11.3.44 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
11.3.45 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3, RIPng);
11.3.46 A solução deve suportar integralmente o padrão IPv6, assim como criação de regras com objetos que utilizem endereços IPv4 e IPv6;
11.3.47 Deve suportar no mínimo as seguintes funcionalidades ou protocolos para o padrão de endereçamento IPv6: Tunel 6 to 4, regras de acesso, objetos de endereço, limitador de conexões IPv6, monitor de conexões, DHCP, gerenciamento HTTPS via IPv6, NAT IPv6, proteção contra ataques to tipo IP Spoofing para IPv6, captura de pacotes IPv6, interface VLAN com endereço IPv6, VPN SSL com o uso do IPv6, controle de URL, Anti-Malware e anti-virus, controle de aplicação, IPS, IKEv2, ICMP6, SNMP, alta disponibilidade, RFC 1981 Path MTU Discovery for IPv6, RFC 2460 IPv6 specification, RFC 2464 Transmission of IPv6 Packets over Ethernet Networks;
11.3.48 Possui suporte a log via syslog;
11.3.49 Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;
11.3.50 Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall;
11.3.51 Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;
11.3.52 Permitir a visualização de estatísticas do uso de CPU do appliance o através da interface gráfica remota em tempo real;
11.3.53 A solução deverá suportar a tecnologia de SD-WAN e deverá ter no mínimo as seguintes funcionalidades:
11.3.53.1 Suportar e implementar QoS com classificação, marcação e priorização de tráfego com base em endereço IP de origem/destino, portas TCP/UDP de origem e destino, DSCP (Differentiated Services Code Point), tipo de aplicação camada 7 e traffic shaping nas interfaces;
11.3.53.2 Capacidade de realizar a saída local de internet para alguns tráfegos selecionados a partir, no mínimo, dos parâmetros de IP, porta e URL;

11.3.54 Controle de caminho automático baseado em políticas, com habilidade de selecionar o caminho, no mínimo, através dos seguintes parâmetros simultâneos ou não:

11.3.54.1 tipo de aplicação;

11.3.54.2 prioridade de negócio;

11.3.54.3 latência;

11.3.54.4 jitter;

11.3.54.5 perda de pacotes.

11.3.55 A comutação dos caminhos deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas;

11.3.56 Permitir a alteração da política de encaminhamento sem impacto no tráfego;

11.3.57 Implementar tecnologia de reconhecimento de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, como também subaplicações associadas como Facebook Messenger e Office 365 Outlook;

11.3.58 A solução deve ser entregue operando em alta disponibilidade no modo Ativo/Standby, com as implementações de Failover;

11.3.59 Não serão permitidas soluções de cluster (HA) que façam com que o equipamento (s) reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador;

11.3.60 A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster;

11.3.61 A solução deve operar em alta disponibilidade implementando monitoramento logico de um host na rede, para verificar a existência de problemas lógicos na rede e possibilitar failover;

11.3.62 A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover;

11.3.63 A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster, incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança;

11.3.64 A solução deve permitir visualizar no equipamento principal, o status da comunicação entre o peers do cluster, status de sincronização das configurações, status atual equipamento backup;

11.3.65 Criptografia 3DES, AES 128 e AES 256;

11.3.66 Autenticação com MD5, SHA-1, SHA-256 e SHA-384;

11.3.67 Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits;

11.3.68 Algoritmo Internet Key Exchange (IKE);

11.3.69 Autenticação via certificado IKE PKI;

11.3.70 Deve possuir interoperabilidade com outros fabricantes de acordo com o padrão IPSEC através de RFC's;

11.3.71 A solução deve suportar VPNs L2TP, incluindo suporte para iPhone, Windows phone, Android com suporte a cliente L2TP;

11.3.72 Solução deve suportar VPNs baseadas em políticas e VPNs baseadas em roteamento estático e dinâmico;

11.3.73 Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;

11.3.74 Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos;

11.3.75 Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário;

11.3.76 Permitir que seja criado políticas de roteamentos estáticos utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego sendo este visto pela regra de roteamento, como uma interface simples de rede para encaminhamento do tráfego;

11.3.77 Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;

11.3.78 Permitir a utilização de LDAP, AD e RADIUS;

11.3.79 Permitir o cadastro manual dos usuários e grupos diretamente na interface de gerência remota do Firewall, caso em que se dispensa um autenticador remoto para o mesmo;

11.3.80 Suporte a uma rede com múltiplos domínios, possibilitando a integração em um ambiente onde existas domínios diferentes e totalmente segregados;

11.3.81 Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo firewall via protocolos HTTP e LDAP;

11.3.82 Permitir o controle de acesso por usuário, para plataformas Windows Me, NT, 2000, 2000, XP, Windows 7, Windows 8 e Windows 10 de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado;

11.3.83 Permitir a restrição de atribuição de perfil de acesso à usuário ou grupo independente ao endereço IP da máquina que o usuário esteja utilizando;

11.3.84 Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente através de regras no Firewall DPI (Deep Packet Inspection) sem a necessidade de uma nova autenticação como por exemplo, para os serviços de navegação a Internet atuando assim de forma toda transparente ao usuário. Serviços como HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores 2008/2012 com AD;

11.3.85 Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance de firewall, onde sua console de gerência deverá residir na mesma console centralizada dos appliances de segurança, com suporte a pelo menos 3.000 assinaturas;

11.3.86 A solução de IPS deverá possuir os seguintes mecanismos de detecção: assinaturas e trabalhar em conjunto com o controle de aplicações;

11.3.87 A solução de IPS deve fazer a inspeção de todo o pacote, independentemente do tamanho;

11.3.88 A solução de IPS deve fazer a inspeção de todo o tráfego de forma bidirecional, analisando qualquer tamanho de pacote sem degradar a performance do equipamento solicitada neste edital;

11.3.89 Possuir capacidade de remontagem de pacotes para identificação de ataques;

11.3.90 O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

11.3.91 Para cada proteção de segurança, deve ser possível consultar informações no site do fabricante;

11.3.92 A ferramenta de log deve possuir a capacidade de criar uma regra de exceção a partir do log visualizado na gerência centralizada;

11.3.93 As regras de exceção devem possuir: origem, destino e serviço;

11.3.94 A solução deve ser capaz de inspecionar tráfego HTTPS;

11.3.95 Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

11.3.96 Detecção de anomalias;

11.3.97 A solução de IPS deve possuir política capaz de definir o modo de operação (bloqueio ou detecção);

11.3.98 O módulo de IPS deve possuir assinaturas voltadas para ambientes de servidores de SMTP, Web e DNS;

11.3.99 O mecanismo de inspeção deve receber e implementar em tempo real atualizações de novas assinaturas sem a necessidade de reiniciar o appliance;

11.3.100 Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na origem e destino;

11.3.101 A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de e-mail, DNS, FTP, SQL Injection, ataques a sistemas operacionais e VOIP;

11.3.102 Deve incluir proteção contra worms;

11.3.103 Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades e a evolução ao logo do tempo dispondo o sumario quantitativo das ameaças analisadas;

11.3.104 A solução deve possuir esquema de atualização de assinaturas através de um click;

11.3.105 Atualização de modo offline, onde poder ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução;

11.3.106 A solução deve suportar importar certificados de servidor para inspeções de tráfego seguro HTTP (HTTPS) de entrada. Depois de importar esses certificados, a solução deve permitir o IPS para Inspeção segura HTTP(HTTPS);

11.3.107 A solução deverá ser capaz de inspecionar e proteger apenas hosts internos;

11.3.108 A solução deverá possuir proteções para sistemas SCADA;

11.3.109 Solução deverá permitir que o administrador bloqueie facilmente o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os ranges de endereços IP dos países que deseja bloquear;

11.3.110 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades abaixo:

11.3.111 Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

11.3.112 Capacidade para realizar filtragens/inspeções dentro de portas TCP conhecidas por exemplo porta 80 http, buscando por aplicações que potencialmente expõe o ambiente como: P2P, Kazaa, Morpheus, BitTorrent ou messengers;

11.3.113 Controlar o uso dos serviços de Instant Messengers como MSN, YAHOO, Google Talk, ICQ, de acordo com o perfil de cada usuário ou grupo de usuários, de modo a definir, para cada perfil, se ele pode ou não realizar download e/ou upload de arquivos.

limitar as extensões dos arquivos que podem ser enviados/recebidos e permissões e bloqueio de sua utilização baseados em horários pré-determinados pelo administrador será obrigatório para este item;

11.3.114 Deverá controlar software FreeProxy tais como ToR, Ultrasurf, Freegate etc.;

11.3.115 Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

11.3.116 Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;

11.3.117 Atualizar a base de assinaturas de aplicações automaticamente;

11.3.118 Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;

11.3.119 A solução de controle de aplicação WEB deve criar regras granulares possibilitando adicionar tipos de aplicação WEB e categorias por regra, sendo assim criando controle granular de qualquer tipo de acesso não permitido pela empresa;

11.3.120 Deve implementar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e protocolos;

11.3.121 Caso a solução não tenha assinaturas pré-definida na solução a mesma deverá possibilitar a criação ou importação de assinaturas personalizadas para os seguintes tipos ou protocolos: HTTP, FTP, Email e extensão de arquivos;

11.3.122 O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados a partir de comandos FTP pré-definidos;

11.3.123 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

11.3.124 Deverá possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, uTorrent, etc.) possuindo granularidade de controle/políticas para os mesmos;

11.3.125 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Facebook e bloquear chat;

11.3.126 Deverá possibilitar a diferenciação de aplicações Proxies possuindo granularidade de controle/políticas para os mesmos;

11.3.127 Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

- 11.3.127.1 Nível de risco da aplicação.
- 11.3.127.2 Categoria de aplicações.
- 11.3.127.3 Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado no firewall;
- 11.3.127.4 Possuir base contendo no mínimo 20 milhões de sites internet web já registrados e classificados com atualização automática;
- 11.3.127.5 Implementar filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.
- 11.3.127.6 A plataforma de proteção deve possuir as seguintes funcionalidades de filtro de URL:
- 11.3.127.7 Permitir a criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra) ;
- 11.3.127.8 Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 11.3.127.9 Deve ser possível à criação de políticas por usuários, grupos de usuários, IPs, redes e grupos de redes;

11.3.127.10 O mecanismo de Controle de aplicação Web/URL deve apresentar contagem de utilização de regra de acordo com a utilização (hit count);

11.3.127.11 Deverá permitir criar política de confirmação de acesso

11.3.127.12 Deve possibilitar a inspeção de tráfego HTTPS (Inbound/Outbound), sendo que para a opção de Outbound não será necessário efetuar o "man-inthe- middle", ou seja, a solução deverá prover mecanismo que irá analisar a conexão HTTPS para verificar se a URL solicitada está na lista de permissões de acesso, de acordo com a política configurada;

11.3.127.13 O administrador poderá adicionar filtros por palavra-chave de modo específico;

11.3.127.14 Deverá permitir o bloqueio Web através de senha pré configura pelo administrador

11.3.127.15 Deverá permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que, antes de iniciar a(navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

11.3.127.16 A solução deve fornecer um mecanismo para solicitação de categorização de URL caso está não esteja categorizada ou categorizada incorretamente;

11.3.127.17 Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação.

11.3.127.18 Suportar a criação de políticas baseadas no controle por URL e categoria de URL;

11.3.127.19 Suportar base ou cache de URLs local no appliance ou possibilitar a replicação da base de conhecimento de URLs do fabricante via instalação de máquina virtual, a infraestrutura da máquina virtual (VM) para uso desse recurso será fornecida pelo CONTRATANTE, evitando delay de comunicação/validação das URLs;

11.3.127.20 Possuir pelo menos 50 categorias de URLs;

11.3.127.21 Suporta a criação de categorias de URLs customizadas;

11.3.127.22 Suporta a exclusão de URLs do bloqueio, por categoria;

11.3.127.23 Deverá possibilitar a categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente;

11.3.127.24 A solução deverá permitir um mecanismo que permita sobrescrever as categorias de URL;

11.3.128 Permite a customização de página de bloqueio;

11.3.129 Deve possuir módulo de antivírus e anti-bot integrado no próprio appliance de segurança;

11.3.130 A solução de anti-virus integrada deve ter capacidade de analisar arquivos maiores que 1Gbps;

11.3.131 A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas;

11.3.132 Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

11.3.133 Implementar funcionalidade de detecção e bloqueio de callbacks;

11.3.134 A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede;

11.3.135 A solução Antibot deve possuir mecanismo de detecção que inclui, reputação de endereço IP;

11.3.136 Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS;

11.3.137 Implementar interface CLI segura através do protocolo SSH;

11.3.138 Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream;

11.3.139 A solução deve permitir criar regras de exceção de acordo com a proteção;

11.3.140 Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou incidentes referentes a incidentes de vírus e Bots;

11.3.141 Permitir o bloqueio de malwares (vírus, worms, spyware e etc.);

11.3.142 A solução deve ser capaz de proteger contra-ataques para DNS;

11.3.143 A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares;

11.3.144 A solução deve ser capaz de prevenir acesso a websites maliciosos;

11.3.145 A solução deve ser capaz de realizar inspeção de tráfego SSL e SSH;

11.3.146 A solução deverá receber atualizações de um serviço baseado em cloud;

11.3.147 A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos;

11.3.148 A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS;

11.3.149 A solução deve suportar funcionalidade de GeoIP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade;

11.3.150 A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de callbacks;

11.3.151 Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS e TLS;

11.3.152 A solução deve ser capaz de inspecionar o tráfego criptografado SSL e SSH;

11.3.153 Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

11.3.154 Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real;

11.3.155 Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb;

11.3.156 Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android;

11.3.157 Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware;

11.3.158 É imprescindível que a solução possua um limite mínimo de tamanho de arquivos de, ao menos, 200Mb, no uso da tecnologia 'gateway antimalware' liveprotection, já que

tal restrição poderia permitir a entrega de arquivos a um usuário final sem qualquer tipo de análise, aumentando significativamente o risco de infecção no ambiente.

11.3.159 A análise de gateway antimalware deve analisar qualquer tamanho de arquivo não permitindo restrições e limitações neste tipo de proteção a fim de mitigar a entrega de arquivos infectados à rede.

11.3.160 A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas;

11.3.161 A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliance através de assinaturas;

11.3.162 Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;

11.3.163 Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

11.3.164 Conter ameaças avançadas de dia zero;

11.3.165 Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;

11.3.166 Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;

11.3.167 Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

11.3.168 Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado;

11.3.169 Implementar a análise de arquivos executáveis, DLLs e ZIP em SSL no ambiente controlado;

11.3.170 Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP, IMAP e CIFS;

11.3.171 Conter ameaças de dia zero de forma transparente para o usuário final;

11.3.172 Conter ameaças de dia zero através de tecnologias em nível de emulação e código de registro;

11.3.173 Implementar mecanismo de pesquisa por diferentes intervalos de tempo;

11.3.174 Conter ameaças de dia zero via tráfego de internet;

11.3.175 Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança;

11.3.176 Conter ameaças de dia zero que possam burlar o sistema operacional emulado;

11.3.177 A solução deve permitir a criação de White list baseado no MD5 do arquivo;

11.3.178 Conter ameaças de dia zero antes da execução e evasão de qualquer código malicioso;

11.3.179 Conter exploits avançados;

11.3.180 A análise "In Cloud" ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Antispyware automaticamente, definir

URLs não confiáveis utilizadas pelo novo Malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede);

11.3.181 Suporte a submissão manual de arquivos para análise através do serviço de Sandbox;

11.3.182 Suportar no mínimo 20.000 usuários autenticados com serviços ativos e identificados passando por este dispositivo de segurança em um único dispositivo de segurança. Políticas baseadas por grupos de usuários deverão ser suportadas por este dispositivo. Está comprovação poderá ser exigida em testes sobe o ambiente de produção com o fornecimento do produto para comprovação deste e demais itens;

11.3.183 Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração;

11.3.184 Fornecer gerência remota, com interface gráfica nativa;

11.3.185 A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do firewall, incluindo a configuração de VPN IPSECs, NAT, perfis de acesso e regras de filtragem;

11.3.186 Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica, sem necessidade de se reinicializar o sistema;

11.3.187 Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;

11.3.188 Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall e a remoção de qualquer uma destas sessões ou conexões;

11.3.189 Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;

11.3.190 Permitir a visualização de estatísticas do uso de CPU, memória da máquina onde o firewall está rodando e tráfego de rede em todas as interfaces do Firewall através da interface gráfica remota, em tempo real e em forma tabular e gráfica;

11.3.191 Permitir a conexão simultânea de vários administradores, sendo um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas. Permitir que o segundo ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração;

11.3.192 Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;

11.3.193 Possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH sendo está múltiplas sessões simultâneas;

11.3.194 Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, podendo opcionalmente exportar os dados visualizados para arquivo formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP origem e/ou destino e porta IP origem e/ou destino, usando uma linguagem textual;

11.3.195 Permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do Firewall quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT (tradução de endereços) é eliminado;

11.3.196 Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP;

11.3.197 Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas;

11.3.198 Ser capaz de visualizar, de forma direta no appliance e em tempo real estado do processamento do produto e througput de dados utilizado pela rede de computadores conectado ao equipamento;

11.3.199 Possibilitar a geração de relatorio de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitindo o download em formato PDF;

11.3.200 Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilizada por política, por protocolo TCP/UDP/IPV4 e IPV6;

11.3.201 Ser capaz de visualizar, de forma direta no appliance e em tempo real as conexões estabelecidas, com possibilidade de aplicar filtros na visualização;

11.3.202 Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web);

11.3.203 Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreio das configurações aplicadas no produto;

11.3.204 Deve permitir a funcionalidade de ARP bridg;

11.3.205 Solução deve permitir o limite na taxa de envio ARP para um mesmo IP, para evitar "ARP Storm";

11.3.206 A solução deverá permitir o acesso aos registros de rastreamento, com opões de acesso as informações com possibilidade de visualização do "registro atual", "último registro", "todos os registros", "último E o atual", e "todos e atual";

11.3.207 Deve ser capaz de emitir relatório, mostrando a saúde do ambiente, agendado ou sob demanda, que liste informações de aplicações, risco, atividade WEB, análise de botnets, análise de malware, ameaças, países por tráfego, Arquivos compartilhados por aplicações, sessões e recomendações;

11.3.208 O administrador poderá ativar ou desativar a permissão de provisionamento através do recurso Zero-Touch.

11.3.209 O licenciamento para todos os serviços de Next Generation Firewall deverá ser de 36 meses;

11.3.210 No momento da entrega dos equipamentos a proponente vencedora deverá fornecer declaração do(s) fabricante(s), em papel timbrado com firma reconhecida, dos produtos ofertados, declarando que a proponente possui credenciamento do mesmo para a implantação e suporte técnico de seus produtos;

11.3.211 Deve ser homologado pela ANATEL.

11.4. SISTEMA DE ENERGIA ININTERRUPTA (UPS/NOBREAK) 2000VA

11.5.1 O UPS deve operar como um UPS de conversão dupla on-line com os seguintes modos:

11.4.1.1 Modo normal: O retificador deve obter energia conforme necessário da concessionária comercial AC ou fonte do gerador e fornecimento filtrado e regulado de energia DC para o inversor on-line. O inversor deve converter a energia DC em sua entrada para uma potência AC altamente regulada e filtrada para as cargas críticas;

11.4.1.2 Modo bateria: Após a falha completa da energia do utilitário, o UPS fornecerá energia para as cargas críticas através do inversor, a partir das baterias internas. Quando a energia da utilidade retornar, a unidade retornará à operação normal;

11.4.1.3 Modo By-Pass: O bypass automático deve transferir a carga crítica para a fonte AC comercial, contornando o inversor/retificador do UPS, no caso de uma sobrecarga, carga falha, ou falha interna;

11.4.1.4 Modo de espera: Quando inicialmente conectado a um utilitário ou outra fonte de energia, o UPS deve iniciar no modo de espera até que o usuário inicie a energia para a carga crítica;

11.4.1.5 Neste modo, o UPS deve recarregar as baterias, mas a energia não deve ser fornecida à carga crítica;

11.5.2 Saída do inversor:

11.4.2.1 Classificações máximas de potência: (VA / W) 2000/1800;

11.4.2.2 Tensão nominal de saída 220/230/240VAC;

11.4.2.3 Eficiência (carga completa, carga resistiva 91%;

11.4.2.4 O UPS deve tentar limpar as sobrecargas enquanto permanece no inversor em funcionamento normal (Modo TI) antes de transferir para o by-pass;

11.4.2.5 Contornar limiares de transferência no modo normal (por cento é por Watt/VA nominal);

11.4.2.5.1 - 105%~130%: 1 Minuto;

11.4.2.5.2 - 130%~150%: 30 segundos;

11.4.2.5.3 - >150%: desligamento após 300 ms;

11.4.2.6 Sobrecarga na bateria;

11.4.2.6.1 - 102%~130%: 12 segundos;

11.4.2.6.2 - 130%~150%: 2 segundos;

11.4.2.7 Forma de onda: Senoidal;

11.4.2.8 Regulação de tensão:

11.4.2.8.1 Modo normal: estado estável ±1%

11.4.2.8.2 Modo bateria: estado estável ±2%

11.4.2.8.3 Modo de conversão de frequência: estado estável ±4%

11.4.2.9 Distorção de tensão de saída THDV% no modo normal:

11.4.2.9.1 Carga linear: <2% de carga linear

11.4.2.9.2 Carga não linear: <5%

11.4.2.10 7. Regulação dinâmica de tensão:

11.4.2.10.1 20% 100% 20% R etapa de carga: ±6%

11.4.2.11 Tempo de recuperação (até 90% de recuperação de tensão):

11.4.2.11.1 0% 100 0% passo de carga não linear: 100ms @ full RCD load

11.4.2.12 Resposta transitória:

11.4.2.12.1 IEC 62040-3 Classificação I (método de teste definido por IEC62040-3 Editon2 2011 para carga R e carga não linear);

11.5.3 Entrada do sistema:

11.4.3.1 Faixa de tensão de entrada:

11.4.3.1.1 a <40% de carga: 100-300V;

11.4.3.1.2 >40% de carga: K-276V;

11.4.3.1.3 - K = (176-100) /(carga%-40%) V;

11.4.3.2 Histerese de tensão de entrada: Baixo +10V / Alto -10V;
11.4.3.3 Frequência – 50/60Hz:
11.4.3.3.1 Sensoriamento automático na inicialização;
11.4.3.3.2 Selecionável através do menu frontal;
11.4.3.4 Faixa de frequência 50Hz: 40-60Hz / 60Hz: 50-70Hz;
11.4.3.5 Histerese de frequência: Baixo +0,5Hz / Alto -0,5Hz;
11.4.3.6 Fator de potência de entrada: >0,99;
11.4.3.7 Distorção da corrente de entrada, THDi%: <5% na tensão de entrada nominal, carga completa e bateria totalmente carregada;

11.5.4 Baterias e Carregador:
11.4.4.1 Tipo de bateria: Ácido de chumbo regulado da válvula (VRLA), não-derramado, células de ácido de chumbo, sem manutenção
11.4.4.2 Aproximados e variam dependendo da configuração de carga e da carga da bateria.
11.4.4.3 Possibilitar a Substituição da bateria – (Baterias internas)
11.4.4.4 Gerenciamento avançado de baterias – O UPS fornecerá gerenciamento avançado debaterias que utiliza circuitos de sensoriamento sofisticados e uma técnica de
11.4.4.5 carregamento de três estágios que amplia a vida útil usada do UPS baterias enquanto otimiza o tempo de recarga da bateria. Além disso, o UPS deve ser capaz de fornecer até 60 dias de aviso sobre o fim da vida útil do serviço da bateria para ajudar no agendamento da bateria substituição.
11.4.4.6 Teste automático da bateria – Se o cliente não usar o gerenciamento avançado da bateria e usar um modo de carregamento constante, o UPS realizará um teste automático de bateria com um conjunto padrão de fábrica de uma vez por semana para determinar a saúde geral da bateria. Este intervalo deve ser definidor para selecionar nenhum teste, todos os dias, sempre semana, ou todos os meses.

11.5.5 Fator de forma
11.4.5.1 O UPS poderá ser usado somente em aplicação torre;
11.4.5.2 O aparelho consiste com uma Tela LCD interativa;
11.4.5.3 O UPS terá as dimensões seguintes: L x A x P (mm) 190 x 327 x 399;
11.4.5.4 O UPS terá o seguinte peso: 17,4 (KG);
11.4.5.5 Conexão de entrada NBR 14136;
11.4.5.6 Recipientes de saída NBR 14136 10A;

11.5.6 O UPS deve ser fornecido com um display LCD completo que fornece as informações e acesso a todas as configurações e recursos de controle do UPS;

11.5.7 A tela de status principal deve incluir todas as seguintes informações em uma única exibição:
11.4.7.1 Status do modo UPS;
11.4.7.2 Informação de carga do Nobreak;
11.4.7.3 Operação do Nobreak: Online / Bateria / Bypass;
11.4.7.4 Informação da Bateria: Porcentagem de carga da bateria;
11.4.7.5 Código de erro do Nobreak: Indica se o Nobreak está em Modo de Falha ou se há avisos, além do tipo de falha ou aviso. Vários tipos de avisos podem ser mostrados alternadamente. O ícone piscará se houver avisos. O ícone aparecerá continuamente quando em modo de falha;
11.4.7.6 Alarme Sonoro;
11.4.7.7 Informação de Entrada e Saída.

11.5.8 O UPS incluirá um slot de comunicação que permitirá que o operador instale em campo um cartão de comunicação de rede [Eaton Network New DX ou equivalente] que é fornecido aparte do UPS. As características mínimas são descritas abaixo:

11.4.8.1 O cartão de comunicação de rede deve ser instalado na traseira do equipamento;
11.4.8.2 Comunica-se com SNMPv3 e IPv6;
11.4.8.3 Suporta IETF UPS MIB;
11.4.8.4 Padrão UL 2900-1 e IEC 62443-4-2;

11.5.9 O UPS fornecerá uma conexão serial RS232. Cabo fornecido para fornecer interface DB-9;

11.5.10 O UPS fornecerá uma conexão USB compatível com HID para conexão de rede;

11.5.11 O UPS fornecerá tanto o recurso de desligamento remoto quanto de on/off remoto.

11.5.12 Desligamento remoto – Permitir que um contato remoto seja usado para desconectar a energia do UPS e de todos os dispositivos conectados. Reiniciar o UPS requer intervenção manual.

11.5.13 Ligar/desligar remotamente – Permite que o contato remoto seja usado para ativar e desativar o UPS. Redefinir o contato para a posição normal retornará automaticamente o NOS de volta ao estado normal sem intervenção manual através do menu frontal.

11.5.14 O UPS será compatível com o software de gerenciamento de energia WinPower ou equivalente. Este software executará as seguintes ações:
11.4.14.1 Monitora o consumo de energia no nível do segmento de carga;
11.4.14.2 Suporte a configuração de UPS redundante;
11.4.14.3 Software leve, não rodando em JRE;
11.4.14.4 Atualização em massa do firmware do cartão de rede;
11.4.14.5 Desencadeia movimento de máquinas virtuais para evitar desligamento de servidor que enfrenta interrupção iminente de energia;

11.5.15 Temperatura de funcionamento: 0 a 40°C (32°F a 104°F)

11.5.16 Temperatura de armazenamento: 0 a 35°C (32°F a 95°F)

11.5.17 Bateria sem temperatura de armazenamento: -25 a 55°C (-13°F a 131°F)

11.5.18 Umidade relativa: 0 a 95%

11.5.19 Supressão de surto: IEEE ANSI C62.41 Gato B2

11.5.20 Ruído audível: <40 dB a 1m

11.5.21 Deve possuir placa de comunicação de rede Gigabit de conectividade UPS que atenda padrões de segurança UL 2900-1 e IEC 62443-4-2 para gerência remota;

11.5.22 A placa de comunicação também deve possuir também:
11.4.22.1 possibilitar a execução ordenadamente de desligamento de servidores e armazenamento;
11.4.22.2 relógio em tempo real com bateria backup e ligação ao NTP (Protocolo de Tempo de Rede);
11.4.22.3 suportar os protocolos HTTPS, TLS 1.2, SNMPv1, SNMPv3, NTP, TFTP, SMTP, SMTPS, BOOTP, DHCP, SLAAC, SSH, MQTTS;
11.4.22.4 Gestão Avançada com API RESTful sobre HTTPS;
11.4.22.5 SMTP seguro para alertas de e-mail;
11.4.22.6 Suportar navegadores Chrome e Firefox para gerência https;
11.4.22.7 Suportar MIB / MIB II – Padrão IETF UPS MIB (RFC 1628).

11.5. SISTEMA DE ENERGIA ININTERRUPTA (UPS/NOBREAK) 20KVA

11.5.1 Entrada
11.5.1.1 Tensão de entrada nominal 1 fase 220/230/240V; 3 fase 380/400/415V;
11.5.1.2 Faixa de tensão de entrada 160V~300V carga completa 100~160V deserção de forro;
11.5.1.3 Frequência de entrada nominal 50 Hz/ 60 Hz;
11.5.1.4 Faixa de frequência de entrada 40 Hz – 70 Hz;

11.5.1.5 Faixa de bloqueio de fase de frequência de entrada 45 Hz – 55 Hz; 54 Hz – 66 Hz;
11.5.1.6 Compatibilidade do sistema TN-S / TI;
11.5.1.7 Corrente de vazamento de terra ≤7mA;
11.5.1.8 Fator de potência de entrada (PF) >0.995, tanto 1 fase quanto 3 fases;
11.5.1.9 Tempo de quebra da linha sem transferência para o modo bateria de 4ms;
11.5.1.10 Classificação de aumento de tensão de tensão de entrada L-N: 405J / L/N-GND: 445J;
11.5.1.11 THDi ≤3% de carga linear / ≤5% de carga não linear;
11.5.1.12 Fiação de entrada: Fase L+N+ G 1 / Fase L1+L2+L3+N+G 3;
11.5.1.13 Conexão de entrada por bloco terminal;
11.5.1.14 Conjunto gerador 2 vezes de energia nominal ups;

11.5.2 Saída

11.5.2.1 Conexão de fase entrada-saída 3-1, 3-3, 1-1;
11.5.2.2 Tensão de saída nominal 1 fase 220/230/240V / 3 fase 380/400/415V;
11.5.2.3 Frequência de saída nominal 50 Hz/ 60 Hz;
11.5.2.4 Potência de aparência de saída nominal 20KVA;
11.5.2.5 Potência ativa de saída nominal 20KW;
11.5.2.6 Max PF 1;
11.5.2.7 Variação de tensão ±1%;
11.5.2.8 Variação de Frequência ±0,1Hz;
11.5.2.9 THDV ≤1% de carga linear / ≤3% de carga não linear;
11.5.2.10 Classificação de desempenho VFI-SS-111 (não inclua o modo ECO ao modo inversor);
11.5.2.11 Relação de crista de carga ≥3:1;
11.5.2.12 Tempo de pausa 0ms (modo ESS para modo inversor 2ms, ECO para modo inversor 10ms);
11.5.2.13 Deslocamento DC de tensão de saída (Fase para Neutro) ±100 mV;
11.5.2.14 Desequilíbrio de tensão de saída ≤3%;
11.5.2.15 Fiação de saída: Fase L+N+ G 1 / Fase L1+L2+L3+N+G 3;
11.5.2.16 Conexão de saída por bloco terminal;
11.5.2.17 Modo de linha de sobrecarga (em tensão nominal) 105%<Carrão≤125%: 10min / 125%<Carreto≤150%: 1min >150%: 0,5s;
11.5.2.18 Modo de bateria de capacidade de sobrecarga (em tensão nominal) 105%<Carreto≤125%: 1min / 125%<Carreto≤150%: 30s >150%: 0,5s;
11.5.2.19 Modo de desvio de capacidade de sobrecarga (em tensão nominal) 105%<Car≤125%: constante / 125%<Carreto≤150%: 30s >150%: 0,5s;
11.5.2.20 Capacidade de liberação curta de saída 30.3A±2A@10s;

11.5.3 Bateria e Carregador

11.5.3.1 EBM UPS sem bateria embutida 2 Padrão EBM;
11.5.3.2 Número EBM máximo 6 *2;
11.5.3.3 Tensão da bateria ±192VDC padrão;
11.5.3.4 Capacidade da bateria 9AH;
11.5.3.5 Tempo de backup 1,8min (±192V) em carga total;
11.5.3.6 Corrente de carregamento 2A (ajuste 0~13A por LCD ou USB/RS232);
11.5.3.7 Método de carregamento ABM;
11.5.3.8 Compensação de temperatura 20mv/pcs/°C;
11.5.3.9 Corrente de ondulação da bateria (RMS) <200mA;
11.5.3.10 Tempo de recarga 3 horas a 90% (2 EBM);

11.5.4 Eficiência da UPS

11.5.4.1 Modo online até 96%;
11.5.4.2 Modo bateria até 94%;
11.5.4.3 Modo ECO ou ESS até 98,8%;
11.5.4.4 Perda de energia sem carga 120w;
11.5.4.5 CVCF (tensão constante e frequência constante) sem depreciação no modo 3-3, 3-1, depreciando para 60% no modo 1-1;
11.5.4.6 Modo paralelo máximo 3 (placa paralela incorporada);
11.5.4.7 Modo ESS (sistema de economia de energia);

11.5.5 Interface
11.5.5.1 Exposição LCD de cores touchscreen (com sensor de gravidade);
11.5.5.2 Idioma Inglês, França, Alemanha, Espanhol, Rússia, Português, Itália, Chinês;
11.5.5.3 RS232 DB9;
11.5.5.4 USB 2.0 tipo B;
11.5.5.5 Contator seco terminal EPO em terminal programável;
11.5.5.6 Slot longo padrão;
11.5.5.7 Porta de detecção automática EBM RJ 45;
11.5.5.8 Porta de detecção automática MBP RJ 45 (mesma porta com detecção de EBM);
11.5.5.9 Porta de controle do segmento de carga MBP RJ 45 (mesma porta com detecção de EBM);

11.5.6 Dimensão (H*W*D) 3U (129) *438 * 589mm;
11.5.7 Peso líquido (Kg) máximo 23.7;
11.5.8 Peso bruto (Kg) máximo 27.5;
11.5.9 Tipo de instalação rack e torre;
11.5.10 Temperatura de operação 0°C ~ 50 °C (0~40 sem depreciação, 40°C ~ 50°C desvalorizando para 50%);
11.5.11 Temperatura de armazenamento 25°C ~ 60°C;
11.5.12 Umidade Relativa 0 ~ 95%;
11.5.13 Altitude operacional 0~4000m (0~1000m sem depreciação, 1000m~4000m a carga derating 1 % a cada 100m);
11.5.14 Ruído ≤55dB;
11.5.15 Nível de proteção (IP) IP20;
11.5.16 EMI C3;
11.5.17 ESD IEC/EN 61000-4-2 Nível 3;
11.5.18 RS IEC/EN 61000-4-3 Nível 3;
11.5.19 EFT IEC/EN 61000-4-4 Nível 4;
11.5.20 Surto IEC/EN 61000-4-4 Nível 4;
11.5.21 MTBF 150 mil horas;
11.5.22 Segurança CE/TLC (nível 1) /RCM
11.5.23 Deve possuir placa de comunicação de rede Gigabit de conectividade UPS que atenda padrões de segurança UL 2900-1 e IEC 62443-4-2 para gerência remota;
11.5.24 A placa de comunicação também deve possuir também:
11.5.24.1 possibilitar a execução ordenadamente de desligamento de servidores e armazenamento;
11.5.24.2 relógio em tempo real com bateria backup e ligação ao NTP (Protocolo de Tempo de Rede);
11.5.24.3 suportar os protocolos HTTPS, TLS 1.2, SNMPv1, SNMPv3, NTP, TFTP, SMTP, SMTPS, BOOTP, DHCP, SLAAC, SSH, MQTTS;
11.5.24.4 Gestão Avançada com API RESTful sobre HTTPS;
11.5.24.5 SMTP seguro para alertas de e-mail;
11.5.24.6 Suportar navegadores Chrome e Firefox para gerência https;

11.5.24.7 Suportar MIB / MIB II – Padrão IETF UPS MIB (RFC 1628).

11.6. SWITCH DE ACESSO L2+L3 48 PORTAS 10/100/1000BASE-T

11.6.1 Deve permitir instalação em rack de 19" padrão Telco EIA;
11.6.2 Deve possuir altura máxima 1 (um) rack unit (RU);
11.6.3 Deve possuir fonte de alimentação interna, do tipo auto-sense, para operar de 100 a 240 VAC;
11.6.4 Deve possuir 48 (quarenta e oito) portas 10/100/1000 Mbps, usando conectores RJ-45;
11.6.5 As portas 10/100/1000 BASE-T devem ser do tipo MDI/MDIX automático;
11.6.6 Deve possuir, no mínimo, 4 (quatro) portas 1 Gbps SFP, as quais não devem operar em modo "combo" com as portas 10/100/1000 BASE-T em par trançado;
11.6.7 Deve possuir, no mínimo, 4 (quatro) portas 1/10/25 Gbps SFP28, as quais não devem operar em modo "combo" com as portas 10/100/1000 BASE-T em par trançado;
11.6.8 Deve possuir capacidade de processamento igual ou superior a 220 (duzentos e vinte) Mpps;
11.6.9 Deve possuir capacidade de switching igual ou superior a 296 (duzentos e noventa e seis) Gbps;
11.6.10 Deve possuir, pelo menos, 4 MB de buffers de pacotes;
11.6.11 Deve possuir, pelo menos, 4 GB de memória DRAM;
11.6.12 Deve possuir, pelo menos, 8 GB de memória NVRAM;
11.6.13 Deve implementar os protocolos IEEE 802.3af Power over Ethernet (PoE) e IEEE 802.3at Power over Ethernet Plus (PoE+);
11.6.14 Deve possuir PoE power budget de pelo menos 370 (trezentos e setenta) watts;
11.6.15 Deve suportar empilhamento futuro de até 10 (dez) unidades outros equipamentos em topologia linear e em anel;
11.6.16 O equipamento deve suportar empilhamento através de cabos de fibra óptica com distância de pelo menos 10 (dez) km entre cada uma das unidades da pilha;
11.6.17 Deve possuir porta de gerenciamento "out-of-band" operando a 10/100/1000 Mbps;
11.6.18 Deve possuir porta de console para gerenciamento utilizando conector RJ-45, USB, mini-USB ou USB Tipo C;
11.6.19 Possui slot USB para inserção de uma mídia de armazenamento removível para fazer upgrade de imagem do switch e backup da configuração;
11.6.20 Deve possuir LEDs indicativos de energização, status de slot USB, atividade do link e velocidade das portas;
11.6.21 Deve possuir botão de reset voltar à para configuração default de fábrica;
11.6.22 Deve implementar o padrão IEE 802.3az (Energy-Efficient Ethernet);
11.6.23 Deve possuir certificado de homologação junto à ANATEL de acordo a resolução 242 com documentos disponíveis publicamente no sítio público dessa agência na Internet;
11.6.24 Deve permitir realizar troubleshooting visual da unidade na pilha, identificando através de LEDs se o switch é master ou slave da pilha, e sua identificação na pilha;
11.6.25 Deve permitir identificar através de sinalização visual onde o switch está localizado no rack através de comandos para ligar e desligar os LEDs do equipamento;
11.6.26 Deve possuir capacidade de no mínimo 32.000 (trinta e dois mil) endereços MAC;
11.6.27 Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad. Deve permitir a configuração de pelo menos 128 (cento e vinte e oito) grupos de LACP com pelo menos 8 (oito) portas dentro de um mesmo grupo;

11.6.28 Deve implementar o protocolo IEEE 802.1Q para criação de pelo menos 4000 (quatro mil) vlans ativas;
11.6.29 Deve implementar o protocolo IEEE 802.1s (Multiple Spanning Tree), IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1D (Spanning Tree);
11.6.30 Deve ser compatível com o protocolo PVST+;
11.6.31 Deve permitir a configuração de pelo menos 250 (duzentas e cinquenta) instâncias de Spanning Tree;
11.6.32 Deve implementar BPDU Guard e Root Guard;
11.6.33 Deve permitir a configuração de VLANs "trunking" de acordo com o protocolo 802.1Q e VLANs nativas (sem tag) simultaneamente na mesma porta;
11.6.34 Deve permitir a criação VLANs privadas;
11.6.35 Deve permitir a configuração de VLAN Q-in-Q Tagging de acordo com o padrão IEEE802.1ad ou IEEE802.1QinQ;
11.6.36 Deve implementar selective QinQ;
11.6.37 Deve implementar para o protocolo UDLD (Uni-Directional Link Detection) ou DLDP (Device Link Detection Protocol) ou similar;
11.6.38 Deve implementar jumbo frames até 9000 bytes nas portas Gigabit Ethernet;
11.6.39 Deve implementar mecanismos para controle do tráfego broadcasts, multicast e unknown unicast;
11.6.40 Deve implementar mecanismo de detecção ativa de loops através do envio frames de detecção. Na detecção de um evento de loop, deve ser capaz de realizar o bloqueio da porta (port shutdown);
11.6.41 Deve permitir a configuração de endereços MAC de unicast multicast estáticos em múltiplas portas ethernet simultaneamente, para permitir a configuração de "clusters" de firewalls;
11.6.42 Deve implementar IGMP Snooping para IGMPv1, IGMPv2 e IGMPv3;
11.6.43 Deve implmenetar MLD snooping v1 e v2;
11.6.44 Deve implementar MVRP (Multiple VLAN Registration Protocol);
11.6.45 Deve implementar MVR (Multicast VLAN Registration);
11.6.46 Deve possuir funcionalidade de refletir a tráfego de entrada de uma porta Ethernet, retornando para um gerador de teste para permitindo medir a continuidade da rede e o desempenho da porta ethernet;
11.6.47 Deve implementar protocolo de proteção de topologia em anel;
11.6.48 Deve permitir roteamento local entre VLANs utilizando interfaces virtuais ou SVIs;
11.6.49 Deve permitir a configuração de rotas estáticas usando endereços IPv4 e IPv6;
11.6.50 Deve permitir a configuração de endereço IPv6 com prefixo de 127 bits para links point-to-point;
11.6.51 Deve implementar roteamento IP usando os protocolos RIPv1/v2 e RIPng;
11.6.52 Deve suportar roteamento IP usando os protocolos OSPFv2 e OSPFv3.
11.6.53 Deve suportar os protocols VRRP e VRRPv3;
11.6.54 Deve implementar ECMP com no mínimo 8 caminhos;
11.6.55 Deve suportar os protocolos de roteamento de multicast PIM-S, PIM-SSM e PIM-DM; Caso a funcionalidade seja ativada por licenciamento, não será necessário o seu fornecimento nesse processo;
11.6.56 Deverá possuir no mínimo 500 (quinhentas) interfaces virtuais para roteamento entre VLANs;
11.6.57 Deve permitir a configuração de pelo menos 2000 (duas mil) rotas estáticas IPv4;
11.6.58 Deve permitir a configuração de pelo menos 1000 (mil) rotas estáticas IPv6;
11.6.59 Deverá suportar a capacidade de pelo menos 16.000 (dezesseis mil) entradas na sua tabela de IPv4;

11.6.60 Deverá suportar a capacidade de pelo menos 4.000 (quatro mil) entradas em sua tabela de roteamento IPv6;
11.6.61 Deve possuir DHCP Server para IPv4 e IPv6;
11.6.62 Deve permitir a configuração de DHCP Relay;
11.6.63 Deve suportar PBR (Policy-Based Routing) para IPv4 e IPv6;
11.6.64 Deve implementar VRF ou VRF-lite, com suporte a pelo menos 16 (dezesseis) instâncias;
11.6.65 Deve implementar túnel GRE;
11.6.66 Deve implementar IPv6 router advertisement (RA) preference na mensagem de RA com informações de múltiplos routers para escolher a rota default apropriada pelo host IPv6;

11.6.67 Deve permitir priorização de tráfego usando 8 (oito) filas de priorização por porta;
11.6.68 Deve permitir priorização de tráfego baseado no padrão IEEE 802.1p e no campo DSCP do protocolo Diffserv;
11.6.69 Deve implementar pelos menos os seguintes métodos para configuração das filas de priorização: ponderada, prioridade estrita e ambas combinadas;
11.6.70 Implementar priorização de tráfego baseado em porta física, protocolo IEEE 802.1p, endereços IP de origem e destino e portas TCP/UDP de origem e destino;
11.6.71 Deve permitir a configuração de Rate Limiting de entrada;
11.6.72 Deve permitir a configuração de Rate Shaping de saída;
11.6.73 Deve implementar os seguintes algoritmos de fila: Strict Priority e Round Robin com distribuição de pesos WRR (Weighted Round Robin) e uma combinação entre os dois métodos SP e WRR;
11.6.74 Deve suportar SDVoE (Software Defined Video over Ethernet);
11.6.75 Deve permitir autenticação de usuários usando o padrão IEEE 802.1x, permitindo associação dinâmica de VLANs e ACLs usando profiles definidas por um servidor RADIUS externo;
11.6.76 Deve permitir a associação de VLANs restritas para usuários que falhem durante a autenticação 802.1X;
11.6.77 Implementar método de autenticação baseado em endereço MAC para os dispositivos que não possuírem suplicantes 802.1X;
11.6.78 Deve possuir capacidade de autenticação 802.1x com atribuição de VLAN, regras de acesso de segurança e QoS individuais para, no mínimo, 02 (dois) dispositivos (Ex.: Telefone IP e PC) conectados em uma única porta e usando VLANs distintas;
11.6.79 Deve permitir, no mínimo e em cada porta, os seguintes tipos de autenticação usando VLANs distintas: (dois) dispositivos que suportam o padrão IEEE 802.1x, (dois) dispositivos MAC que não suportam o padrão IEEE 802.1x, (um) dispositivo que suporta o padrão IEEE 802.1x e 1 (um) dispositivo MAC que não suporta o padrão IEEE 802.1x;
11.6.80 O equipamento deve permitir a configuração de reautenticação 802.1x periódica;
11.6.81 O equipamento ofertado deve permitir a autenticação via Web Authentication para usuários que não possuem 802.1x;
11.6.82 Deve implementar "Change of Authorization" de acordo com a RFC 5176;
11.6.83 Deve permitir a autenticação de usuários para acesso às funções de gerenciamento usando-se os protocolos RADIUS, TACACS ou TACACS+;
11.6.84 Deve permitir a criação de ACLs para a filtragem de tráfego IPv4 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, bits do protocolo 802.1p e campo DSCP do protocolo Diffserv;

11.6.85 Deve permitir a criação de ACLs para a filtragem de tráfego IPv6 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, campo PCP do protocolo 802.1p e campo DSCP do protocolo Diffserv;

11.6.86 Deve implementar ACLs de entrada e ACLs de saída para IPv4;

11.6.87 Deve implementar ACLs de entrada e ACLs de saída para IPv6;

11.6.88 Permitir a filtragem do tráfego através de pelo menos 1000 (mil) regras de ACL (Access Control List);

11.6.89 Deve implementar segurança de acesso baseada em endereços MAC de origem, com a possibilidade de bloqueio permanente ou temporário das portas onde for detectada uma violação de segurança;

11.6.90 Deve permitir a criação de filtros de endereço MAC de origem e destino;

11.6.91 Deve possuir protocolos para proteção de ataques de Denial of Service;

11.6.92 Deve possuir funcionalidade de proteção contra servidores DHCP não autorizados DHCPv4 snooping e DHCPv6 snooping;

11.6.93 Deve possuir funcionalidade de proteção contra-ataques do tipo "ARP Poisoning";

11.6.94 Deve implementar IP Source Guard;

11.6.95 Deve implementar proteção contra-ataques do tipo TCP SYN e ataques do tipo Smurf;

11.6.96 Deve permitir o monitoramento da movimentação de um endereço MAC de uma porta para outra, facilitando a distinção entre um movimento legítmo com um movimento malicioso de um ataque de MAC spoofing;

11.6.97 Deve implementar IPv6 RA guard e IPv6 ND inspection;

11.6.98 Deve implementar RADsec conforme RFC6614;

11.6.99 Deve permitir monitoração e configuração usando SNMP v1, v2 e v3;

11.6.100 Deve permitir o gerenciamento via SNMPv3 com as seguintes opções: sem autenticação e sem privacidade, com autenticação e sem privacidade e com autenticação e com privacidade;

11.6.101 Deve ser possível enviar "traps" e realizar o gerenciamento via SNMP através das redes IPv4 e IPv6;

11.6.102 Deve permitir a configuração de porta para espelhamento de tráfego, para a coleta de pacotes em analisadores de protocolo ou detecção de intrusão;

11.6.103 Deve permitir espelhamento de tráfego baseado em Porta, VLAN, Filtro MAC e ACL;

11.6.104 Deve permitir a configuração de porta para espelhamento de tráfego para uma porta em um switch remoto;

11.6.105 Deve implementar gerenciamento usando SSH v2 utilizando os algoritmos de criptografia 3DES e AES. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

11.6.106 Deve implementar gerenciamento via Telnet. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

11.6.107 Deve implementar pelo menos 4 (quatro) grupos de RMON;

11.6.108 Deve permitir o monitoramento dos transceivers óticos, retornando informação de temperatura, potência de transmissão (dBm), potência de recepção (dBm) e status;

11.6.109 Deve implementar funcionalidade de diagnóstico do cabo de par trançado, retornando informação de comprimento do cabo, status do link;

11.6.110 Deve permitir a atualização de arquivos de configuração e imagens de firmware usando TFTP ou FTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

11.6.111 Deve permitir a atualização de imagens de firmware dos equipamentos de uma pilha sem a necessidade de reinicialização simultânea de todos os equipamentos da pilha, permitindo a continuidade do tráfego de dados durante o processo de atualização;

11.6.112 Deve permitir configuração automática do seu próprio endereço IP e a seguir carga automática de um arquivo de configuração pré-definido, usando um servidor DHCP e um servidor TFTP ou FTP;

11.6.113 Deve implementar o protocolo LLDP conforme o padrão IEEE 802.1AB, bem como LLDP-MED;

11.6.114 Deve implementar o protocolo OpenFlow 1.3 com suporte para portas híbridas em Camada 2 e Camada 3;

11.6.115 Deve permitir o monitoramento de tráfego através dos protocolos sFlow, NetFlow ou IPFIX. Deve ser possível exportar o tráfego de redes IPv4 e IPv6;

11.6.116 Deve permitir a configuração de seu relógio interno de forma automática através do protocolo NTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

11.6.117 Deve permitir armazenamento simultâneo de duas imagens de firmware em memória flash;

11.6.118 Deve permitir atualização de imagem de firmware através de mídia de armazenamento externa conectado ao slot USB;

11.6.119 Deve permitir o envio de mensagens de syslog à pelo menos 2 servidores distintos;

11.6.120 Deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

11.6.121 Deve permitir o envio de syslog com formato conforme RF5424 para prover mais informações no seu header;

11.6.122 Deve possuir suporte a automação com Ansible.

11.6.123 Deve suportar RESTCONF;

11.6.124 Deve implementar funcionalidade de rollback automático de configuração, permitindo que o switch retorne automaticamente para uma configuração estável prévio caso o administrador não confirmar a alteração realizada dentro de um prazo de tempo configurável

11.7. SWITCH 48 PORTAS FIBER COM 2 PORTAS UPLINK/STACK QSFP28

11.7.1 Deve permitir instalação em rack de 19" padrão Telco EIA;

11.7.2 Deve possuir altura máxima 1 (um) rack unit (RU);

11.7.3 Deve possuir fonte de alimentação interna, do tipo auto-sense, para operar de 100 a 240 VAC;

11.7.4 Deve possuir fonte de alimentação redundante interna e hot-swappable;

11.7.5 Deve possuir capacidade de processamento igual ou superior a 670 (seiscentos e setenta) Mpps;

11.7.6 Deve possuir capacidade de switching igual ou superior a 900 (novecentos) Gbps;

11.7.7 Deve possuir 48 (quarenta e oito) portas SFP, sendo que no mínimo 12 (doze) dessas portas devem operando 1G/10GbE compatíveis com SFP/SFP+ e o restante das portas devem operar em 1GbE SFP;

11.7.8 Deve permitir empilhamento de até 10 (dez) unidades outros equipamentos em topologia linear e em anel, e permitir gerenciar a pilha com um único endereço IP;

11.7.9 Deve possuir banda agregada de empilhamento mínima de 160 (cento e sessenta) Gbps ,podendo ser através de 2 (duas) portas de 40 (quarenta) Gbps operando em full-duplex. As portas de empilhamento deverão ser fornecidas nesse certame;

11.7.10 O equipamento deve permitir empilhamento através de cabos de fibra óptica com distância de pelo menos 10 (dez) km entre cada uma das unidades da pilha;

11.7.11 Deve suportar expansão futura de pelo mínimo 1 (uma) porta 100Gbps QSFP28 adicional as portas solicitadas nesse certame;

11.7.12 Deve suportar expansão futura de pelo no mínimo 2 (duas) portas 40Gbps QSFP+ adicionais as portas solicitadas nesse certame;

11.7.13 Deve suportar expansão futura de pelo menos 4 (quatro) portas 1/10Gbps SFP+ adicionais as portas solicitadas nesse certame;

11.7.14 Deve ser compatível com SFP 1000BASE-SX, 1000BASE-LX e 1000Base-T;

11.7.15 Deve ser compatível com SFP+ 10GBASE-SR,10GBASE-LR, 10GBASE-ER;

11.7.16 Deve ser compatível com QSFP+ 40GBASE-SR4, 40GBASE-LR4 e 40G-BiDi;

11.7.17 Deve ser compatível com QSFP28 100GBASE-SR4, 100GBASE-LR4 e 100GBASE-CWDM4;

11.7.18 Deve possuir pelo menos 8MB de buffer de pacotes;

11.7.19 Deve possuir, no mínimo, 4GB de memória DRAM e 4GB de memória NVRAM (flash);

11.7.20 deve possuir ventilação front to back, isto é, o fluxo de ar deve seguir no sentido das portas de interface para as fontes de energia;

11.7.21 Deve suportar a inversão do fluxo de ar de ventilação para o modo "back to front" através de pelo menos um dos seguinte métodos: troca de ventiladores e fontes, atualização de firmware ou alteração do arquivo de configuração;

11.7.22 Deve possuir porta de gerenciamento "out-of-band" operando a 10/100/1000 Mbps;

11.7.23 Deve possuir porta de console para gerenciamento utilizando conector RJ-45, USB, mini-USB ou USB Tipo C;

11.7.24 Possui slot USB para inserção de uma mídia de armazenamento removível para fazer upgrade de imagem do switch e backup da configuração;

11.7.25 Deve possuir LEDs indicativos de energização, status de slot USB, atividade do link e velocidade das portas;

11.7.26 Deve permitir realizar troubleshooting visual da unidade na pilha, identificando através de LEDs se o switch é master ou slave da pilha, e sua identificação na pilha;

11.7.27 Deve permitir identificar através de sinalização visual onde o switch está localizado no rack através de comandos para ligar e desligar os LEDs do equipamento;

11.7.28 Deve possuir botão de reset voltar a para configuração default de fábrica;

11.7.29 O proponente deve apresentar carta oficial de revenda autorizada pelo fabricante do equipamento ofertado;

11.7.30 A proposta comercial deve descriminar o fabricante e o modelo do equipamento ofertado bem como seus respectivos "P/Ns";

11.7.31 Deve ser novo e em plena fabricação. Não serão aceitos equipamentos com avisos de "End of Life" emitidos pelo fabricante;

11.7.32 Deve possuir certificado de homologação junto à ANATEL de acordo a resolução 242 com documentos disponíveis publicamente no sítio público dessa agência na Internet;

11.7.33 Deve possuir capacidade de no mínimo 110.000 (cento e dez mil) endereços MAC;

11.7.34 Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad. Deve permitir a configuração de pelo menos 250 (duzentos e cinquenta) grupos de LACP com pelo menos 16 (dezesseis) portas dentro de um mesmo grupo;

11.7.35 Deve permiter a configuração de grupos de portas agregadas (LAGs) com balanceamento simétrico, garantindo que o tráfego de um mesmo origem e destino passe pela mesma porta de um LAG de forma bidirecional;

11.7.36 Deve implementar o protocolo IEEE 802.1Q para criação de pelo menos 4000 (quatro mil) vlans ativas;

11.7.37 Deve implementar o protocolo IEEE 802.1s (Multiple Spanning Tree), IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1D (Spanning Tree);

11.7.38 Deve ser compatível com o protocolo PVST+;

11.7.39 Deve permitir a configuração de pelo menos 250 (duzentas e cinquenta) instâncias de Spanning Tree;
11.7.40 Deve implementar BPDU Guard e Root Guard;
11.7.41 Deve permitir a configuração de VLANs "trunking" de acordo com o protocolo 802.1Q e VLANs nativas (sem tag) simultaneamente na mesma porta;
11.7.42 Deve permitir a criação VLANs privadas;
11.7.43 Deve permitar a configuração de VLAN Q-in-Q Tagging de acordo com o padrão IEEE802.1ad ou IEEE802.1QinQ;
11.7.44 Deve implementar selective QinQ;
11.7.45 Deve implementar para o protocolo UDLD (Uni-Directional Link Detection) ou DLDP (Device Link Detection Protocol) ou similar;
11.7.46 Deve implementar jumbo frames até 9000 bytes nas portas Gigabit Ethernet;
11.7.47 Deve implementar mecanismos para controle do tráfego broadcasts, multicast e unknown unicast;
11.7.48 Deve implementar mecanismo de detecção ativa de loops através do envio frames de detecção. Na detecção de um evento de loop, deve ser capaz de realizar o bloqueio da porta (port shutdown) ;
11.7.49 Deve permitir a configuração de endereços MAC de unicast multicast estáticos em múltiplas portas ethernet simultaneamente, para permitir a configuração de "clusters" de firewalls;
11.7.50 Deve implementar IGMP Snooping para IGMPv1, IGMPv2 e IGMPv3;
11.7.51 Deve implmenetar MLD snooping v1 e v2;
11.7.52 Deve implementar MVRP (Multiple VLAN Registration Protocol);
11.7.53 Deve possuir funcionalidade de refletir a tráfego de entrada de uma porta Ethernet, retornando para um gerador de teste para permitindo medir a continuidade da rede e o desempenho da porta ethernet;
11.7.54 Deve implementar protocolo de proteção de topologia em anel;
11.7.55 Deve permitir roteamento local entre VLANs utilizando interfaces virtuais ou SVIs;
11.7.56 Deve permitir a configuração de rotas estáticas usando endereços IPv4 e IPv6;
11.7.57 Deve permitir a configuração de endereço IPv6 com prefixo de 127 bits para links point-to-point;
11.7.58 Deve implementar roteamento IP usando os protocolos RIPv1/v2 e RIPng;
11.7.59 Deve implementar roteamento IP usando os protocolos OSPFv2 e OSPFv3;
11.7.60 Deve implementar roteamento usando o protocolo BGP4 e BGP4+;
11.7.61 Deve implementar criação de túneis GRE;
11.7.62 Deve implementar VRF ou VRF-lite, com suporte a pelo menos 32 (trinta e duas) instâncias;
11.7.63 Deve implementar os protocolos VRRP e VRRPv3;
11.7.64 Deve implementar ECMP com no mínimo 8 (oito) caminhos;
11.7.65 Deve implementar os protocolos de roteamento de multicast PIM-S, PIM-SSM e PIM-DM;
11.7.66 Deve suportar PIM-Passive para reduzir e minimizar tráfego de controle.
11.7.67 Deverá possuir no mínimo 500 (quinhentas) interfaces virtuais para roteamento entre VLANs
11.7.68 Deve permitir a configuração de pelo menos 2.000 (duas mil) rotas estáticas IPv4;
11.7.69 Deve permitir a configuração de pelo menos 1.000 (mil) rotas estáticas IPv6;
11.7.70 Deverá suportar a capacidade pelo menos 97.000 (noventa e sete mil) entradas em sua tabela de roteamento IPv4;
11.7.71 Deverá suportar a capacidade de pelo menos 17.000 (dezessete mil) entradas em sua tabela de roteamento IPv6;

11.7.72 Deve possuir DHCP Server para IPv4 e IPv6;
11.7.73 Deve permitir a configuração de DHCP Relay;
11.7.74 Deve implementar PBR (Policy-Based Routing) para IPv4 e IPv6;
11.7.75 Deve implementar IPv6 router advertisement (RA) preference na mensagem de RA com informações de múltiplos routers para a escolher a rota default apropriada pelo host IPv6;
11.7.76 Deve pemitir priorização de tráfego usando 8 (oito) filas de priorização por porta;
11.7.77 Deve permitir priorização de tráfego baseado no padrão IEEE 802.1p e no campo DSCP do protocolo Diffserv;
11.7.78 Deve implementar pelos menos os seguintes métodos para configuração das filas de priorização: ponderada, prioridade estrita e ambas combinadas;
11.7.79 Implementar priorização de tráfego baseado em porta física, protocolo IEEE 802.1p, endereços IP de origem e destino e portas TCP/UDP de origem e destino;
11.7.80 Deve permitir a configuração de Rate Limiting de entrada;
11.7.81 Deve permitir a configuração de Rate Shaping de saída;
11.7.82 Deve implementar os seguintes algoritmos de fila: Strict Priority e Round Robin com distribuição de pesos WRR (Weighted Round Robin) e uma combinação entre os dois métodos SP e WRR;
11.7.83 Deve permitir autenticação de usuários usando o padrão IEEE 802.1x, permitindo associação dinâmica de VLANs e ACLs usando profiles definidas por um servidor RADIUS externo;
11.7.84 Deve permitir a associação de VLANs restritas para usuários que falhem durante a autenticação 802.1X;
11.7.85 Implementar método de autenticação baseado em endereço MAC para os dispositivos que não possuirem suplicantes 802.1X;
11.7.86 Deve possuir capacidade de autenticação 802.1x com atribuição de VLAN, regras de acesso de segurança e QoS individuais para, no mínimo, 02 (dois) dispositivos (Ex.: Telefone IP e PC) conectados em uma única porta e usando VLANs distintas;
11.7.87 Deve permitir, no mínimo e em cada porta, os seguintes tipos de autenticação usando VLANs distintas:
6.7.87.1 2 (dois) dispositivos que suportam o padrão IEEE 802.1x;
6.7.87.2 5.5.2 2 (dois) dispositivos MAC que não suportam o padrão IEEE 802.1x;
6.7.87.3 5.5.3 1 (um) dispositivo que suporta o padrão IEEE 802.1x e 1 (um) dispositivo MAC que não suporta o padrão IEEE 802.1x;
11.7.88 O equipamento deve permitir a configuração de reautenticação 802.1x periódica;
11.7.89 O equipamento ofertado deve permitir a autenticação via Web Authentication para usuários que não possuem 802.1x;
11.7.90 Deve implementar "Change of Authorization" de acordo com a RFC 5176;
11.7.91 Deve permitir a autenticação de usuários para acesso às funções de gerenciamento usando-se os protocolos RADIUS, TACACS ou TACACS+;
11.7.92 Deve permitir a criação de ACLs para a filtragem de tráfego IPv4 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, bits do protocolo 802.1p e campo DSCP do protocolo Diffserv;
11.7.93 Deve permitir a criação de ACLs para a filtragem de tráfego IPv6 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, campo PCP do protocolo 802.1p e campo DSCP do protocolo Diffserv;
11.7.94 Deve implementar ACLs de entrada e ACLs de saída para IPv4;
11.7.95 Deve implementar ACLs de entrada e ACLs de saída para IPv6;

11.7.96 Deve implementar segurança de acesso baseada em endereços MAC de origem, com a possibilidade de bloqueio permanente ou temporário das portas onde for detectada uma violação de segurança;
11.7.97 Deve permitir a criação de filtros de endereço MAC de origem e destino;
11.7.98 Deve possuir protocolos para proteção de ataques de Denial of Service;
11.7.99 Deve possuir funcionalidade de proteção contra servidores DHCP não autorizados DHCPv4 snooping e DHCPv6 snooping;
11.7.100 Deve possuir funcionalidade de proteção contra ataques do tipo "ARP Poisoning";
11.7.101 Deve permitir a configuração de Dynamic ARP Inspection em pelo menos 500 vlans;
11.7.102 Deve implementar IP Source Guard;
11.7.103 Deve implementar proteção contra ataques do tipo TCP SYN e ataques do tipo Smurf;
11.7.104 Deve permitir o monitoramento da movimentação de um endereço MAC de uma porta para outra, facilitando a distinção entre um movimento legítmo com um movimento malicioso de um ataque de MAC spoofing;
11.7.105 Deve implementar IPv6 RA guard e IPv6 ND inspection;
11.7.106 Deve implementar RADsec conforme RFC6614;
11.7.107 Deve implementar unicast Reverse Path Forwarding (uRPF) como ferramenta para evitar ataques do tipo source IP spoofing;
11.7.108 Deve permitir monitoração e configuração usando SNMP v1, v2 e v3;
11.7.109 Deve permitir o gerenciamento via SNMPv3 com as seguintes opções: sem autenticação e sem privacidade, com autenticação e sem privacidade e com autenticação e com privacidade;
11.7.110 Deve ser possível enviar "traps" e realizar o gerenciamento via SNMP através das redes IPv4 e IPv6;
11.7.111 Deve permitir a configuração de porta para espelhamento de tráfego, para a coleta de pacotes em analisadores de protocolo ou detecção de intrusão;
11.7.112 Deve permitir espelhamento de tráfego baseado em Porta, VLAN, Filtro MAC e ACL;
11.7.113 Deve permitir a configuração de porta para espelhamento de tráfego para uma porta em um switch remoto;
11.7.114 Deve implementar gerenciamento usando SSH v2 utilizando os algoritimos de criptografia 3DES e AES. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;
11.7.115 Deve implementar gerenciamento via Telnet. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;
11.7.116 Deve implementar pelo menos 4 (quatro) grupos de RMON;
11.7.117 Deve permitir o monitoramento dos transceivers óticos, retornando informação de temperatura, potência de transmissão (dBm), potência de recepção (dBm) e status;
11.7.118 Deve permitir a atualização de arquivos de configuração e imagens de firmware usando TFTP ou FTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
11.7.119 Deve permitir a atualização de imagens de firmware dos equipamentos de uma pilha sem a necessidade de reinicialização simultânea de todos os equipamentos da pilha, permitindo a continuidade do tráfego de dados durante o processo de atualização;
11.7.120 Deve permitir configuração automática do seu próprio endereço IP e a seguir carga automática de um arquivo de configuração pré-definido, usando um servidor DHCP e um servidor TFTP ou FTP;
11.7.121 Deve implementar o protocolo LLDP conforme o padrão IEEE 802.1AB, bem como LLDP-MED;
11.7.122 Deve implementar o protocolo OpenFlow 1.3 com suporte para portas híbridas em Camada 2 e Camada 3;

11.7.123 Deve permitir o monitoramento de tráfego através dos protocolos sFlow, NetFlow ou IPFIX. Deve ser possível exportar o tráfego de redes IPv4 e IPv6;

11.7.124 Deve permitir a configuração de seu relógio interno de forma automática através do protocolo NTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

11.7.125 Deve permitir armazenamento simultâneo de duas imagens de firmware em memória flash.

11.7.126 Deve permitir atualização de imagem de firmware através de mídia de armazenamento externa conectado ao slot USB;

11.7.127 Deve permitir o envio de mensagens de syslog à pelo menos 2 servidores distintos. Deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

11.7.128 Deve permitir o envio de syslog com formato conforme RF5424 para prover mais informações no seu header;

11.7.129 Deve possuir suporta a automação com Ansible;

11.7.130 Deve implementar RESTCONF;

11.7.131 Deve implementar funcionalidade de rollback automático de configuração, permitindo que o switch retorne automaticamente para uma configuração estável prévio caso o administrador não confirmar a alteração realizada dentro de um prazo de tempo configurável.

11.8. ESTAÇÃO DE TRABALHO DO TIPO DESKTOP COMPACTO TIPO 1

11.8.1 Processador com frequência mínima de 3 Ghz baseada em processador;

11.8.2 Possuir memória cache de 18 MB ou superior;

11.8.3 Possuir, no mínimo, 06 (seis) núcleos físicos;

11.8.4 Não serão aceitos processadores descontinuados pelos fabricantes dos processadores;

11.8.5 Tecnologia DDR-4, 2.666 MHz ou superior;

11.8.6 Suporte à tecnologia Dual Channel;

11.8.7 08 (oito) GB de memória instalada;

11.8.8 Suporte a expansão a 128 GB de memória, sendo permitida a troca dos módulos de memória;

11.8.9 BIOS UEFI do fabricante ou desenvolvida pelo próprio fabricante do equipamento. Desenvolvida em Flash ROM, devendo permitir a atualizações por meio de software. Deverá ser desenvolvida em português ou inglês, compatível com o padrão UEFI, sendo o fabricante do computador membro da UEFI.org, comprovado através do site http://www.uefi.org/members, em qualquer categoria;

11.8.10 Possibilitar que a senha de acesso ao BIOS seja ativada e desativada via SETUP;

11.8.11 Permitir senhas de Setup para Power On e Administrador;

11.8.12 Permitir inserir registro de controle patrimonial em memória não volátil;

11.8.13 Deverá possuir campo específico com o número de série do equipamento, gravado em memória não volátil e campo não editável;

11.8.14 De fabricação própria e exclusiva para o modelo ofertado, não sendo aceitas placas utilizadas em livre comércio;

11.8.15 Possuir no mínimo 09 (nove) portas USB 3.1 ou superior, com pelo menos 2 (duas) portas USB instaladas na parte frontal do gabinete;

11.8.16 Pelo menos 01 (uma) das portas USB 3.1 solicitadas no item anterior deverá ser do Tipo C da geração 2 ou superior;

11.8.17 Não será permitida a utilização de hubs ou em adaptadores PCI;

11.8.18 Possuir, no mínimo, 01 (um) slot padrão PCI Express x16 na versão 3.0, 02 (dois) slots padrão PCI Express x1 na versão 3.0 e mais um slot PCI Express M.2;

11.8.19 O chipset deve ser da mesma marca do fabricante do processador.
11.8.20 Mínimo 4 (quatro) slots para memória tipo DDR4, permitindo a instalação de até 128 (cento e vinte e oito) Gigabytes;
11.8.21 Sistema de detecção de intrusão de chassis, com acionador instalado no gabinete que permita a detecção de abertura ainda que o equipamento esteja desligado da fonte de energia;
11.8.22 Controladora SATA 3 ou versão superior, integrada e compatível com os periféricos adiante especificados;
11.8.23 Regulagem da velocidade de rotação do cooler da CPU de forma automática, de acordo com a variação de temperatura da CPU;
11.8.24 Suportar o inventário remoto de hardware, assumindo-se que o equipamento possa estar desligado, porém energizado pela rede elétrica e conectado localmente a rede de dados.
11.8.25 Disco sólido (SSD) padrão M.2 com capacidade mínima de armazenamento de no mínimo 512GB GB;
11.8.26 Velocidade de leitura sequencial de no mínimo, 1600 MB/s e de escrita sequencial de, no mínimo, 400 MB/s;
11.8.27 Suporte às tecnologias S.M.A.R.T (Self-Monitoring, Analysis and Reporting Technology) e NCQ (Native Command Queuing).
11.8.28 Em conformidade com o padrão 802.3;
11.8.29 Suporte aos protocolos WOL e PXE;
11.8.30 Operar a 10/100/1000 Mbps, com reconhecimento automático da velocidade da rede;
11.8.31 Capacidade de operar no modo full-duplex;
11.8.32 Conector RJ-45 fêmea.
11.8.33 Controladora de vídeo integrada ao processador com capacidade de 2GB de memória, ou superior, compartilhada dinamicamente;
11.8.34 Suporte à resolução mínima de 1920 x 1080 @ 60 Hz;
11.8.35 Possuir 03 (três) conectores de vídeo digital Display Port ou HDMI;
11.8.36 Suporte a DirectX 12 e OpenGL 4.5;
11.8.37 Suporte a 03 monitores simultaneamente.
11.8.38 Controladora de Áudio High Definition Integrada à placa mãe;
11.8.39 Conectores frontais para Headphone e microfone sendo aceita interface tipo combo;
11.8.40 Alto-falante integrado ao gabinete ou placa mãe;
11.8.41 Gabinete do tipo SFF (Small Form Factor);
11.8.42 Deve permitir a abertura do gabinete sem utilização de ferramentas (tool less), de forma a possibilitar a troca de componentes como discos de armazenamento e memória. Não serão aceitas quaisquer adaptações sobre o gabinete original do fabricante do equipamento;
11.8.43 Deve possuir alto-falante integrado, com capacidade de reproduzir os sons gerados pelo sistema operacional e alarmes gerados por problemas de inicialização. Não serão aceitas adaptações;
11.8.44 Possuir, pelo menos, 02 (duas) baias internas, podendo ser uma de 2,5 polegadas e uma de 3,5 polegadas, ou 02 (duas) de 3,5 polegadas ou 02 (duas) de 2,5 polegadas;
11.8.45 Fonte de alimentação interna ao gabinete, devendo ser do mesmo fabricante do equipamento, com tensão de entrada 110/220 VAC, com potência dimensionada para suportar a configuração máxima do equipamento, com eficiência mínima de 90%, em 50% de carga;
11.8.46 A fonte de alimentação deverá possuir certificação 80PLUS;
11.8.47 O cabo de força deverá estar de acordo com a exigência da nova norma do INMETRO NBR 14136;

11.8.48 Deve possuir sensor de intrusão integrado ao gabinete;

11.8.49 O gabinete deve permitir a utilização na posição horizontal e vertical sem comprometer os componentes internos e o funcionamento do computador, de forma segura através de base antiderrapante para ambas as orientações, integradas ao gabinete ou através de base original do fabricante do microcomputador quando utilizado na posição vertical;

11.8.50 Deve possibilitar a instalação de cadeado ou lacre de segurança em slot ou trava externa específica de forma a impedir a abertura do gabinete;

11.8.51 Teclado Padrão ABNT-II, com conector USB com teclas de Iniciar e de Atalho do MS – Windows;

11.8.52 Cabo para conexão do teclado ao microcomputador com, no mínimo, 1,5m;

11.8.53 A impressão sobre as teclas deverá ser do tipo permanente, não podendo apresentar desgaste por abrasão ou uso prolongado;

11.8.54 O teclado deverá ser do mesmo fabricante do equipamento ofertado, sendo aceito em regime de OEM.

11.8.55 O teclado deverá ser resistente a derramamento de líquidos.

11.8.56 Mouse Ótico com conector USB;

11.8.57 Dispositivo dotado com 3 botões (sendo um botão para rolagem de telas – "scroll") com resolução mínima de 1000dpi;

11.8.58 O mouse deverá ser do mesmo fabricante do equipamento ofertado, sendo aceito em regime de OEM;

11.8.59 Monitor LED com área de no mínimo 21,5 polegadas na diagonal. Brilho de no mínimo 250 cd/m2. Pixel Pitch de no máximo 0,275 mm (ou menor). Contraste mínimo: estático 1000:1 ou dinâmico 15000:1. Deverá possui resolução nativa de 1920x1080 ou superior. No mínimo 16 milhões de cores.

11.8.60 No mínimo os seguintes ajustes de imagem: Contraste, Brilho, Posição (Ver cal e Horizontal), Autoajuste, Reset (Geometria / Cor), Ajuste de imagem (fino e grosseiro) e Posição (H/V), ajuste de imagem (fino e grosso) e posição (H/V). Deverá acompanhar software que permita realizar estes ajustes através do computador.

11.8.61 Compatível com padrão Energy Star.

11.8.62 Os cabos de comunicação do monitor com o microcomputador deverão ser fornecidos junto com o equipamento.

11.8.63 O monitor deverá ser do mesmo fabricante do equipamento ou aceito em regime de OEM e possuir a mesma tonalidade do gabinete (cor).

11.8.64 Acompanhar licença de sistema operacional Microsoft Windows 10 Pro 64bits, em português do Brasil (PT-BR);

11.8.65 O sistema operacional deve estar pré-instalado, bem como, todos os drivers de dispositivos internos, necessários para seu funcionamento;

11.8.66 O fabricante deve disponibilizar no seu respectivo web site, download gratuito de todos os Drivers de dispositivos, para o microcomputador ofertado, na versão mais atual para download.

11.8.67 Sistema de localização de equipamentos ou serviço em caso de roubo ou perda. O computador deve incluir um componente persistente que não pode ser apagado no BIOS, mesmo que o firmware do dispositivo seja formatado ou o disco rígido seja substituído. Gerenciado e instalado a partir de um console virtual com validade de X anos, a partir da entrega ao cliente ou a mesma validade da garantia ou validade do contrato. Deve incluir as seguintes funcionalidades:

11.8.67.1 Segurança de dados e dispositivos;

11.8.67.2 Limpe remotamente dados confidenciais em dispositivos comprometidos;

11.8.67.3 Construir uma trilha de auditoria de arquivos excluídos para demonstrar a conformidade;

11.8.67.4 Funcionalidade de apagamento seguro e permanente;

11.8.67.5 Congelar um dispositivo e enviar uma mensagem ao usuário;

11.8.67.6 Recupere arquivos remotamente de um dispositivo, independentemente do usuário ou local;

11.8.67.7 Funcionalidade de bloqueio de dispositivos online e ofline. O sistema deve ter a capacidade de configurar políticas de bloqueio ofline que permitem que o dispositivo congele se o dispositivo não se conectar à Internet após 4 dias;

11.8.67.8 Gestão de ativos;

11.8.67.9 Administração centralizada a partir de um único console de onde você pode enviar comandos para dispositivos remotamente;

11.8.67.10 Rastreamento completo de dispositivos e softwares dentro e fora da rede local;

11.8.67.11 Coletar informações precisas e completas sobre cada dispositivo em qualquer um dos componentes de hardware, software ou geolocalização;

11.8.67.12 Configuração de políticas e alertas para receber uma notificação quando for detectada uma alteração em algum dos componentes;

11.8.67.13 Deve incluir informações de propriedade, identificação do usuário, localização física, dados de hardware e software, status de antivírus e status de criptografia, bem como atualizações do sistema operacional;

11.8.67.14 Localização e rastreamento do dispositivo;

11.8.67.15 Banco de dados autorizado pelo Google Maps Wi-Fi;

11.8.67.16 Rastreamento de dispositivos em um mapa digital que inclui localização histórica e atual;

11.8.67.17 Investigar e determinar o status do dispositivo com base em sua localização física;

11.8.67.18 Criação de geofences (limites georreferenciados) para determinar o uso autorizado de cada dispositivo;

11.8.68 O sistema de proteção de endpoint deverá ser composto por um conjunto de módulos de software integrados por um único fabricante de forma a atender ao conjunto de requisitos técnicos exigidos nessa especificação;

11.8.69 Devido ao progresso de ataques a dispositivos e regulamentações nacionais e internacionais, far-se-á necessária o fornecimento de módulo de detecção e resposta de endpoints, coletando, inspecionando e centralizando as informações importantes que acontecem em tempo real, para que, a qualquer momento, mesmo após a ocorrência de um incidente de segurança, a equipe técnica do contratante possa investigar a causa raiz e responder/mitigar o impacto com o máximo de informações possíveis remediando os endpoints da rede corporativa por ventura comprometidos com maior rapidez

11.8.70 Deve suportar a integração de forma nativa com gerência centralizada da solução de segurança, para trabalhar de forma harmônica e sincronizada com os demais componentes.

11.8.71 Deve ser entregue com o gerenciamento do sistema ofertado baseado em modelo de nuvem computacional;

11.8.72 Deverá implementar mecanismo de descoberta de ameaças cibernéticas baseado em análise de inteligência artificial permitindo a coleta de dados dos endpoints e seu armazenamento centralizado em console de gerência em ambiente de nuvem (SaaS).

11.8.73 Todos os módulos de software de proteção do sistema ofertado deverão atender às especificações técnicas descritas neste documento em sua integralidade.

11.8.74 A console de gerência do software de proteção deverá ser centralizada com interface gráfica web e deverá prover mecanismo que permita a instalação inicial de agentes de segurança nos endpoints pelos administradores de forma silenciosa.

11.8.75 A gerência centralizada deverá permitir a distribuição de atualizações nos módulos de Next Generation antivírus em execução nos agentes de segurança.

11.8.76 Deve prover detecção e prevenção de ameaças em real-time;

11.8.77 O funcionamento da solução deve operar analisando a pré-execuçao e pós-execução da ameaça em potencial, em nível de sistema operacional (O/S), memória e prevenindo a entrada de códigos maliciosos.

11.8.78 Capacidade de análise automática do código do arquivo, identificando suas características antes da sua capacidade de execução.

11.8.79 A solução deve aplicar análise baseada em código algoritmo, para identificar programas maliciosos antes da sua execução.

11.8.80 Caso seja encontrado um programa malicioso a sua execução não deve ser permitida.

11.8.81 A solução deve identificar e bloquear a execução de códigos executáveis, scripts ou comandos.

11.8.82 A solução de endpoint deve prevenir e detectar qualquer alteração oriunda de código malicioso em programas que sejam executados em memória.

11.8.83 Deve utilizar a tecnologia de "Machine Learning" para identificar qualquer ameaça nos arquivos potencialmente perigosos.

11.8.84 Caso necessário a solução deve ter a capacidade de encaminhar arquivos identificados como ameaças para uma solução de "Sandbox On-premises ou On-Cloud", com o objetivo de fazer uma segunda análise em diferentes sistemas operacionais.

11.8.85 Identificar ameaças avançadas, chamadas de "Zero-day", sem a necessidade de base de assinaturas (DATs) e suas atualizações, detecção por heurística, detecção por comportamento ou sandboxing.

11.8.86 Deve permitir controlar dispositivos de conectados via USB, permitindo bloquear ou liberar acesso e adicionalmente criação de exceções na política, pelo número de série, identificador do fabricante e tipo de dispositivo.

11.8.87 Deve ter a capacidade de detectar e controlar no mínimo os seguintes dispositivos USB;

11.8.88 Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado no cliente instalados nas estações de trabalho;

11.8.89 Possuir base contendo, no mínimo, 20 milhões de sites internet web já registrados e classificados com atualização automática;

11.8.90 Deve atuar como filtro de conteúdo transparente de forma a dispensar a configuração dos browsers das máquinas clientes;

11.8.91 Permitir a criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra) ;

11.8.92 Permitir proteger os acessos a sites categorizados maliciosos e possuir no mínimo 50 categorias de URLs;

11.8.93 Suporta a exclusão ou inclusão de URLs do bloqueio, por categoria;

11.8.94 Deverá possibilitar a categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente, utilizando-se ferramenta do próprio fabricante;

11.8.95 A solução deverá permitir um mecanismo que permita criar whitelist ou blacklist de URLs;

11.8.96 A solução não deve depender de base de assinaturas para a identificação de qualquer ameaças.

11.8.97 A solução deve sempre manter o monitoramento contínuo e ativo no endpoint para remover a necessidade de escaneamentos periódicos, baseando – se na análise comportamental dos arquivos.

11.8.98 Deve prover proteção em real-time, independente do estado de conexão da máquina;

11.8.99 O módulo de controle e análise de scripts deve ser capaz de analisar no mínimo scripts em powershell, macros ou VBA.

11.8.100 O módulo de controle e análise de scripts deve possuir as seguintes ações em caso se violação;

11.9. ESTAÇÃO DE TRABALHO DO TIPO DESKTOP COMPACTO TIPO 2

11.9.1 Processador com frequência mínima de 2,10 Ghz baseada em processador;

11.9.2 Possuir memória cache de 25 MB ou superior;

11.9.3 Possuir, no mínimo, 12 (doze) núcleos físicos;

11.9.4 Não serão aceitos processadores descontinuados pelos fabricantes dos processadores;

11.9.5 Tecnologia DDR-4, 2.666 MHz ou superior;

11.9.6 Suporte à tecnologia Dual Channel;

11.9.7 16 (dezeseis) GB de memória instalada;

11.9.8 Suporte a expansão a 128 GB de memória, sendo permitida a troca dos módulos de memória;

11.9.9 BIOS UEFI do fabricante ou desenvolvida pelo próprio fabricante do equipamento. Desenvolvida em Flash ROM, devendo permitir a atualizações por meio de software. Deverá ser desenvolvida em português ou inglês, compatível com o padrão UEFI, sendo o fabricante do computador membro da UEFI.org, comprovado através do site http://www.uefi.org/members, em qualquer categoria;

11.9.10 Possibilitar que a senha de acesso ao BIOS seja ativada e desativada via SETUP;

11.9.11 Permitir senhas de Setup para Power On e Administrador;

11.9.12 Permitir inserir registro de controle patrimonial em memória não volátil;

11.9.13 Deverá possuir campo específico com o número de série do equipamento, gravado em memória não volátil e campo não editável;

11.9.14 De fabricação própria e exclusiva para o modelo ofertado, não sendo aceitas placas utilizadas em livre comércio;

11.9.15 Possuir no mínimo 09 (nove) portas USB 3.1 ou superior, com pelo menos 2 (duas) portas USB instaladas na parte frontal do gabinete;

11.9.16 Pelo menos 01 (uma) das portas USB 3.1 solicitadas no item anterior deverá ser do Tipo C da geração 2 ou superior;

11.9.17 Não será permitida a utilização de hubs ou em adaptadores PCI;

11.9.18 Possuir, no mínimo, 01 (um) slot padrão PCI Express x16 na versão 3.0, 02 (dois) slots padrão PCI Express x1 na versão 3.0 e mais um slot PCI Express M.2;

11.9.19 O chipset deve ser da mesma marca do fabricante do processador.

11.9.20 Mínimo 4 (quatro) slots para memória tipo DDR4, permitindo a instalação de até 128 (cento e vinte e oito) Gigabytes;

11.9.21 Sistema de detecção de intrusão de chassis, com acionador instalado no gabinete que permita a detecção de abertura ainda que o equipamento esteja desligado da fonte de energia;

11.9.22 Controladora SATA 3 ou versão superior, integrada e compatível com os periféricos adiante especificados;

11.9.23 Regulagem da velocidade de rotação do cooler da CPU de forma automática, de acordo com a variação de temperatura da CPU;

11.9.24 Suportar o inventário remoto de hardware, assumindo-se que o equipamento possa estar desligado, porém energizado pela rede elétrica e conectado localmente a rede de dados.

11.9.25 Disco sólido (SSD) padrão M.2 com capacidade mínima de armazenamento de no mínimo 512GB GB;

11.9.26 Velocidade de leitura sequencial de no mínimo, 1600 MB/s e de escrita sequencial de, no mínimo, 400 MB/s;

11.9.27 Suporte às tecnologias S.M.A.R.T (Self-Monitoring, Analysis and Reporting Technology) e NCQ (Native Command Queuing).

11.9.28 Em conformidade com o padrão 802.3;

11.9.29 Suporte aos protocolos WOL e PXE;

11.9.30 Operar a 10/100/1000 Mbps, com reconhecimento automático da velocidade da rede;

11.9.31 Capacidade de operar no modo full-duplex;

11.9.32 Conector RJ-45 fêmea.

11.9.33 Controladora de vídeo integrada ao processador com capacidade de 2GB de memória, ou superior, compartilhada dinamicamente;

11.9.34 Suporte à resolução mínima de 1920 x 1080 @ 60 Hz;

11.9.35 Possuir 03 (três) conectores de vídeo digital Display Port ou HDMI;

11.9.36 Suporte a DirectX 12 e OpenGL 4.5;

11.9.37 Suporte a 03 monitores simultaneamente.

11.9.38 Controladora de Áudio High Definition Integrada à placa mãe;

11.9.39 Conectores frontais para Headphone e microfone sendo aceita interface tipo combo;

11.9.40 Alto-falante integrado ao gabinete ou placa mãe;

11.9.41 Gabinete do tipo SFF (Small Form Factor);

11.9.42 Deve permitir a abertura do gabinete sem utilização de ferramentas (tool less), de forma a possibilitar a troca de componentes como discos de armazenamento e memória. Não serão aceitas quaisquer adaptações sobre o gabinete original do fabricante do equipamento;

11.9.43 Deve possuir alto-falante integrado, com capacidade de reproduzir os sons gerados pelo sistema operacional e alarmes gerados por problemas de inicialização. Não serão aceitas adaptações;

11.9.44 Possuir, pelo menos, 02 (duas) baias internas, podendo ser uma de 2,5 polegadas e uma de 3,5 polegadas, ou 02 (duas) de 3,5 polegadas ou 02 (duas) de 2,5 polegadas;

11.9.45 Fonte de alimentação interna ao gabinete, devendo ser do mesmo fabricante do equipamento, com tensão de entrada 110/220 VAC, com potência dimensionada para suportar a configuração máxima do equipamento, com eficiência mínima de 90%, em 50% de carga;

11.9.46 A fonte de alimentação deverá possuir certificação 80PLUS;

11.9.47 O cabo de força deverá estar de acordo com a exigência da nova norma do INMETRO NBR 14136;

11.9.48 Deve possuir sensor de intrusão integrado ao gabinete;

11.9.49 O gabinete deve permitir a utilização na posição horizontal e vertical sem comprometer os componentes internos e o funcionamento do computador, de forma segura através de base antiderrapante para ambas as orientações, integradas ao gabinete ou através de base original do fabricante do microcomputador quando utilizado na posição vertical;

11.9.50 Deve possibilitar a instalação de cadeado ou lacre de segurança em slot ou trava externa específica de forma a impedir a abertura do gabinete;

11.9.51 Teclado Padrão ABNT-II, com conector USB com teclas de Iniciar e de Atalho do MS – Windows;

11.9.52 Cabo para conexão do teclado ao microcomputador com, no mínimo, 1,5m;

11.9.53 A impressão sobre as teclas deverá ser do tipo permanente, não podendo apresentar desgaste por abrasão ou uso prolongado;

11.9.54 O teclado deverá ser do mesmo fabricante do equipamento ofertado, sendo aceito em regime de OEM.

11.9.55 O teclado deverá ser resistente a derramamento de líquidos.

11.9.56 Mouse Ótico com conector USB;

11.9.57 Dispositivo dotado com 3 botões (sendo um botão para rolagem de telas – "scroll") com resolução mínima de 1000dpi;

11.9.58 O mouse deverá ser do mesmo fabricante do equipamento ofertado, sendo aceito em regime de OEM;

11.9.59 Monitor LED com área de no mínimo 21,5 polegadas na diagonal. Brilho de no mínimo 250 cd/m2. Pixel Pitch de no máximo 0,275 mm (ou menor). Contraste mínimo: estático 1000:1 ou dinâmico 15000:1. Deverá possui resolução nativa de 1920x1080 ou superior. No mínimo 16 milhões de cores.

11.9.60 No mínimo os seguintes ajustes de imagem: Contraste, Brilho, Posição (Ver cal e Horizontal), Autoajuste, Reset (Geometria / Cor), Ajuste de imagem (fino e grosseiro) e Posição (H/V), ajuste de imagem (fino e grosso) e posição (H/V). Deverá acompanhar software que permita realizar estes ajustes através do computador.

11.9.61 Compatível com padrão Energy Star.

11.9.62 Os cabos de comunicação do monitor com o microcomputador deverão ser fornecidos junto com o equipamento.

11.9.63 O monitor deverá ser do mesmo fabricante do equipamento ou aceito em regime de OEM e possuir a mesma tonalidade do gabinete (cor).

11.9.64 Acompanhar licença de sistema operacional Microsoft Windows 11 Pro 64bits, em português do Brasil (PT-BR);

11.9.65 O sistema operacional deve estar pré-instalado, bem como, todos os drivers de dispositivos internos, necessários para seu funcionamento;

11.9.66 O fabricante deve disponibilizar no seu respectivo web site, download gratuito de todos os Drivers de dispositivos, para o microcomputador ofertado, na versão mais atual para download.

11.9.67 Sistema de localização de equipamentos ou serviço em caso de roubo ou perda. O computador deve incluir um componente persistente que não pode ser apagado no BIOS, mesmo que o firmware do dispositivo seja formatado ou o disco rígido seja substituído. Gerenciado e instalado a partir de um console virtual com validade de X anos, a partir da entrega ao cliente ou a mesma validade da garantia ou validade do contrato. Deve incluir as seguintes funcionalidades:

- 11.9.67.1 Segurança de dados e dispositivos;
- 11.9.67.2 Limpe remotamente dados confidenciais em dispositivos comprometidos;
- 11.9.67.3 Construir uma trilha de auditoria de arquivos excluídos para demonstrar a conformidade;
- 11.9.67.4 Funcionalidade de apagamento seguro e permanente;
- 11.9.67.5 Congelar um dispositivo e enviar uma mensagem ao usuário;
- 11.9.67.6 Recupere arquivos remotamente de um dispositivo, independentemente do usuário ou local;
- 11.9.67.7 Funcionalidade de bloqueio de dispositivos online e offline. O sistema deve ter a capacidade de configurar políticas de bloqueio offline que permitem que o dispositivo congele se o dispositivo não se conectar à Internet após 4 dias;
- 11.9.67.8 Gestão de ativos;

11.9.67.9 Administração centralizada a partir de um único console de onde você pode enviar comandos para dispositivos remotamente;

11.9.67.10 Rastreamento completo de dispositivos e softwares dentro e fora da rede local;

11.9.67.11 Coletar informações precisas e completas sobre cada dispositivo em qualquer um dos componentes de hardware, software ou geolocalização;

11.9.67.12 Configuração de políticas e alertas para receber uma notificação quando for detectada uma alteração em algum dos componentes;

11.9.67.13 Deve incluir informações de propriedade, identificação do usuário, localização física, dados de hardware e software, status de antivírus e status de criptografia, bem como atualizações do sistema operacional;

11.9.67.14 Localização e rastreamento do dispositivo;

11.9.67.15 Banco de dados autorizado pelo Google Maps Wi-Fi;

11.9.67.16 Rastreamento de dispositivos em um mapa digital que inclui localização histórica e atual;

11.9.67.17 Investigar e determinar o status do dispositivo com base em sua localização física;

11.9.67.18 Criação de geofences (limites georreferenciados) para determinar o uso autorizado de cada dispositivo;

11.9.68 O sistema de proteção de endpoint deverá ser composto por um conjunto de módulos de software integrados por um único fabricante de forma a atender ao conjunto de requisitos técnicos exigidos nessa especificação;

11.9.69 Devido ao progresso de ataques a dispositivos e regulamentações nacionais e internacionais, far-se-á necessária o fornecimento de módulo de detecção e resposta de endpoints, coletando, inspecionando e centralizando as informações importantes que acontecem em tempo real, para que, a qualquer momento, mesmo após a ocorrência de um incidente de segurança, a equipe técnica do contratante possa investigar a causa raiz e responder/mitigar o impacto com o máximo de informações possíveis remediando os endpoints da rede corporativa por ventura comprometidos com maior rapidez

11.9.70 Deve suportar a integração de forma nativa com gerência centralizada da solução de segurança, para trabalhar de forma harmônica e sincronizada com os demais componentes.

11.9.71 Deve ser entregue com o gerenciamento do sistema ofertado baseado em modelo de nuvem computacional;

11.9.72 Deverá implementar mecanismo de descoberta de ameaças cibernéticas baseado em análise de inteligência artificial permitindo a coleta de dados dos endpoints e seu armazenamento centralizado em console de gerência em ambiente de nuvem (SaaS).

11.9.73 Todos os módulos de software de proteção do sistema ofertado deverão atender às especificações técnicas descritas neste documento em sua integralidade.

11.9.74 A console de gerência do software de proteção deverá ser centralizada com interface gráfica web e deverá prover mecanismo que permita a instalação inicial de agentes de segurança nos endpoints pelos administradores de forma silenciosa.

11.9.75 A gerência centralizada deverá permitir a distribuição de atualizações nos módulos de Next Generation antivírus em execução nos agentes de segurança.

11.9.76 Deve prover detecção e prevenção de ameaças em real-time;

11.9.77 O funcionamento da solução deve operar analisando a pré-execuçao e pós-execução da ameaça em potencial, em nível de sistema operacional (O/S), memória e prevenindo a entrada de códigos maliciosos.

11.9.78 Capacidade de análise automática do código do arquivo, identificando suas características antes da sua capacidade de execução.

11.9.79 A solução deve aplicar análise baseada em código algoritmo, para identificar programas maliciosos antes da sua execução.

11.9.80 Caso seja encontrado um programa malicioso a sua execução não deve ser permitida.

11.9.81 A solução deve identificar e bloquear a execução de códigos executáveis, scripts ou comandos.

11.9.82 A solução de endpoint deve prevenir e detectar qualquer alteração oriunda de código malicioso em programas que sejam executados em memória.

11.9.83 Deve utilizar a tecnologia de "Machine Learning" para identificar qualquer ameaça nos arquivos potencialmente perigosos.

11.9.84 Caso necessário a solução deve ter a capacidade de encaminhar arquivos identificados como ameaças para uma solução de "Sandbox On-premises ou On-Cloud", com o objetivo de fazer uma segunda análise em diferentes sistemas operacionais.

11.9.85 Identificar ameaças avançadas, chamadas de "Zero-day", sem a necessidade de base de assinaturas (DATs) e suas atualizações, detecção por heurística, detecção por comportamento ou sandboxing.

11.9.86 Deve permitir controlar dispositivos de conectados via USB, permitindo bloquear ou liberar acesso e adicionalmente criação de exceções na política, pelo número de série, identificador do fabricante e tipo de dispositivo.

11.9.87 Deve ter a capacidade de detectar e controlar no mínimo os seguintes dispositivos USB;

11.9.88 Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado no cliente instalados nas estações de trabalho;

11.9.89 Possuir base contendo, no mínimo, 20 milhões de sites internet web já registrados e classificados com atualização automática;

11.9.90 Deve atuar como filtro de conteúdo transparente de forma a dispensar a configuração dos browsers das máquinas clientes;

11.9.91 Permitir a criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra) ;

11.9.92 Permitir proteger os acessos a sites categorizados maliciosos e possuir no mínimo 50 categorias de URLs;

11.9.93 Suporta a exclusão ou inclusão de URLs do bloqueio, por categoria;

11.9.94 Deverá possibilitar a categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente, utilizando-se ferramenta do próprio fabricante;

11.9.95 A solução deverá permitir um mecanismo que permita criar whitelist ou blacklist de URLs;

11.9.96 A solução não deve depender de base de assinaturas para a identificação de qualquer ameaças.

11.9.97 A solução deve sempre manter o monitoramento contínuo e ativo no endpoint para remover a necessidade de escaneamentos periódicos, baseando – se na análise comportamental dos arquivos.

11.9.98 Deve prover proteção em real-time, independente do estado de conexão da máquina;

11.9.99 O módulo de controle e análise de scripts deve ser capaz de analisar no mínimo scripts em powershell, macros ou VBA.

11.9.100 O módulo de controle e análise de scripts deve possuir as seguintes ações em caso se violação;

11.10. NOTEBOOK COM TELA DE 14"

11.10.1 Processador com arquitetura mínima de 10 núcleos físicos e 12 threads;
11.10.2 Memória cache integrada de, no mínimo, 12 MB;
11.10.3 Frequência de clock base de, no mínimo, 1,70 GHz, baseada em processador;
11.10.4 Tela com 14" polegadas de área visível com tecnologia LED e tratamento anti-reflexo;
11.10.5 Resolução gráfica de no mínimo 1920x1080 pixels;
11.10.6 Controladora de vídeo com capacidade para controlar 02 (dois) monitores simultaneamente e permitir a extensão da tela do notebook, com no mínimo mais um monitor conectado na interface digital, podendo ser HDMI ou Display Port;
11.10.7 A controladora deverá possuir compatibilidade com a tecnologia DirectX 12 e OpenGL 4.5.
11.10.8 Possuir 2x slots de memória RAM tipo DDR4 3200Mhz;
11.10.9 Possuir no mínimo 16 GB de memória RAM;
11.10.10 O tamanho total de memória RAM suportado pelo equipamento deve ser de, no mínimo, 32 GB;
11.10.11 Disco sólido (SSD) padrão SATA ou M.2 com capacidade mínima de armazenamento de no mínimo 512 GB;
11.10.12 Velocidade de leitura sequencial de, no mínimo, 2.000 MB/s e de escrita sequencial de, no mínimo, 1.300 MB/s;
11.10.13 Deve possuir a tecnologia S.M.A.R.T (Self-Monitoring, Analysis and Reporting Technology);
11.10.14 O chipset deve ser da mesma marca do processador ou integrado com tecnologia SoC (System on a Chip);
11.10.15 Possuir, no mínimo, 3 slots M.2, sendo 1 no padrão M.2 2230 para WiFi e 2 no padrão M.2 2242 para SSD;
11.10.16 Regulagem da velocidade de rotação do cooler da CPU de forma automática, de acordo com a variação de temperatura da CPU;
11.10.17 Suportar boot por pen drive ou disco conectado a uma porta USB 3.2 ou superior;
11.10.18 Tipo Flash Memory, utilizando memória não volátil e reprogramável, e compatível com os padrões ACPI 3.0 e Plug-and-Play;
11.10.19 Lançada a partir de 2022 e entregue na versão mais atual disponibilizada pelo fabricante;
11.10.20 Possuir senhas de Setup para Power On e Administrador;
11.10.21 Permitir a inserção de código de identificação do equipamento dentro da própria BIOS (número do patrimônio e número de série). Serão aceitas BIOS com reprogramação via software desde que estes estejam devidamente licenciados para o equipamento e constantes para download no website do fabricante.
11.10.22 Controladora de rede, integrada à placa mãe com velocidade de 10/100/1000 Mbits/s, padrões Ethernet, Fast-Ethernet e Gigabit Ethernet, autosense, full-duplex, plug-and-play, configurável totalmente por software, com conector padrão RJ-45;
11.10.23 Controladora de rede sem fio, dual band, padrão 802.11 ax;
11.10.24 Possuir interface Bluetooth, no padrão 5.1 ou superior;
11.10.25 Não serão aceitas nenhuma das interfaces ou controladoras de rede acima descritas, ofertadas via conectores USB ou PCMCIA.
11.10.26 Todos os conectores das portas de entrada/saída devem ser identificados pelos nomes ou respectivos símbolos;
11.10.27 Possuir, no mínimo, 3 (três) interfaces USB integradas, sendo pelo menos 1 (uma) interface USB padrão 3.2Gen 2;
11.10.28 Pelo menos 1 (uma) das interfaces USB 3.2Gen 2 deverá ser do tipo "Type C" e suportar o carregamento da bateria do equipamento;

11.10.29 Possuir, no mínimo, 01 (uma) interface HDMI;
11.10.30 Possuir interface de áudio para microfone e fone de ouvido, podendo ser uma única entrada do tipo combo;
11.10.31 Possuir câmera integrada com resolução mínima de 720p;
11.10.32 Possuir alto falantes integrados;
11.10.33 Placa de vídeo integrada;
11.10.34 O gabinete deverá ter estrutura robusta, revestido em composto de carbono, liga de magnésio, alumínio, titânio ou fibra de vidro, para proteção contra impactos e acabamento de alta resistência para maior durabilidade;
11.10.35 Deve possuir Botão liga/desliga e led indicador do computador ligado (Power-on);
11.10.36 O chassi deve possuir espessura máxima de 19mm;
11.10.37 Possuir teclado integrado ao gabinete do notebook compatível com o padrão ABNT-2, com no mínimo 85 teclas, alfanumérico, com 12 teclas de função;
11.10.38 A impressão sobre as teclas deverá ser do tipo permanente, não podendo apresentar desgastes por abrasão ou por uso prolongado;
11.10.39 O teclado deve ser do tipo retro iluminado com função de ajuste da intensidade da iluminação;
11.10.40 O teclado deve suportar o derramamento acidental de líquidos.
11.10.41 Deverá ser fornecida 01 (uma) fonte de alimentação com faixa de tensão de entrada de 100VAC a 240VAC automática, e frequência de 50-60 Hz.
11.10.42 Possuir mouse integrado ao gabinete do notebook;
11.10.43 Mouse tipo Touchpad;
11.10.44 Mouse com 2 botões ou click pad para seleção de objetos;
11.10.45 O Touchpad deve suportar multitoques.
11.10.46 Deverá ser fornecida 01 (uma) bateria primária de Íons de Lítio ou Lítio Polímero, com autonomia (descarga) mínima de 600 (seiscentos) minutos.
11.10.47 Possuir entrada para cabo de segurança integrada ao gabinete;
11.10.48 Possuir leitor de impressões digitais.
11.10.49 Acompanhar licença de sistema operacional Microsoft Windows 10 Pro 64bits, em português do Brasil (PT-BR);
11.10.50 O sistema operacional deve estar pré-instalado, bem como, todos os drivers de dispositivos internos, necessários para seu funcionamento;
11.10.51 O fabricante deve disponibilizar no seu respectivo web site, download gratuito de todos os Drivers de dispositivos, para o microcomputador ofertado, na versão mais atual para download.
11.10.52 Sistema de localização de equipamentos ou serviço em caso de roubo ou perda. O computador deve incluir um componente persistente que não pode ser apagado no BIOS, mesmo que o firmware do dispositivo seja formatado ou o disco rígido seja substituído. Gerenciado e instalado a partir de um console virtual com validade de X anos, a partir da entrega ao cliente ou a mesma validade da garantia ou validade do contrato. Deve incluir as seguintes funcionalidades:
11.10.52.1 Segurança de dados e dispositivos;
11.10.52.2 Limpe remotamente dados confidenciais em dispositivos comprometidos;
11.10.52.3 Construir uma trilha de auditoria de arquivos excluídos para demonstrar a conformidade;
11.10.52.4 Funcionalidade de apagamento seguro e permanente;
11.10.52.5 Congelar um dispositivo e enviar uma mensagem ao usuário;
11.10.52.6 Recupere arquivos remotamente de um dispositivo, independentemente do usuário ou local;

11.10.52.7 Funcionalidade de bloqueio de dispositivos online e ofline. O sistema deve ter a capacidade de configurar políticas de bloqueio ofline que permitem que o dispositivo congele se o dispositivo não se conectar à Internet após 4 dias;

11.10.52.8 Gestão de ativos;

11.10.52.9 Administração centralizada a partir de um único console de onde você pode enviar comandos para dispositivos remotamente;

11.10.52.10 Rastreamento completo de dispositivos e softwares dentro e fora da rede local;

11.10.52.11 Coletar informações precisas e completas sobre cada dispositivo em qualquer um dos componentes de hardware, software ou geolocalização;

11.10.52.12 Configuração de políticas e alertas para receber uma notificação quando for detectada uma alteração em algum dos componentes;

11.10.52.13 Deve incluir informações de propriedade, identificação do usuário, localização física, dados de hardware e software, status de antivírus e status de criptografia, bem como atualizações do sistema operacional;

11.10.52.14 Localização e rastreamento do dispositivo;

11.10.52.15 Banco de dados autorizado pelo Google Maps Wi-Fi;

11.10.52.16 Rastreamento de dispositivos em um mapa digital que inclui localização histórica e atual;

11.10.52.17 Investigar e determinar o status do dispositivo com base em sua localização física;

11.10.52.18 Criação de geofences (limites georreferenciados) para determinar o uso autorizado de cada dispositivo;

11.10.53 O sistema de proteção de endpoint deverá ser composto por um conjunto de módulos de software integrados por um único fabricante de forma a atender ao conjunto de requisitos técnicos exigidos nessa especificação;

11.10.54 Devido ao progresso de ataques a dispositivos e regulamentações nacionais e internacionais, far-se-á necessária o fornecimento de módulo de detecção e resposta de endpoints, coletando, inspecionando e centralizando as informações importantes que acontecem em tempo real, para que, a qualquer momento, mesmo após a ocorrência de um incidente de segurança, a equipe técnica do contratante possa investigar a causa raiz e responder/mitigar o impacto com o máximo de informações possíveis remediando os endpoints da rede corporativa por ventura comprometidos com maior rapidez

11.10.55 Deve suportar a integração de forma nativa com gerência centralizada da solução de segurança, para trabalhar de forma harmônica e sincronizada com os demais componentes.

11.10.56 Deve ser entregue com o gerenciamento do sistema ofertado baseado em modelo de nuvem computacional;

11.10.57 Deverá implementar mecanismo de descoberta de ameaças cibernéticas baseado em análise de inteligência artificial permitindo a coleta de dados dos endpoints e seu armazenamento centralizado em console de gerência em ambiente de nuvem (SaaS).

11.10.58 Todos os módulos de software do sistema ofertado deverão atender às especificações técnicas descritas neste documento em sua integralidade.

11.10.59 Suporte total para os seguintes sistemas operacionais Windows 7 (32 e 64 bits), Windows 8 e Windows 8.1 (32 e 64 bits), Windows Server 2008 R2 (32 e 64 bits), Windows Server 2012, Windows Server 2016;

11.10.60 A console de gerência centralizada com interface gráfica web deverá prover mecanismo que permita a instalação inicial de agentes de segurança nos endpoints pelos administradores de forma silenciosa.

11.10.61 A gerência centralizada e deverá permitir a distribuição de atualizações nos módulos de Next Generation antivírus em execução nos agentes de segurança.

11.10.62 Deve prover detecção e prevenção de ameaças em real-time;

11.10.63 O funcionamento da solução deve operar analisando a pré-execuçao e pós-execução da ameaça em potencial, em nível de sistema operacional (O/S), memória e prevenindo a entrada de códigos maliciosos.

11.10.64 Capacidade de análise automática do código do arquivo, identificando suas características antes da sua capacidade de execução.

11.10.65 A solução deve aplicar análise baseada em código algoritmo, para identificar programas maliciosos antes da sua execução.

11.10.66 Caso seja encontrado um programa malicioso a sua execução não deve ser permitida.

11.10.67 A solução deve identificar e bloquear a execução de códigos executáveis, scripts ou comandos.

11.10.68 A solução de endpoint deve prevenir e detectar qualquer alteração oriunda de código malicioso em programas que sejam executados em memória.

11.10.69 Deve utilizar a tecnologia de "Machine Learning" para identificar qualquer ameaça nos arquivos potencialmente perigosos.

11.10.70 Caso necessário a solução deve ter a capacidade de encaminhar arquivos identificados como ameaças para uma solução de "Sandbox On-premises ou On-Cloud", com o objetivo de fazer uma segunda análise em diferentes sistemas operacionais.

11.10.71 Identificar ameaças avançadas, chamadas de "Zero-day", sem a necessidade de base de assinaturas (DATs) e suas atualizações, detecção por heurística, detecção por comportamento ou sandboxing.

11.10.72 Deve permitir controlar dispositivos de conectados via USB, permitindo bloquear ou liberar acesso e adicionalmente criação de exceções na política, pelo número de série, identificador do fabricante e tipo de dispositivo.

11.10.73 Deve ter a capacidade de detectar e controlar no mínimo os seguintes dispositivos USB;

11.10.74 Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado no cliente instalados nas estações de trabalho;

11.10.75 Possuir base contendo, no mínimo, 20 milhões de sites internet web já registrados e classificados com atualização automática;

11.10.76 Deve atuar como filtro de conteúdo transparente de forma a dispensar a configuração dos browsers das máquinas clientes.

11.10.77 A plataforma deve possuir as seguintes funcionalidades de filtro de URL: Permitir a criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra), permitir proteger os acessos a sites categorizados maliciosos e possuir no mínimo 50 categorias de URLs, suportar a exclusão ou inclusão de URLs do bloqueio, por categoria, deverá possibilitar a categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente e utilizando-se ferramenta do próprio fabricante;

11.10.78 A solução deverá permitir um mecanismo que permita criar whitelist ou blacklist de URLs;

11.10.79 A solução não deve depender de base de assinaturas para a identificação de qualquer ameaças.

11.10.80 A solução deve sempre manter o monitoramento contínuo e ativo no endpoint para remover a necessidade de escaneamentos periódicos, baseando – se na análise comportamental dos arquivos.

11.10.81 Deve prover proteção em real-time, independente do estado de conexão da máquina;
11.10.82 O módulo de controle e análise de scripts deve ser capaz de analisar no mínimo scripts em powershell, macros ou VBA.
11.10.83 O módulo de controle e análise de scripts;

11.11. CÂMERA DE VIDEOCONFERÊNCIA

11.11.1 Um terminal com câmera, microfones e alto-falantes estéreo integrados, do tipo "ALL-IN-ONE";
11.11.2 Deve ser baseado em plataforma tipo appliance, não sendo permitido o uso de plataformas x86;
11.11.3 Sistema de Controle Touch Screen;
11.11.4 Todos os componentes devem ser do mesmo fabricante e deve acompanhar todos os itens para seu pleno funcionamento;
11.11.5 Ser novo e de primeiro uso, não podendo estar fora da linha comercial do fabricante, na data de entrega das propostas;
11.11.6 O fabricante da solução deve possuir suporte técnico nacional;
11.11.7 A solução deve possuir certificado ANATEL entregue junto com a proposta técnica na data do certame;
11.11.8 Não poderá ser baseado em plataforma convencional de computador;
11.11.9 Devem ser certificados para as seguintes plataformas:
11.11.10 Zoom Room Appliances, a comprovação será feita acessando o site de suporte da Zoom: https://support.zoom.us/hc/en-us/articles/360033608731-Zoom-Rooms-Certified-Hardware
11.11.11 Devem ser certificados como Microsoft Teams Room para Android, a comprovação será feita acessando o site de suporte da Microsoft: https://docs.microsoft.com/pt-br/microsoftteams/devices/teams-ip-phones
11.11.12 Deve possuir câmera integrada com as seguintes características:
11.11.13 Enquadramento automático de pessoas
11.11.14 Campo de visão mínimo de 82°
11.11.15 Zoom de no mínimo 4X
11.11.16 Resolução Ultra HD (4K)
11.11.17 Movimentação de Pan e Tilt eletrônica ou motorizada.
11.11.18 Deve possuir dispositivo mecânico para privacidade da câmera, caso não possua este dispositivo, serão aceitos dispositivos externos fabricados com materiais plásticos rígidos ou metálicos, permitindo bloqueio mecânico total da lente.
11.11.19 Deve acompanhar o suporte para montagem em parede.
11.11.20 Deve possuir entrada HDMI para compartilhamento de conteúdo.
11.11.21 Deve possuir 2 (duas) saídas HDMI 1080p para conexão com os monitores.
11.11.22 Deve suportar a operação através de televisores sensíveis ao toque, permitindo a funcionalidade de White board
11.11.23 Deve suportar conectividade através dos seguintes meios:
11.11.24 Uma porta de rede padrão Ethernet com suporte às taxas 10/100/1000Mbps, com suporte a IPv4 e IPv6 e IEEE 802.1x
11.11.25 Redes sem fio WiFi Dual Band (2,4GHz/5GHz);
11.11.26 Bluetooth
11.11.27 Deve possuir microfones integrados com a captação de no mínimo 7,6 metros, caso o sistema não suporte este alcance, deverão ser fornecidos 02 (dois) microfones de mesa com captação de 360°. No caso do fornecimento dos microfones de mesa, os

mesmos devem ser cabeados, com cabeamento de 15 metros e ser entregues os suportes de fixação na mesa.

11.11.28 O equipamento deve possuir alto falantes integrados com potência mínima de 20 Watts (RMS).

11.11.29 Caso estes alto-falantes não atinjam a potência solicitada, deverá acompanhar caixa acústica do tipo soundbar com os seguintes recursos de áudio:

11.11.30 Deve possuir no mínimo potência de 40W RMS;

11.11.31 Resposta de frequência: 90 Hz a 20 KHz;

11.11.32 Deve possuir saída de vídeo HDMI

11.11.33 Deve possui entrada de vídeo HDMI

11.11.34 Deve possuir portas de entrada óptica, Bluetooth e USB.

11.11.35 Deve Apresentar as "interfaces" para as operações e gerenciamento em, obrigatoriamente, pelo menos, 2 (duas) línguas: inglesa (Estados Unidos) e portuguesa (Brasil);

11.11.36 Deve permitir o controle das operações básicas por Sistema de Controle Touch Screen, do mesmo fabricante da solução com, no mínimo, as características abaixo:

11.11.37 Deve possuir uma interface touchscreen capacitiva de, no mínimo, 8";

11.11.38 Deve possuir interface gráfica intuitiva e amigável, para acesso, controle e configuração, com no mínimo as seguintes funcionalidades:

11.11.39 Gerenciar chamadas de vídeo;

11.11.40 Gerenciamento dos participantes conectados na plataforma de nuvem;

11.11.41 Controle de volume e mute

11.11.42 Para melhor visualização, deve permitir a montagem inclinada do painel Touch Screen entre 30° e 60°.

11.11.43 Deve suportar alimentação sobre Ethernet Standard 802.3af;

11.11.44 Deve ser fornecido com fonte de alimentação 110/220V com comutação automática;

11.11.45 Deve suportar 802.1x

11.11.46 A solução deverá possuir software de gerenciamento e configuração centralizado do mesmo fabricante da câmera, permitindo que os equipamentos sejam gerenciados e configurados remotamente.

11.11.47 Deve permitir a conectividade BYOD, ou seja, deve suportar a operação do equipamento no modo USB, permitindo que colaboradores e convidados conectem seus computadores na porta USB e HDMI para utilização dos recursos audiovisuais do equipamento de vídeo (Câmera, Microfones, alto-falantes e compartilhamento de tela).Caso o equipamento não possua esta funcionalidade, deverá ser fornecida solução USB com câmeras com as mesmas características do sistema de vídeo, sistema de som e microfones com conectividade com uma única porta USB e HDMI

11.11.48 Todos os cabos devem ser fornecidos pelo proponente

11.11.49 O terminal de vídeo e painel de controle touch deverão possuir suporte a trava mecânica tipo Kensington;

11.12. PROCESSADOR / GERENCIADOR PARA MONITORES DE VIDEOWALL

11.12.1 Fornecer 08 (oito) interfaces de saída HDMI (adaptável para DVI-D) e BNC;

11.12.2 Resolução de até 4K (3840 × 2160@30Hz) via interfaces de saída HDMI (somente para interface ímpar);

11.12.3 Compressão de vídeo H.265+/H.265, H.264+/H.264, Hik264, MPEG4 e MJPEG;

11.12.4 Formatos de encapsulamento PS, RTP, TS, ES, HIK;

11.12.5 Três níveis de codificação: linha de base, principal e alto perfil;

11.12.6 Compressão de áudio G.722, G711A, G726, G711U, MPEG2-L2 e AAC;
11.12.7 Dois modos de decodificação: decodificação ativa e decodificação passiva;
11.12.8 Saída de decodificação de arquivos de vídeo remotos;
11.12.9 Suporta áudio bidirecional via software cliente;
11.12.10 Fornecer interfaces de entrada VGA e DVI;
11.12.11 Suportar abertura de janela, roaming de janela e divisão de janela;
11.12.12 Suportar controle de tela múltipla com PC instalado com servidor RSC;
11.12.13 Suportar stream e decodifica via URL e RTSP de dispositivos de codificação;
11.12.14 Exibir o fluxo de vídeo decodificado na parede de vídeo, vinculando diretamente as câmeras ou encaminhando o fluxo de mídia;
11.12.15 Configuração do video wall por meio do navegador web;
11.12.16 Tela virtual regular e irregular configurável para exibir múltiplas fontes de sinal e se livrar da restrição de tela física.
11.12.17 Acessível pela câmera DeepinView de 2,4 MP.
11.12.18 Áudio bidirecional.
11.12.19 Tecnologia de agregação de portas (Ethernet Channel).
11.12.20 Resolução de decodificação: até 24MP (apenas para o modo de 3 faixas do codificador)
11.12.21 Capacidade de decodificação: 24MP@30fps: 4-ch, 12MP@20fps:8-ch, 8MP@30fps: 16-ch, 5MP@30fps: 24-ch, 3MP@30fps: 40-ch, 1080p@30fps: 64-ch
11.12.22 Divisão de tela: 1/4/6/8/9/12/16/25/36
11.12.23 Interfaces: Interface RJ45 × 2, 10/100/1000 Mbps adaptável para Interface óptica × 2, 100 base-FX/1000 base-X ou uma interface RJ45 e uma interface óptica formando uma combinação.
11.12.24 Interface Serial RS-232 (RJ45)
11.12.25 Saída de áudio bidirecional 3.5 mm conector, 2.0 Vp-p, 1 KΩ
11.12.26 Entrada de áudio bidirecional 3.5 mm conector, 2.0 Vp-p, 1 KΩ
11.12.27 Dimensões Máximas 450 mm × 340 mm × 45 mm
11.12.28 O sistema deve ser fornecido com software de gerenciamento de mesma origem da fabricante para melhor compatibilidade;
11.12.29 O sistema deve possuir opção de configuração em massa, permitindo alterarem-se as configurações em vários dispositivos ao mesmo tempo com poucos cliques, independentemente de estarem no mesmo site ou remotos;
11.12.30 O sistema deve permitir a configuração de gerenciamento de modelos de programação de horários de acesso, possibilitando configurar modelos de período de tempo que podem ser aplicados a níveis de controle de acesso.
11.12.31 O sistema deve permitir a configuração remota dos decoders
11.12.32 O sistema deve ter a possibilidade de a associação de dois ou mais decoders, através de um controlador de videowall, para melhor gerenciamento de telas através

11.13. MONITOR PROFISSIONAL PARA VIDEOWALL

11.13.1 Monitor com tamanho diagonal 55" (polegadas), tipo de painel Direct LED, resolução1,920 x 1,080, pixel pitch0.63x0.63, brilho (típico) MAX 500 cd/ m², contraste1,200:1, ângulo de visão (horizontal / vertical) 178/178, tempo de resposta 8ms, gama de cores 72%, opacidade do vidro 0.28 %, varredura horizontal 65kHz ~ 70kHz, frequência máxima de pixels 154MHz (77MHzx2) e varredura vertical 47Hz ~ 63Hz;

11.13.2 Conectividade com 2 (duas) entradas HDMI, 01 (uma) entrada DP, 01 (uma) entrada DVI, 01 (uma) USB, 01 (uma) IR, 01 (uma) entrada de áudio, 01 (uma) saída estéreo Mini Jack, 01 (uma) saída de vídeo, 01 (uma) entrada RS232, 01 (uma) saída RS232 e 01 (uma) entrada RJ45;

11.13.3 Alimentação de energia composta de fonte de energiaAC100-240V 50/60Hz, consumo de energia (quando ligado) 242W e consumo de energia (stand-by) 0.5W;

11.13.4 Condições operacionais de temperatura entre 0°C~ 40°C e umidade entre 10 ~ 90%;

11.13.5 Especificação mecânica contendo suporte VESA (mm) 600 x 400 mm, largura da borda 0.9mm(U/L), 0.9mm(R/B) e material da moldura Glossy;

11.13.6 Certificação de conformidade EMC Class A e Segurança 60950-1;

11.13.7 Deverão ser fornecidos os monitores e serviços de instalação dos periféricos;

11.13.8 Visualização imersiva e confiável, 24 horas por dia, 7 dias por semana;

11.13.9 Profundidade do gabinete de no máximo 72 mm;

11.13.10 Possuir ângulos de visão de 178 graus horizontal e vertical que possibilitem projeção(de conteúdo; facilmente visível, mesmo se os espectadores não estiverem diretamente na frente da tela;

11.13.11 Suportar painéis antirreflexo distribuindo uniformemente a luz pela tela para manter um conteúdo vibrante e preciso;

11.14. SUPORTE PARA MONITOR PROFISSIONAL PARA VIDEOWALL

11.14.1 O suporte em alumínio ou aço, com tratamento antiferrugem;

11.14.2 Projetado e fabricado para operação contínua, 24 (vinte e quatro) horas por dia, 365 (trezentos e sessenta e cinto) dias por ano;

11.14.3 Possuir fixação para colocação dos monitores profissionais de 55";

11.14.4 Possuir sistema com trava de segurança;

11.14.5 Permitir o travamento e desbloqueio rápido dos monitores para garantir a segurança da instalação;

11.14.6 Possuir sistema de extensão Pop-Out perpendicular a estrutura com abertura de 19cm;

11.14.7 Permitir micro ajuste multidimensional com precisão de altura, profundidade e inclinação dos monitores de vídeo wall;

11.14.8 Compatibilidade eletromagnética, de modo a operar corretamente livre de interferências e não atuar como fonte de interferência para os demais equipamentos da sala de reuniões do Grupamento;

11.14.9 Deve permitir fácil acesso na parte traseira para manutenção no seu interior;

11.14.10 Permitir a retirada de um único monitor para manutenção sem comprometer a opção do sistema;

11.14.11 Deverão ser fornecidos os materiais e serviços de instalação dos acabamentos periféricos em formato de moldura ao redor de todo painel, ou seja, o fechamento complementar do tipo carenagem nas duas extremidades laterais, inferior e superior no contorno de todo painel.

11.14.12 Max Vesa 600x400;

11.14.13 Suportar até 70Kg;

11.15. PROJETOR 2800 LUMENS PADRÃO 21118

11.15.1 Tipo de tela: Matriz ativa TFT de poli-silício

11.15.2 Resolução: 1280 × 800 pixels (WXGA)

11.15.3 Lente: F = 1.58 a 1.72

11.15.4 Distância focal: 16,9 a 20,28 mm
11.15.5 Reprodução de cores: Full color, 16,77 milhões de cores
11.15.6 Brilho:
11.15.7 PowerLite Home Cinema 725HD
11.15.8 Modo de consumo de energia normal
11.15.9 Emissão de luz branca 2800 lúmens (padrão ISO 21118)
11.15.10 Emissão de luz colorida 2800 lúmens
11.15.11 Modo de consumo de energia ECO:
11.15.12 Emissão de luz branca 1960 lúmens (padrão ISO 21118)
11.15.13 PowerLite Home Cinema 730HD:
11.15.14 Modo de consumo de energia normal:
11.15.15 Emissão de luz branca 3000 lúmens (padrão ISO 21118)
11.15.16 Emissão de luz colorida 3000 lúmens
11.15.17 Modo de consumo de energia ECO:
11.15.18 Emissão de luz branca 2100 lúmens (padrão ISO 21118)
11.15.19 A emissão de luz colorida é medida de acordo com IDMS 15.4; a emissão de luz branca é medida de acordo com ISO 21118.
11.15.20 Relação de contraste: Até 12000:1
11.15.21 Tamanho da imagem: 0,83 a 8,13 metros
11.15.22 Distância de projeção: 0,9 a 10,8 metros
11.15.23 Métodos de projeção: Frontal, traseira, montada no teto
11.15.24 Relação de aspecto ótico (largura-altura): 16:10
11.15.25 Ajuste de foco: Manual
11.15.26 Ajuste de zoom Manual (óptico)
11.15.27 Relação de zoom (Tele-a-Wide): 1:1.2
11.15.28 Sistema de som interno 2 W monaural
11.15.29 Nível de ruído 37 dB (Modo de consumo de energia normal) e 29 dB (Modo de consumo de energia ECO)
11.15.30
11.15.31 Ângulo de correção de efeito trapézio Vertical: ± 30° / Horizontal: ± 30°
11.15.32 Compatibilidade da porta USB Type B Compatível com USB 1.1 e 2.0 para exibição USB ou uso como mouse externo
11.15.33 Compatibilidade da porta USB Type A Uma porta compatível com USB 1.1 e 2.0 para entrada de dispositivo USB
11.15.34 Lâmpada do projetor do tipo UHE (Eficiência Ultra-Alta)
11.15.35 Consumo de energia 200 W
11.15.36 Vida útil da lâmpada em modo de consumo de energia normal de até cerca de 5000 horas e modo de consumo de energia ECO de até cerca de 6000 horas

11.16. PROJETOR 12000 LUMENS 4K UHD LASER

11.16.1 Deve possuir tecnologia avançada de deslocamento de pixels 4K PRO-UHD
11.16.2 Deve possuir placa de vidro de deslocamento de precisão
11.16.3 Processador de imagem de no mínimo 32 bits
11.16.4 Fonte de luz de matriz de laser
11.16.5 Processamento completo de cores HDR de 10 bits que aceita 100% das informações da fonte HDR
11.16.6 Taxa de atualização de 120 Hz
11.16.7 imagem excepcional e uniformidade de foco de ponta a ponta. Esta pode ser uma das melhores tecnologias de lentes de projetor que a Epson já desenvolveu

11.16.8 Deslocamento de lente motorizado de 3 eixos
11.16.9 Correção de cena adaptável em tempo real
11.16.10 HDMI 2.1
11.16.11 Brilho Branco de 2.700 ANSI Lumens
11.16.12 Brilho da cor de 2.700 lúmens CLO
11.16.13 Resolução de 3840 x 2160
11.16.14 Proporção da tela 16:9 (4K HD)
11.16.15 Permitir Íris Dinâmica
11.16.16 Exibição em chips 3LCD de 2 cm
11.16.17 Processamento de cores de 10 bits
11.16.18 Modos de vídeo em 720p, 1080i, 1080p/60, 576i, 576p, 480p, 480i
11.16.19 Modos de dados máxima 4096 x 2160
11.16.20 Lâmpada tipo laser fósforo
11.16.21 Vida útil da lâmpada de no mínimo 20.000 horas
11.16.22 Permitir zoom motorizado de 2.1x, foco motorizado
11.16.23 Deslocamento da Lente Horizontal de +/-47% e Vertical +/-96%
11.16.24 Distância de projeção de 3,1m até 9,0 m
11.16.25 Ruído Audível de 30 dB / 22 dB (Eco)
11.16.26 2x Interfaces HDMI 2.1
11.16.27 1x Interface de Rede RJ-45
11.16.28 1x Interface RS232 DB-9 pinos USB x 2

11.17. ADAPTADOR DISPLAY PORT/HDMI

11.17.1 Adaptador Conversor DisplayPort para HDMI para conexão de um monitor LCD, LED ou Plasma, projetor ou Televisores FullHD a um MacBook ou um PC equipado com um conector DisplayPort.
11.17.2 Suportar transmissão de até 8.64 gigabits, o que permite o uso de resoluções de até 2560×1600 (com 60 Hz) e refresh-rates mais altos, de até 120 Hz, em resoluções mais baixa\os.
11.17.3 Compatível com MacBook, MacBook Air ou MacBook Pro e todos os equipamentos com saída DisplayPort.
11.17.4 Tamanho do cabo máximo de 23 centímetros

11.18. ALICATE DE CRIMPAR

11.18.1 Corpo de aço com revestimento termoplástico;
11.18.2 Executa a inserção das garras de contato do conector RJ-45 macho e aciona o prensa-cabo;
11.18.3 Permite a conectorização de conectores RJ-45 macho CAT.5e, CAT.5e (blindado) e CAT.6;
11.18.4 Tipo de Conector RJ-45;
11.18.5 Material do Corpo do Produto: Termoplástico / Aço;
11.18.6 Ambiente de Instalação Interno;

11.19. UNIDADE DE DISCO EXTERNO 2TB

11.19.1 Tipo externo portátil, conexão USB 3.0,
11.19.2 Capacidade de armazenamento de 2TB;
11.19.3 Velocidade mínima de transferência de dados 480 Mb/s usando USB 2.0;
11.19.4 Alimentação via USB;
11.19.5 Dimensões aproximadas do produto (cm - A x L x P) 1,7 x 8,2 x 11,1 cm;

11.19.6 Peso máximo de 220 gramas.
11.19.7 Compatível com Windows 7 e posterior, Mac OS X v.10.6.x ou superior, Linux v.2.6.x ou superior

11.20. MONITOR 24"

11.20.1 Ângulo de visão: 178°
11.20.2 Proporção de tela: 16:9
11.20.3 Resolução: 1920 x 1080
11.20.4 Tamanho: 24"
11.20.5 Brilho (Min): 200 cd / m2
11.20.6 Resolução: 1920x1080 (Full HD)
11.20.7 Cor: 16.7M
11.20.8 Power: Adaptador Externo
11.20.9 Voltagem: 100~240V 50/60Hz
11.20.10 Stand By Power: 0.3W
11.20.11 Consumo de energia (máx.): 25W
11.20.12 Consumo (desligado): <0,3W
11.20.13 Consumo típico: 24W
11.20.14 Consumo anual: 35 kWh/ano
11.20.15 Game Mode
11.20.16 Flicker Free
11.20.17 AMD Free Sync
11.20.18 Tempo de Resposta: 4 ms
11.20.19 Dimensão conj. c/ suporte: 547,8 x 418,2 x 206,5 mm
11.20.20 Dimensão conj. s/ suporte: 547,8 x 326,3 x 87,6 mm
11.20.21 1x VGA
11.20.22 1x HDMI
11.20.23 1x Fones de ouvido
11.20.24 Temperatura: 10-40°C
11.20.25 Umidade: 10-80% (sem condensação)

11.21. PLACA DE VIDEO 1GB HDMI

11.21.1 Memória de Vídeo: GDDR3 1GB
11.21.2 Barramento: PCI Express 2.0
11.21.3 Clock do Processador (Base): 520 MHz
11.21.4 Clock do Processador (Completo): 1237 MHz
11.21.5 Clock de Memória (Completo): 1200 MHz
11.21.6 1x DVI: (DVI-D)
11.21.7 1x HDMI
11.21.8 1x D-Sub
11.21.9 Máximo de Monitores: 2
11.21.10 Resolução máxima Digital: 2560 x 1600
11.21.11 Resolução máxima analógica: 2048 x 1536
11.21.12 OpenGL 3.1
11.21.13 DirectX 10.1
11.21.14 300 W

11.22. PLACA DE REDE PADRÃO PCI-EXPRESS

11.22.1 Chipset: Realtek RTL8111 ou superior
11.22.2 Placa de Rede 1000 Base-T de Alto desempenho

11.22.3 Compatibilidade: Redes 10/100 Base-T
11.22.4 Suporte automático: Redes 10/100/1000 Base-T
11.22.5 Compatibilidade PCI: PCI Express revisão 1.1
11.22.6 Taxa de transferência: Até 2.5 Gbps Full Duplex
11.22.7 Padrões de comunicação compatíveis: IEEE 802.3, 802.3u, 802.3ab IEEE 802.1Q VLAN (somente Windows® 2000 e XP)
11.22.8 Controle de fluxo: Half Duplex e Full Duplex (IEEE 802.3x)
11.22.9 Padrão de cabeamento compatível: CAT-5/6 UTP
11.22.10 Autodetecção e correção: Detecção e correção de cabo crossover
11.22.11 Sistemas operacionais compatíveis: Windows® 98 SE / ME / 2000 / XP 32-64 bit / Server 2003 32-64 bit / Server 2008 32-64 bit / Vista 32-64 bit / Seven (7) 32-64 bit, Linux®, Ms-DOS® e Mac OS® 10.4 ou superior.

11.23. MEMÓRIA RAM DDR3 8GB

11.23.1 8GB DDR3 1600MHz com tensão de alimentação de 1,5V e pinagem de 240 pinos.

11.24. MEMÓIRA RAM DDR 4 8GB

11.24.1 8GB DDR4, 2666MHz, Non-ECC, CL17, X8, 1.2V, Unbuffered, DIMM, 288-pin

11.25. ÁLCOOL ISOPROPÍLICO

11.25.1 70% de álcool etílico e 30% de água.

11.26. LICENÇA OFFICE

11.26.1 Linguagem: português (podendo ser alterado pelo usuário);
11.26.2 Tecnologia: 32 / 64 bits para computadores com Windows 10 e Windows 11;
11.26.3 O conjunto deve incluir Word, Excel, OneNote, PowerPoint, Outlook, Publisher, Access e Teams;
11.26.4 Processador com 2 núcleos, 1,6 GHz;
11.26.5 Sistema operacional: Windows 11 ou Windows 10;
11.26.6 Memória: 4 GB (64 bits), 2 GB (32 bits) de RAM;
11.26.7 Espaço em disco rígido: 4 GB de espaço disponível em disco;
11.26.8 Tela: Resolução de 1024 x 768;
11.26.9 Elementos gráficos: Placa gráfica DirectX 10 para a aceleração de hardware gráfico;
11.26.10 Requisitos adicionais do sistema: Acesso à Internet.

12. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

12.1 A tabela abaixo demonstra o custo total da contratação baseado na média das propostas enviadas para o CMB.

ITEM	DESCRIÇÃO	QTDE	PREÇO UNITÁRIO	PREÇO TOTAL
01	PONTOS DE ACESSO PARA REDE SEM FIO (INDOOR)	60	R$ 23.371,20	R$ 1.402.272,00
02	PONTOS DE ACESSO PARA REDE SEM	06	R$ 25.011,00	R$ 150.066,00

	FIO (OUTDOOR)			
03	FIREWALL PARA ALTA DISPONIBILIDADE	01	R$ 121.489,29	R$ 121.489,29
04	SISTEMA DE ENERGIA ININTERRUPTA (UPS/NOBREAK) 2000VA	30	R$ 7.469,68	R$ 224.090,28
05	SISTEMA DE ENERGIA ININTERRUPTA (UPS/NOBREAK) 20KVA	01	R$ 56.070,45	R$ 56.070,45
06	SWITCH DE ACESSO L2+L3 48 PORTAS 10/100/1000BASE-T	10	R$ 54.155,96	R$ 541.559,60
07	SWITCH 48 PORTAS FIBER COM 2 PORTAS UPLINK/STACK QSFP28	02	R$ 178.622,40	R$ 357.244,80
08	ESTAÇÃO DE TRABALHO DO TIPO DESKTOP COMPACTO TIPO 1	30	R$ 8.985,00	R$ 269.549,94
09	ESTAÇÃO DE TRABALHO DO TIPO DESKTOP COMPACTO TIPO 2	20	R$ 12.152,00	R$ 243.040,00
10	NOTEBOOK	30	R$ 12.535,68	R$ 376.070,40
11	CÂMERA DE VIDEOCONFERENCIA CORPORATIVA	05	R$ 11.873,33	R$ 59.366,67
12	PROCESSADOR / GERENCIADOR PARA MONITORES DE VIDEOWALL	01	R$ 24.670,00	R$ 24.670,00
13	MONITOR PROFISSIONAL PARA VIDEOWALL	08	R$ 17.413,33	R$ 139.306,67
14	SUPORTE PARA MONITOR PROFISSIONAL PARA VIDEOWALL	08	R$ 1.577,50	R$ 12.620,00
15	PROJETOR 2800 LUMENS PADRÃO 21118	60	R$ 8.939,80	R$ 536.388,00
16	PROJETOR 12000 LUMENS 4K UHD LASER	02	R$ 119.929,67	R$ 239.859,33
17	ADAPTADOR DISPLAY PORT/HDMI	100	R$ 52,46	R$ 5.245,80
18	ALICATE DE CRIMPAR	05	R$ 319,25	R$ 1.596,25
19	UNIDADE DE DISCO EXTERNO 2TB	30	R$ 1.061,04	R$ 31.831,20
20	MONITOR 24"	50	R$ 1.559,23	R$ 77.961,67
21	PLACA DE VIDEO 1GB HDMI	50	R$ 1.684,31	R$ 84.215,58
22	PLACA DE REDE PADRÃO PCI-EXPRESS	30	R$ 180,60	R$ 5.418,00
23	MEMÓRIA RAM DDR3 8GB	30	R$ 229,67	R$ 6.890,00
24	MEMÓIRA RAM DDR 4 8GBPO	30	R$ 324,94	R$ 9.748,30

25	ÁLCOOL ISOPROPÍLICO	10	R$ 20,29	R$ 202,92
26	LICENÇA OFFICE	50	R$ 2.401,57	R$ 120.078,42
			TOTAL	**R$ 5.096.851,57**

13. JUSTIFICATIVA TÉCNICA DA ESCOLHA DA SOLUÇÃO

Esse processo de compra ocorre principalmente para o aumento da capacidade de atendimento da rede sem fio do CMB. Os itens 1, 2 e 3 são os principais itens de compra desse processo. Ressalta-se que os demais itens são complementares para que a rede sem fio funcione de maneira adequada. Desta forma, justifica-se a escolha desses itens que compõem a solução total, pelos seguintes aspectos:

13.1 Proteção contra acesso não autorizado: A segurança da rede Wi-Fi do CMB impede que pessoas não autorizadas se conectem a ela. Isso evita o roubo de dados e o uso indevido da conexão à internet.

13.2 Privacidade dos dados: Configurações de segurança garantem a privacidade dos dados transmitidos pela rede do CMB. Isso impede que terceiros interceptem e acessem informações confidenciais, como senhas e informações pessoais.

13.3 Prevenção de ataques cibernéticos: Uma rede Wi-Fi segura ajuda a proteger os dispositivos e dados contra ameaças cibernéticas, como ataques de hackers, malware e phishing.

13.4 Controle de acesso: As configurações de segurança permitem que o CMB controle quem pode acessar a rede, definindo senhas ou usando outras medidas de autenticação, como filtros de endereços MAC.

13.5 Maior estabilidade e desempenho: A segurança pode melhorar o desempenho da rede do CMB, uma vez que evita que dispositivos não autorizados acessem a rede e a sobrecarreguem.

13.6 Conformidade legal: Em muitas jurisdições, a implementação de medidas de segurança em redes Wi-Fi é um requisito legal para proteger a privacidade dos usuários e evitar responsabilidades legais decorrentes de atividades maliciosas realizadas em sua rede.

13.7 Segurança de dispositivos conectados: A rede Wi-Fi segura do CMB ajuda a proteger os dispositivos conectados à rede, como computadores, smartphones e câmeras de segurança, contra ameaças externas.

13.8 Mitigação de riscos de segurança: reduz a exposição a riscos cibernéticos, como invasões e vazamento de informações confidenciais.

13.9 Confiabilidade: A rede Wi-Fi segura do CMB é mais confiável, uma vez que minimiza as interrupções causadas por atividades não autorizadas ou maliciosas.

14. JUSTIFICATIVA ECONÔMICA DA ESCOLHA DA SOLUÇÃO

Esse processo justifica-se economicamente viável conforme demonstrado no item 10 deste documento.

15. BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

A ampliação da rede Wi-Fi no CMB oferece diversos benefícios significativos para alunos, professores, e a instituição como um todo. Aqui estão alguns dos principais benefícios:

15.1 Acesso à Internet: Acesso à internet de alta velocidade permite que alunos e professores acessem uma vasta gama de recursos educacionais online, como pesquisas, vídeos educacionais, plataformas de e-learning e materiais de estudo.

15.2 Aprendizado personalizado: a rede Wi-Fi do CMB visa permitir a implementação de métodos de ensino personalizados, como aulas online, pesquisa independente e recursos interativos, atendendo às diferentes necessidades de aprendizado dos alunos.

15.3 Colaboração: Os alunos podem colaborar em projetos escolares, pesquisas e tarefas online, o que promove o trabalho em equipe e habilidades de comunicação.

15.4 Mobilidade: com a rede Wi-Fi, professores e alunos podem acessar recursos educacionais de qualquer lugar na escola, tornando o aprendizado mais flexível e eficiente.

15.5 Recursos digitais: O acesso à internet sem fio permite que escolas incorporem tecnologias digitais em suas práticas educacionais, incluindo tablets, laptops e outros dispositivos que podem melhorar a experiência de aprendizado.

15.6 Redução de custos: Embora a infraestrutura inicial possa ser um investimento, a implementação de uma rede Wi-Fi pode, a longo prazo, reduzir os custos de impressão, armazenamento de materiais físicos e distribuição de documentos.

15.7 Melhoria na administração escolar: a rede Wi-Fi pode melhorar a administração do CMB, simplificando tarefas como registro de alunos, comunicação com os pais e funcionários, e gerenciamento de recursos.

15.8 Acesso a recursos educacionais globais: Alunos e professores podem acessar uma vasta gama de recursos educacionais de todo o mundo, enriquecendo seus conhecimentos e perspectivas.

15.9 Preparação para o mundo digital: A educação digital prepara os alunos para o mundo cada vez mais digital em que vivemos, fornecendo habilidades tecnológicas essenciais.

15.10 Maior engajamento: Recursos interativos e a capacidade de pesquisa online podem aumentar o engajamento dos alunos, tornando o processo de aprendizado mais interessante e envolvente.

15.11 Acompanhamento e avaliação: As tecnologias Wi-Fi permitem um acompanhamento mais preciso do desempenho dos alunos e a avaliação de seu progresso de forma contínua.

15.12 Comunicação e colaboração com os pais: O CMB pode usar a rede Wi-Fi para manter os pais informados sobre eventos, atividades escolares e o desempenho de seus filhos.

Em resumo, uma rede Wi-Fi bem implementada no CMB pode melhorar significativamente a qualidade da educação, promovendo a aprendizagem, a colaboração, o acesso a recursos educacionais e a preparação dos alunos para um mundo cada vez mais digital. No entanto, é importante que o CMB também garanta a segurança e a privacidade dos dados dos alunos ao implementar tal rede.

16. PROVIDÊNCIAS A SEREM ADOTADAS

Algumas providências que devem ser adotadas para continuidade desse processo de aquisição:

16.1 Publicação do Edital: O edital contendo todas as informações sobre a licitação deve ser publicado de acordo com os prazos e procedimentos definidos em lei.

16.2 Divulgação e Ampliação da Concorrência: Divulgar o edital em locais de amplo acesso, em plataformas oficiais, para garantir que um número suficiente de fornecedores em potencial tenha conhecimento da licitação.

16.3 Esclarecimento de Dúvidas: Durante o período de preparação e envio das propostas, permitir que os fornecedores façam perguntas e solicitem esclarecimentos sobre o edital.

16.4 Recebimento de Propostas: Estabelecer prazo para a apresentação das propostas pelos fornecedores interessados;

16.5 Análise das Propostas: Avaliar as propostas recebidas com base nos critérios definidos no edital, como preço, qualidade, prazo de entrega, entre outros.

16.6 Habilitação dos Fornecedores: Verificar se os fornecedores que apresentaram as melhores propostas atendem aos requisitos de habilitação, como regularidade fiscal e jurídica.

16.7 Julgamento da Licitação: Realizar a sessão de julgamento para declarar o vencedor da licitação com base na combinação de preço e qualidade, conforme os critérios estabelecidos no edital.

16.8 Recurso e Impugnação: Permitir que os participantes recorram das decisões, se necessário, e forneça um procedimento para resolver impugnações ou contestações.

16.9 Adjudicação e Homologação: Após a fase de recursos, declarar o vencedor da licitação e, em seguida, homologar o resultado.

16.10 Contratação e Execução: Elaborar o contrato com o fornecedor vencedor e monitore a execução do contrato para garantir que os termos sejam cumpridos.

17. DECLARAÇÃO DE VIABILIDADE

17.1 Os estudos preliminares evidenciaram que a aquisição dos equipamentos para continuidade de implantação da rede sem fio, são compatíveis com a solução atualmente utilizada no Colégio Militar de Brasília e vai ampliar a garantia e suporte técnico e consequentemente o tempo de uso da tecnologia existente atualmente.

17.2 Mostra-se exequível a realização da aquisição pretendida não só no aspecto técnico, mas também econômico/administrativo, conforme demonstrado no item 10 deste documento, para o atendimento das necessidades de gestão de capacidade dos elementos de infraestrutura necessários ao funcionamento dos serviços e soluções de TI;

17.3 Aos aspectos técnicos, administrativos e econômicos, declara-se que a aquisição, apresentada no item 06 deste documento, como viável, uma vez que existem fornecedores no mercado ofertando regularmente os produtos necessários para alcançar os resultados pretendidos pelo CMB.

17.4 Esta equipe de planejamento sugere as contratações mediante Pregão Eletrônico SRP conforme amparo abaixo trancrito:

> "**DECRETO Nº 11.462, DE 31 DE MARÇO DE 2023** Regulamenta os art. 82 a art. 86 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o sistema de registro de preços para a contratação de bens e serviços, inclusive obras e serviços de engenharia, no âmbito da Administração Pública federal direta, autárquica e fundacional.
> Art. 3º O SRP poderá ser adotado quando a Administração julgar pertinente, em especial:
> II - quando for conveniente a aquisição de bens com previsão de **entregas parceladas** ou contratação de serviços remunerados por unidade de medida, como quantidade de horas de **serviço**, postos de trabalho ou **em regime de tarefa**;
> III - quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas;"

18. RESPONSÁVEL

COLÉGIO MILITAR DE BRASÍLIA - CMB
Fls. 210
Rub:

INTEGRANTE TÉCNICO E REQUISITANTE
ALEX JULIO FAVELA DOS SANTOS – 1º Ten **Matrícula:** 838.474.801-20 Brasília-DF, 28 de maio de 2024.

19. APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

9.1 Integrante Técnico - O presente planejamento foi elaborado em consonância com a Instrução Normativa nº 1/2019 – Secretaria de Governo Digital do Ministério da Economia, bem como demais normativos e instrumentos legais que embasaram o presente Estudo Técnico Preliminar, e ainda em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da contratação ora pretendida.

9.2 Integrante Requisitante - O presente planejamento atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade para a Administração Pública, os riscos envolvidos são administráveis e a área requisitante priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que recomendamos a contratação pretendida.

9.3 Autoridade Competente da Área Administrativa - O presente planejamento está em conformidade com os requisitos administrativos necessários à consecução do objeto da contratação ora pretendida.

INTEGRANTE ADMINISTRATIVO
DARKO KERIMBEY BARBOSA BITAR - Cel CPF:808.826.507-00 Brasília-DF, 28 de maio de 2024.

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
COLÉGIO MILITAR DE BRASÍLIA

COLÉGIO MILITAR DE BRASÍLIA - CMB
Fls. 52 V
Rub:

AUTORIDADE MÁXIMA DA ÁREA DE TIC)

LUCIANO AUGUSTO WOSIACH
Matrícula: 625.953.509-00

Brasília-DF, 28 de maio de 2024.

AUTORIDADE SUPERIOR – § 3° do art. 11)

THALES MOTA DE ALENCAR – Cel
Ordenador de Despesas
Matrícula: 464.953.473.91

Brasília-DF, 28 de maio de 2024.

COLÉGIO MILITAR DE BRASÍLIA
Fls. 521
Rub:

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
COLÉGIO MILITAR DE BRASÍLIA

(Processo Administrativo n° 64250.011956/2023-72)

ANEXO II – **MINUTA DE TERMO DE CONTRATO**

CONTRATO ADMINISTRATIVO nº ...../2024, QUE FAZEM ENTRE SI A UNIÃO, POR INTERMÉDIO DO COLÉGIO MILITAR DE BRASÍLIA E .....

A União por intermédio do Colégio Militar de Brasília, com sede no SGAN 902, Conjunto "A", Asa Norte, CEP 70.790-020, na cidade de Brasília-DF, inscrito no CNPJ sob o nº 09.604.923/0001-27, neste ato representado pelo Sr THALES MOTA DE ALENCAR, nomeado pela Portaria nº ....., de ..... de ..... de 20..., publicada no DOU de ..... de ..... de ....., portador da Matrícula Funcional nº ....., doravante denominado CONTRATANTE, e o(a) ....., inscrito(a) no CNPJ/MF sob o nº ....., sediado(a) na ....., doravante designado CONTRATADO, neste ato representado(a) por ..... (nome e função no contratado), conforme atos constitutivos da empresa OU procuração apresentada nos autos, tendo em vista o que consta no Processo nº ..... e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão Eletrônico nº 01/2024, mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – OBJETO (art. 92, I e II)

1.1. O objeto do presente instrumento é a aquisição de pontos de acesso e equipamentos complementares para arede sem fio, nas condições estabelecidas no Termo de Referência.

1.2. Objeto da contratação:

ITEM	ESPECIFICAÇÃO	Un medida	Qntd	VALOR UNITÁRIO R$	VALOR TOTAL R$
01	Pontos de acesso para rede sem fio (indoor)	Un	60		
02	Pontos de acesso para rede sem fio (outdoor)	Un	06		
03	Firewall para alta disponibilidade	Un	01		
04	Sistema de energia ininterrupta (ups/nobreak) 2000va	Un	30		
05	Sistema de energia ininterrupta (ups/nobreak) 20kva	Un	01		
06	Switch de acesso l2+l3 48 portas 10/100/1000base-t	Un	10		
07	Switch 48 portas fiber com 2 portas uplink/stack qsfp28	Un	02		
08	Estação de trabalho do tipo desktop compacto tipo 1	Un	50		
09	Estação de trabalho do tipo desktop compacto tipo 2	Un	30		
10	Notebook	Un	30		

Minuta Aprovada pelo DESPACHO n. 00148/2024/CGAO/SCGP/CCU/AGU, de 16 de abril de 2024

ITEM	ESPECIFICAÇÃO	Un medida	Qntd	VALOR UNITÁRIO R$	VALOR TOTAL R$
11	Câmere de videoconferencia corporativa	Un	05		
12	Processador / gerenciador para monitores de videowall	Un	01		
13	Monitor profissional para videowall	Un	08		
14	Suporte para monitor profissional para videowall	Un	08		
15	Projetor datashow 4600 lumens	Un	60		
16	Projetor 12000 4k uhd laser	Un	02		
17	Adaptador display port/hdmi	Un	100		
18	Alicate de crimpar	Un	5		
19	Unidade de disco externo 2tb	Un	30		
20	Monitor 24"	Un	50		
21	Placa de vídeo 1gb hdmi	Un	50		
22	Placa de rede padrão pci-express	Un	30		
23	Memória ram ddr3 8gb	Un	30		
24	Memóira ram ddr4 8gbpo	Un	30		
25	Álcool isopropílico	Un	10		
26	Licença office	Un	50		

1.3. Vinculam esta contratação, independentemente de transcrição:

1.3.1. O Termo de Referência;

1.3.2. O Edital da Licitação;

1.3.3. A Proposta do contratado;

1.3.4. Eventuais anexos dos documentos supracitados.

CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de 90 (noventa) dias contados da data de assinatura do contrato, na forma do artigo 105 da Lei nº 14.133, de 2021.

2.1.1. O prazo de vigência será automaticamente prorrogado, independentemente de termo aditivo, quando o objeto não for concluído no período firmado acima, ressalvadas as providências cabíveis no caso de culpa do contratado, previstas neste instrumento.

2.2. O contratado não tem direito subjetivo à prorrogação contratual.

2.3. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

2.4. O contrato não poderá ser prorrogado quando o contratado tiver sido penalizado nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS (art. 92, IV, VII e XVIII)

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. Não será admitida a subcontratação do objeto contratual.

CLÁUSULA QUINTA – PREÇO (art. 92, V)

5.1. O valor total da contratação é de R$ ..... (.....)

COLÉGIO MILITAR DE BRASÍLIA - CMB
Fls. 51V
Rub:

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

5.3. O valor acima é meramente estimativo, de forma que os pagamentos devidos ao contratado dependerão dos quantitativos efetivamente fornecidos.

CLÁUSULA SEXTA - PAGAMENTO (art. 92, V e VI)

6.1. O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

CLÁUSULA SÉTIMA - REAJUSTE (art. 92, V)

7.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em 14/11/2023.

7.2. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do índice IGPM, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

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

7.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

7.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

7.6. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

7.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

7.8. O reajuste será realizado por apostilamento.

CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE (art. 92, X, XI e XIV)

8.1. São obrigações do Contratante:

8.2. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

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

8.4. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

8.5. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

8.6. Efetuar o pagamento ao Contratado do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência.

8.7. Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

8.8. Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;

8.9. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

8.10. A Administração terá o prazo de 30 (trinta) dias, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

8.11. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 30 (trinta) dias.

8.12. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

8.13. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO (art. 92, XIV, XVI e XVII)

9.1. O Contratado deve cumprir todas as obrigações constantes deste Contrato e em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

9.2. Entregar o objeto acompanhado do manual do usuário, com uma versão em português, e da relação da rede de assistência técnica autorizada;

9.3. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

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

9.5. Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior (art. 137, II, da Lei n.º 14.133, de 2021) e prestar todo esclarecimento ou informação por eles solicitados;

9.6. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os bens nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

9.7. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;

9.8. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o contratado deverá entregar ao setor responsável pela fiscalização do contrato, junto com a Nota Fiscal para fins de pagamento, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Estadual ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;

9.9. Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas, previdenciárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao contratante e não poderá onerar o objeto do contrato;

9.10. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto contratual.

9.11. Paralisar, por determinação do contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

9.12. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

9.13. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116, da Lei n.º 14.133, de 2021);

9.14. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único, da Lei n.º 14.133, de 2021);

9.15. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

9.16. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021.

9.17. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do contratante;

9.18. Alocar os empregados necessários, com habilitação e conhecimento adequados, ao perfeito cumprimento das cláusulas deste contrato, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

9.19. Orientar e treinar seus empregados sobre os deveres previstos na Lei nº 13.709, de 14 de agosto de 2018, adotando medidas eficazes para proteção de dados pessoais a que tenha acesso por força da execução deste contrato;

9.20. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local de execução do objeto e nas melhores condições de segurança, higiene e disciplina.

9.21. Submeter previamente, por escrito, ao contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.

9.22. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

CLÁUSULA DÉCIMA– GARANTIA DE EXECUÇÃO (art. 92, XII)

10.1. Não haverá exigência de garantia contratual da execução.

CLÁUSULA DÉCIMA PRIMEIRA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS (art. 92, XIV)

11.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o contratado que:

a) der causa à inexecução parcial do contrato;

b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

c) der causa à inexecução total do contrato;

d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

f) praticar ato fraudulento na execução do contrato;

COLÉGIO MILITAR DE BRASÍLIA Fls. 323 Rub: 8

g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

11.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

i. **Advertência**, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);

ii. **Impedimento de licitar e contratar**, quando praticadas as condutas descritas nas alíneas "b", "c" e "d" do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

iii. **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nas alíneas "e", "f", "g" e "h" do subitem acima deste Contrato, bem como nas alíneas "b", "c" e "d", que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

iv. **Multa:**

1. Moratória de 1% (um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

2. Moratória de 1% (um por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 30% (trinta por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.

i. O atraso superior a 30 (trinta) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

3. Compensatória, para as infrações descritas nas alíneas "e" a "h" do subitem 11.1, de 20% a 30% do valor do Contrato.

4. Compensatória, para a inexecução total do contrato prevista na alínea "c" do subitem 11.1, de 10% a 15% do valor do Contrato.

5. Para infração descrita na alínea "b" do subitem 11.1, a multa será de 5% a 10% do valor do Contrato.

6. Para infrações descritas na alínea "d" do subitem 11.1, a multa será de 15% a 20% do valor do Contrato.

7. Para a infração descrita na alínea "a" do subitem 11.1, a multa será de 1% a 5% do valor do Contrato, ressalvadas as seguintes infrações:

11.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021)

11.3.1. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

11.3.2. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021)

11.3.3. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).

11.3.4. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

11.4. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no **caput** e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

11.5. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

a) a natureza e a gravidade da infração cometida;

b) as peculiaridades do caso concreto;
c) as circunstâncias agravantes ou atenuantes;
d) os danos que dela provierem para o Contratante;
e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

11.6. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

11.7. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021).

11.8. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161, da Lei nº 14.133, de 2021).

11.9. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

11.10. Os débitos do contratado para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o contratado possua com o mesmo órgão ora contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

CLÁUSULA DÉCIMA SEGUNDA– DA EXTINÇÃO CONTRATUAL (art. 92, XIX)

12.1. O contrato será extinto quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado para tanto.

12.2. Se as obrigações não forem cumpridas no prazo estipulado, a vigência ficará prorrogada até a conclusão do objeto, caso em que deverá a Administração providenciar a readequação do cronograma fixado para o contrato.

12.2.1. Quando a não conclusão do contrato referida no item anterior decorrer de culpa do contratado:

a) ficará ele constituído em mora, sendo-lhe aplicáveis as respectivas sanções administrativas; e

b) poderá a Administração optar pela extinção do contrato e, nesse caso, adotará as medidas admitidas em lei para a continuidade da execução contratual.

12.3. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

12.3.1. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

12.3.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

12.3.2.1. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

12.4. O termo de extinção, sempre que possível, será precedido:

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

12.4.2. Relação dos pagamentos já efetuados e ainda devidos;

12.4.3. Indenizações e multas.

12.5. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, *caput*, da Lei n.º 14.133, de 2021).

12.6. O contrato poderá ser extinto caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

CLÁUSULA DÉCIMA TERCEIRA – DOTAÇÃO ORÇAMENTÁRIA (art. 92, VIII)

13.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União deste exercício, na dotação abaixo discriminada:

13.1.1. Gestão/Unidade:

13.1.2. Fonte de Recursos:

13.1.3. Programa de Trabalho:

13.1.4. Elemento de Despesa:

13.1.5. Plano Interno:

13.1.6. Nota de Empenho:

13.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

CLÁUSULA DÉCIMA QUARTA – DOS CASOS OMISSOS (art. 92, III)

14.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA QUINTA – ALTERAÇÕES

15.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

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

15.3. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

15.4. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

CLÁUSULA DÉCIMA SEXTA – PUBLICAÇÃO

16.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, *caput*, da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012.

CLÁUSULA DÉCIMA SÉTIMA– FORO (art. 92, §1º)

17.1. Fica eleito o Foro da Justiça Federal em Brasília, Seção Judiciária do Distrito Federal para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21.

Brasília-DF, ... de ..... de 2024.

COLÉGIO MILITAR DE BRASÍLIA
Fls. 565
Rub:

Representante legal do CONTRATANTE

Representante legal do CONTRATADO

TESTEMUNHAS:

1-

2-

EM BRANCO

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
COLÉGIO MILITAR DE BRASÍLIA

ANEXO III – **MINUTA** DE ATA DE REGISTRO DE PREÇOS

O Colégio Militar de Brasília, com sede no SGAN 902, Conjunto "A", Asa Norte, CEP 70.790-020, na cidade de Brasília-DF, inscrito no CNPJ/MF sob o nº 09.604.923/0001-27, neste ato representado pelo Sr. THALES MOTA DE ALENCAR, nomeado pela Portaria nº ..... de ..... de ..... de 202..., publicada no ..... de ..... de ..... de ....., considerando o julgamento da licitação na modalidade de pregão, na forma eletrônica, para REGISTRO DE PREÇOS nº 01/2024, publicada no DOU de ...../...../2024, processo administrativo nº 64250.011956/2023-72, RESOLVE registrar os preços da(s) empresa(s) indicada(s) e qualificada(s) nesta ATA, de acordo com a classificação por ela(s) alcançada(s) e na(s) quantidade(s) cotada(s), atendendo as condições previstas no Edital de licitação, sujeitando-se as partes às normas constantes na Lei nº 14.133, de 1º de abril de 2021, no Decreto n.º 11.462, de 31 de março de 2023, e em conformidade com as disposições a seguir:

1. DO OBJETO

1.1. A presente Ata tem por objeto o registro de preços para a eventual aquisição de pontos de acesso e equipamentos complementares para rede sem fio, especificados nos itens do Termo de Referência, anexo I do edital de Licitação nº 01/2024, que é parte integrante desta Ata, assim como as propostas cujos preços tenham sido registrados, independentemente de transcrição.

2. DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

2.1. O preço registrado, as especificações do objeto, as quantidades mínimas e máximas de cada item, fornecedor(es) e as demais condições ofertadas na(s) proposta(s) são as que seguem:

Fornecedor (razão social, CNPJ/MF, endereço, contatos, representante)					
Item	Especificação	Un	Qnt	Valor Unitário	Valor Total
01	Pontos de acesso para rede sem fio (indoor)	Un	60		
02	Pontos de acesso para rede sem fio (outdoor)	Un	06		
03	Firewall para alta disponibilidade	Un	01		
04	Sistema de energia ininterrupta (ups/nobreak) 2000va	Un	30		
05	Sistema de energia ininterrupta (ups/nobreak) 20kva	Un	01		
06	Switch de acesso l2+l3 48 portas 10/100/1000base-t	Un	10		
07	Switch 48 portas fiber com 2 portas uplink/stack qsfp28	Un	02		
08	Estação de trabalho do tipo desktop compacto tipo 1	Un	50		
09	Estação de trabalho do tipo desktop compacto tipo 2	Un	30		
10	Notebook	Un	30		
11	Câmere de videoconferencia corporativa	Un	05		

Fornecedor (razão social, CNPJ/MF, endereço, contatos, representante)					
Item	Especificação	Un	Qnt	Valor Unitário	Valor Total
12	Processador / gerenciador para monitores de videowall	Un	01		
13	Monitor profissional para videowall	Un	08		
14	Suporte para monitor profissional para videowall	Un	08		
15	Projetor datashow 4600 lumens	Un	60		
16	Projetor 12000 4k uhd laser	Un	02		
17	Adaptador display port/hdmi	Un	100		
18	Alicate de crimpar	Un	5		
19	Unidade de disco externo 2tb	Un	30		
20	Monitor 24"	Un	50		
21	Placa de video 1gb hdmi	Un	50		
22	Placa de rede padrão pci-express	Un	30		
23	Memória ram ddr3 8gb	Un	30		
24	Memóira ram ddr4 8gbpo	Un	30		
25	Álcool isopropílico	Un	10		
26	Licença office	Un	50		

2.2. A listagem do cadastro de reserva referente ao presente registro de preços consta como anexo a esta Ata.

3. ÓRGÃOS GERENCIADOR E PARTICIPANTES

3.1. O órgão gerenciador será o Colégio Militar de Brasília.

3.2. Além do gerenciador, é órgão e entidade pública participante do registro de preços:

Item nº	Órgãos Participantes	Unidade	Quantidade
18	IFCE – Campus Limoreiro do Norte	Unidade	3
19			2
20			6
25			2

4. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

4.1. Não será admitida a adesão à ata de registro de preços decorrente desta licitação ou desta contratação direta, conforme justificativa apresentada nos estudos técnicos preliminares.

Vedação a acréscimo de quantitativos

4.2. É vedado efetuar acréscimos nos quantitativos fixados na ata de registro de preços.

5. VALIDADE, FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS E CADASTRO RESERVA

5.1. A validade da Ata de Registro de Preços será de **1** (um) ano, contado a partir do primeiro dia útil subsequente à data de divulgação no PNCP, podendo ser prorrogada por igual período, mediante a anuência do fornecedor, desde que comprovado o preço vantajoso.

5.1.1. O contrato decorrente da ata de registro de preços terá sua vigência estabelecida no próprio instrumento contratual e observará no momento da contratação e a cada exercício financeiro a disponibilidade de créditos orçamentários, bem como a previsão no plano plurianual, quando ultrapassar 1 (um) exercício financeiro.

5.1.2. Na formalização do contrato ou do instrumento substituto deverá haver a indicação da disponibilidade dos créditos orçamentários respectivos.

5.2. A contratação com os fornecedores registrados na ata será formalizada pelo órgão ou pela entidade interessada por intermédio de instrumento contratual, emissão de nota de empenho de despesa, autorização de compra ou outro instrumento hábil, conforme o art. 95 da Lei nº 14.133, de 2021.

5.2.1. O instrumento contratual de que trata o item 5.2. deverá ser assinado no prazo de validade da ata de registro de preços.

5.3. Os contratos decorrentes do sistema de registro de preços poderão ser alterados, observado o art. 124 da Lei nº 14.133, de 2021.

5.4. Após a homologação da licitação ou da contratação direta, deverão ser observadas as seguintes condições para formalização da ata de registro de preços:

5.4.1. Serão registrados na ata os preços e os quantitativos do adjudicatário, devendo ser observada a possibilidade de o licitante oferecer ou não proposta em quantitativo inferior ao máximo previsto no edital e se obrigar nos limites dela;

5.4.2. Será incluído na ata, na forma de anexo, o registro dos licitantes ou dos fornecedores que:

5.4.2.1. Aceitarem cotar os bens, as obras ou os serviços com preços iguais aos do adjudicatário, observada a classificação da licitação; e

5.4.2.2. Mantiverem sua proposta original.

5.4.3. Será respeitada, nas contratações, a ordem de classificação dos licitantes ou dos fornecedores registrados na ata.

5.5. O registro a que se refere o item 5.4.2 tem por objetivo a formação de cadastro de reserva para o caso de impossibilidade de atendimento pelo signatário da ata.

5.6. Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem reduzir suas propostas para o preço do adjudicatário antecederão aqueles que mantiverem sua proposta original.

5.7. A habilitação dos licitantes que comporão o cadastro de reserva a que se refere o item 5.4.2.2 somente será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

5.7.1. Quando o licitante vencedor não assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital; e

5.7.2. Quando houver o cancelamento do registro do licitante ou do registro de preços nas hipóteses previstas no item 9.

5.8. O preço registrado com indicação dos licitantes e fornecedores será divulgado no PNCP e ficará disponibilizado durante a vigência da ata de registro de preços.

5.9. Após a homologação da licitação ou da contratação direta, o licitante mais bem classificado ou o fornecedor, no caso da contratação direta, será convocado para assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital de licitação ou no aviso de contratação direta, sob pena de decair o direito, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

5.9.1. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação do licitante ou fornecedor convocado, desde que apresentada dentro do prazo, devidamente justificada, e que a justificativa seja aceita pela Administração.

5.10. A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no Sistema de Registro de Preços.

5.11. Quando o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital ou no aviso de contratação, e observado o disposto no item 5.7, observando o item 5.7 e subitens, fica facultado à Administração convocar os licitantes remanescentes do cadastro

de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

5.12. Na hipótese de nenhum dos licitantes que trata o item 5.4.2.1, aceitar a contratação nos termos do item anterior, a Administração, observados o valor estimado e sua eventual atualização nos termos do edital, poderá:

5.12.1. Convocar para negociação os demais licitantes ou fornecedores remanescentes cujos preços foram registrados sem redução, observada a ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

5.12.2. Adjudicar e firmar o contrato nas condições ofertadas pelos licitantes ou fornecedores remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.

5.13. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente justificada.

6. ALTERAÇÃO OU ATUALIZAÇÃO DOS PREÇOS REGISTRADOS

6.1. Os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

6.1.1. Em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos da alínea "d" do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;

6.1.2. Em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou a superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

6.1.3. Na hipótese de previsão no edital ou no aviso de contratação direta de cláusula de reajustamento ou repactuação sobre os preços registrados, nos termos da Lei nº 14.133, de 2021.

6.1.3.1. No caso do reajustamento, deverá ser respeitada a contagem da anualidade e o índice previstos para a contratação;

6.1.3.2. No caso da repactuação, poderá ser a pedido do interessado, conforme critérios definidos para a contratação.

7. NEGOCIAÇÃO DE PREÇOS REGISTRADOS

7.1. Na hipótese de o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, o órgão ou entidade gerenciadora convocará o fornecedor para negociar a redução do preço registrado.

7.1.1. Caso não aceite reduzir seu preço aos valores praticados pelo mercado, o fornecedor será liberado do compromisso assumido quanto ao item registrado, sem aplicação de penalidades administrativas.

7.1.2. Na hipótese prevista no item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam reduzir seus preços aos valores de mercado e não convocará os licitantes ou fornecedores que tiveram seu registro cancelado.

7.1.3. Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da ata de registro de preços, adotando as medidas cabíveis para obtenção de contratação mais vantajosa.

7.1.4. Na hipótese de redução do preço registrado, o gerenciador comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços para que avaliem a conveniência e a oportunidade de diligenciarem negociação com vistas à alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

7.2. Na hipótese de o preço de mercado tornar-se superior ao preço registrado e o fornecedor não poder cumprir as obrigações estabelecidas na ata, será facultado ao fornecedor requerer ao

gerenciador a alteração do preço registrado, mediante comprovação de fato superveniente que supostamente o impossibilite de cumprir o compromisso.

7.2.1. Neste caso, o fornecedor encaminhará, juntamente com o pedido de alteração, a documentação comprobatória ou a planilha de custos que demonstre a inviabilidade do preço registrado em relação às condições inicialmente pactuadas.

7.2.2. Não hipótese de não comprovação da existência de fato superveniente que inviabilize o preço registrado, o pedido será indeferido pelo órgão ou entidade gerenciadora e o fornecedor deverá cumprir as obrigações estabelecidas na ata, sob pena de cancelamento do seu registro, nos termos do item 9.1, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021, e na legislação aplicável.

7.2.3. Na hipótese de cancelamento do registro do fornecedor, nos termos do item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam manter seus preços registrados, observado o disposto no item 5.7.

7.2.4. Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da ata de registro de preços, nos termos do item 9.4, e adotará as medidas cabíveis para a obtenção da contratação mais vantajosa.

7.2.5. Na hipótese de comprovação da majoração do preço de mercado que inviabilize o preço registrado, conforme previsto no item 7.2 e no item 7.2.1, o órgão ou entidade gerenciadora atualizará o preço registrado, de acordo com a realidade dos valores praticados pelo mercado.

7.2.6. O órgão ou entidade gerenciadora comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços sobre a efetiva alteração do preço registrado, para que avaliem a necessidade de alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

8. REMANEJAMENTO DAS QUANTIDADES REGISTRADAS NA ATA DE REGISTRO DE PREÇOS

8.1. As quantidades previstas para os itens com preços registrados nas atas de registro de preços poderão ser remanejadas pelo órgão ou entidade gerenciadora entre os órgãos ou as entidades participantes e não participantes do registro de preços.

8.2. O remanejamento somente poderá ser feito:

8.2.1. De órgão ou entidade participante para órgão ou entidade participante; ou

8.2.2. De órgão ou entidade participante para órgão ou entidade não participante.

8.3. O órgão ou entidade gerenciadora que tiver estimado as quantidades que pretende contratar será considerado participante para efeito do remanejamento.

8.4. Na hipótese de remanejamento de órgão ou entidade participante para órgão ou entidade não participante, serão observados os limites previstos no art. 32 do Decreto nº 11.462, de 2023.

8.5. Competirá ao órgão ou à entidade gerenciadora autorizar o remanejamento solicitado, com a redução do quantitativo inicialmente informado pelo órgão ou pela entidade participante, desde que haja prévia anuência do órgão ou da entidade que sofrer redução dos quantitativos informados.

8.6. Caso o remanejamento seja feito entre órgãos ou entidades dos Estados, do Distrito Federal ou de Municípios distintos, caberá ao fornecedor beneficiário da ata de registro de preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente do remanejamento dos itens.

8.7. Na hipótese da compra centralizada, não havendo indicação pelo órgão ou pela entidade gerenciadora, dos quantitativos dos participantes da compra centralizada, nos termos do item 8.3, a distribuição das quantidades para a execução descentralizada será por meio do remanejamento.

COLEGIO MILITAR DE BRASÍLIA
Fls. 548
Rub:

9. CANCELAMENTO DO REGISTRO DO LICITANTE VENCEDOR E DOS PREÇOS REGISTRADOS

9.1. O registro do fornecedor será cancelado pelo gerenciador, quando o fornecedor:

9.1.1. Descumprir as condições da ata de registro de preços, sem motivo justificado;

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

9.1.3. Não aceitar manter seu preço registrado, na hipótese prevista no artigo 27, § 2º, do Decreto nº 11.462, de 2023; ou

9.1.4. Sofrer sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021.

9.1.4.1. Na hipótese de aplicação de sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021, caso a penalidade aplicada ao fornecedor não ultrapasse o prazo de vigência da ata de registro de preços, poderá o órgão ou a entidade gerenciadora poderá, mediante decisão fundamentada, decidir pela manutenção do registro de preços, vedadas contratações derivadas da ata enquanto perdurarem os efeitos da sanção.

9.2. O cancelamento de registros nas hipóteses previstas no item 9.1 será formalizado por despacho do órgão ou da entidade gerenciadora, garantidos os princípios do contraditório e da ampla defesa.

9.3. Na hipótese de cancelamento do registro do fornecedor, o órgão ou a entidade gerenciadora poderá convocar os licitantes que compõem o cadastro de reserva, observada a ordem de classificação.

9.4. O cancelamento dos preços registrados poderá ser realizado pelo gerenciador, em determinada ata de registro de preços, total ou parcialmente, nas seguintes hipóteses, desde que devidamente comprovadas e justificadas:

9.4.1. Por razão de interesse público;

9.4.2. A pedido do fornecedor, decorrente de caso fortuito ou força maior; ou

9.4.3. Se não houver êxito nas negociações, nas hipóteses em que o preço de mercado tornar-se superior ou inferior ao preço registrado, nos termos do artigos 26, § 3º e 27, § 4º, ambos do Decreto nº 11.462, de 2023.

10. DAS PENALIDADES

10.1. O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no edital.

10.1.1. As sanções também se aplicam aos integrantes do cadastro de reserva no registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente após terem assinado a ata.

10.2. É da competência do gerenciador a aplicação das penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preço (art. 7º, inc. XIV, do Decreto nº 11.462, de 2023), exceto nas hipóteses em que o descumprimento disser respeito às contratações dos órgãos ou entidade participante, caso no qual caberá ao respectivo órgão participante a aplicação da penalidade (art. 8º, inc. IX, do Decreto nº 11.462, de 2023).

10.3. O órgão ou entidade participante deverá comunicar ao órgão gerenciador qualquer das ocorrências previstas no item 9.1, dada a necessidade de instauração de procedimento para cancelamento do registro do fornecedor.

11. CONDIÇÕES GERAIS

11.1. As condições gerais de execução do objeto, tais como os prazos para entrega e recebimento, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no Termo de Referência, ANEXO AO EDITAL.

11.2. No caso de adjudicação por preço global de grupo de itens, só será admitida a contratação de parte de itens do grupo se houver prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou a entidade.

Para firmeza e validade do pactuado, a presente Ata foi lavrada em 02 (duas) vias de igual teor, que, depois de lida e achada em ordem, vai assinada pelas partes e encaminhada cópia aos demais órgãos participantes (se houver).

Brasília-DF, ... de junho de 2024.

COLÉGIO MILITAR DE BRASÍLIA - CMB
Fls. 569
Rub:

THALES MOTA DE ALENCAR – Cel
REPRESENTANTE LEGAL DO CMB

XXXXXXXXXXXXXXXXXXX
REPRESENTANTE LEGAL EMPRESA

Anexo

Cadastro Reserva

Seguindo a ordem de classificação, segue relação de fornecedores que aceitaram cotar os itens com preços iguais ao adjudicatário:

Item do TR	Fornecedor (razão social, CNPJ/MF, endereço, contatos, representante)							
X	Especificação	Marca (se exigida no edital)	Modelo (se exigido no edital)	Unidade	Quantidade Máxima	Quantidade Mínima	Valor Un	Prazo garantia ou validade

Seguindo a ordem de classificação, segue relação de fornecedores que mantiveram sua proposta original:

Item do TR	Fornecedor (razão social, CNPJ/MF, endereço, contatos, representante)							
X	Especificação	Marca (se exigida no edital)	Modelo (se exigido no edital)	Unidade	Quantidade Máxima	Quantidade Mínima	Valor Un	Prazo garantia ou validade

LOGO MARCA DA EMPRESA

COLÉGIO MILITAR DE BRASÍLIA - CMB
Fls. 530
Rub:

Anexo IV – MODELO DE PROPOSTA DE PREÇO

PREGÃO ELETRÔNICO nº 01/2024
(Processo Administrativo n° 64250.011956/2023-72)

Item	Especificação	Un	Qnt	V. Unit R$	V. Total R$
1	Pontos de acesso para rede sem fio (indoor)	Un	60		
2	Pontos de acesso para rede sem fio (outdoor)	Un	06		
3	Firewall para alta disponibilidade	Un	01		
4	Sistema de energia ininterrupta (ups/ nobreak) 2000va	Un	30		
5	Sistema de energia ininterrupta (ups/ nobreak) 20kva	Un	01		
6	Switch de acesso l2+l3 48 portas 10/ 100/1000base-t	Un	10		
7	Switch 48 portas fiber com 2 portas uplink /stack qsfp28	Un	02		
8	Estação de trabalho do tipo desktop compacto tipo 1	Un	50		
9	Estação de trabalho do tipo desktop compacto tipo 2	Un	30		
10	Notebook	Un	60		
11	Câmere de videocon-ferência corporativa	Un	05		
12	Processador / geren-ciador para monitores de videowall	Un	01		
13	Monitor profissional para videowall	Un	08		
14	Suporte para monitor profissional para videowall	Un	08		
15	Projetor data show 4600 lumens	Un	60		
16	Projetor 12000 4k uhd laser	Un	02		
17	Adaptador display port/hdmi	Un	100		
18	Alicate de crimpar	Un	8		
19	Unidade de disco externo 2tb	Un	32		
20	Monitor 24"	Un	56		
21	Placa de video 1gb hdmi	Un	50		
22	Placa de rede padrão pci-express	Un	30		
23	Memória ram ddr3 8gb	Un	30		
24	Memóira ram ddr4 8gb po	Un	30		

Item	Especificação	Un	Qnt	V. Unit R$	V. Total R$
25	Álcool isopropílico	Un	12		
26	Licença office	Un	50		
Valor Total					

COLÉGIO MILITAR DE BRASÍLIA - CMB
Fls. 530V
Rub:

1. Prazo de validade da Proposta é de: 60 (sessenta) dias.

2. Dados da Empresa:
Endereço:
CEP:
Telefone:
E-mail:

3. Dados Bancários:

Nome do Banco:
Nr da Agência:
Nr da Conta:

4. Declaramos que nos preços cotados estão incluídas todas as despesas que, direta ou indiretamente, fazem parte do presente objeto, tais como gastos da empresa com suporte técnico e administrativo, impostos, seguros, taxas, ou quaisquer outros que possam incidir sobre gastos da empresa, sem quaisquer acréscimos em virtude de expectativa inflacionária e deduzidos os descontos eventualmente concedidos.

Local - UF, _____ de XXXXX de 2024.

Nome completo
Representante Legal da empresa

COLÉGIO MILITAR DE BRASÍLIA - CMB
Fls. 531
Rub.

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
COLÉGIO MILITAR DE BRASÍLIA

(Processo Administrativo nº 64250.011956/2023-72)

CERTIDÃO

1. Recebi o processo com o Numero Único de Protocolo (NUP) 64250.011955/2023-28, cujo obseto é registro de preços de materiais permanentes para atender as demandas da Colégio Militar de Brasília (CMB) e Unidades Gestoras Participantes, submetido análise jurídica da Advocacia Geral da União (AGU) conforme Documento Interno do Exército (DIEx) nº 10 SALC/DA/CMB, de 1º de abril de 2024.

2. Após analise jurídica pela AGU o processo foi devolvido conforme DIEx nº 524-CONJUR-EB, de 17 de abril de 2024, com os seguintes anexos:

2.1. Parecer n. 00112/2024/CGAO/SCGP/CCU/AGU, de 10 de abril de 2024.

2.2. DESPACHO n. 00148/2024/CGAO/SCGP/CCU/AGU, de 16 de abril de 2024 aprovando o parecer acima descrito com a seguinte recomendações abaixo transcrita:

> "I. Aprovo O Parecer n. 00112/2024/CGAO/SCGP/CCU/AGU, da lavra do Advogado da União Mário Henrique C. Gil Rodrigues, desta Coordenação-geral Jurídica de Aquisições.
>
> (...)
>
> 4. Em síntese, a manifestação consultiva arrematou no sentido da possibilidade jurídica do prosseguimento do processo, desde que Observadas as recomendações assinaladas no parecer, especialmente as que constaram dos itens 12, 23, 28, 38, 48, 52, 55, 58, 59, 60, 67, 72 e 78.
>
> (...)"

2.3. DESPACHO n. 00139/2024/DIAO/SCGP/CCU/AGU, de 17 de abril de 2024 aprovando o DESPACHO n. 00148/2024/CGAO/SCGP/CCU/AGU, de 16 de abril de 2024.

3. Diante do exposto acima segue abaixo as transcrições das recomendações e as suas respectivas respostas:

3.1. Item 12. "Entretanto, relativamente à certificação de observância quanto à autorização a que se refere o art. 3º do Decreto nº 10.193/2019, a letra "h" da fl. 13 do seq. 16 menciona o "limite e instância de governança previsto consoante § 3º, para contratos com valor igual ou inferior a R$ 1.000.000,00 (um milhão de reais)". Acontece que a presente contratação totaliza o montante de R$ 5.950.420,07 (cinco milhões, novecentos e cinquenta mil, quatrocentos e vinte reais e sete centavos),

devendo assim ocorrer a certificação de observância de limite e instância de governança consoante o § 2° do aludido art. 3" do Decreto n° 10.193/2019, referente a contratos com valor inferior a R$ 10.000.000,00 (dez milhões de reais)."

Resposta: Será cumprida a recomendação no momento da Assinatura do Termo Substitutivo/Termo de Contrato.

3.2. Item 52. "Diante de todo o exposto, e apesar dos aspectos técnicos envolvidos no docume avaliação cabe ao próprio órgão assessorado, entende-se que o TR, sob o ponto de vista for jurídico, não necessita de maiores ponderações ou medidas corretivas a serem empregadas, devendo-se apenas renumerar os seguintes subitens: 1.6; 5.9 e seguintes; 9.4 e seguintes; e 10.3.

Resposta: Foram ajustadas todas as numerações do TR, confome Fls. 471V, 472V, 478 e 478V.

3.3. Item 58. "No caso dos autos, o órgão não anexou documento comprobatório da realização do procedimento da IRP - não obstante a verificação de processo de Participação de Intenção de Registro de Preços do Instituto Federal de Educação, Ciência e Tecnologia do Ceará -, cabendo, portanto, providências corretivas.

Resposta: A consulta foi realizada em data oportuna porém o responsável não salvou a consulta, consequentemnte será corrido esse equivoco nos próximos processos.

3.4. Item 59. "Vale destacar que, conforme o art. 10 do decreto referido, os órgãos e as entidades de que trata o art. 1°, antes de iniciar processo licitatório ou a contratação direta consultarão as IRPs em andamento e deliberarão a respeito da conveniência de sua participação, sendo que essa deliberação deverá constar dos autos do processo de contratação.

Resposta: A consulta foi realizada em data oportuna porém o responsável não salvou a consulta, consequentemnte será corrido esse equivoco nos próximos processos.

3.5. Item 60. "Não consta dos autos que o órgão tenha consultado a existência de IRPs em andamento devendo, portanto, ser adotada medida corretiva concernente à consulta e deliberação a respeito da conveniência de sua participação.

Resposta: A consulta foi realizada em data oportuna porém o responsável não salvou a consulta, consequentemnte será corrido esse equivoco nos próximos processos.

3.6. Item 67. " Apesar disso, são necessárias as correções e aprimoramentos abaixo indicados:

a) Na capa incluir a entidade participante; e

b) quanto ao critério de julgamento, que poderá ser o de menor preço ou o de maior desconto (art. 6", XLI, da Lei n" 14.133/2021), a capa do edital chega a falar em "menor preço por item e grupo", e o item 8.1 do Termo de Referência estipula a "adoção do critério de julgamento pelo MENOR PREÇO". Acontece que a minuta de edital, em algumas passagens, a exemplo dos subitens 4.2, 4.12 e 5.9.3, deixa o critério de julgamento em aberto, o que deve ser remediado.

Resposta letra a: Foi incluído na Capa, conforme Fl. 461;

Resposta Letra b:

Subitem 8.1 do TR: permaneceu a "critério de julgamento pelo menor preço", Fl. 476;

Fm Adrisoni

Capa do Edital: foi ajustada a redação para "menor preço", conforme Fl. 461;

Subitem 4.2 do Edital: foi ajustada a redação "MENOR PREÇO", conforme Fl. 461;

Subitem 4.12 do Edital: O correto seria subitem 4.12.1. permaneceu a redação "MENOR PREÇO, conforme Fl. 374 e 463V;

Subitem 5.9.3 do Edital: foi excluido o subitem por se tratar de menor preço e não maior desconto, conforme Fl. 464;

3.7. Item 72. "É obrigatória a divulgação e a manutenção do inteiro teor do edital de licitação e dos seus anexos, incluído o termo de contrato, no Portal Nacional de Contratações Públicas (PNCP) e a publicação de extrato do edital no Diário Oficial da União, conforme determinam os art. 54, capta e § 1°, e art. 94 da Lei n° 14.133/2021. Enfatiza-se também que, após a homologação do processo licitatório, é obrigatória a disponibilização no referido Portal (PNCP) dos documentos elaborados na fase preparatória que porventura não tenham integrado o edital e seus anexos, conforme determina o art. 54, § 3°, da Lei n° 14.133/2021. Nesse sentido o órgão deve estar atento.

Resposta: Será atendido a recomendação no momento da divulgação do Edital no Diário Oficial da União e consequentemente o próprio sistema realizará a divulgação no PNCP

3.8. Item 78. "Nessa esteira, recomenda-se ao órgão assessorado que não inclua nos instrumentos de contratação números de documentos pessoais limitando-se a informar, no preâmbulo do ajuste, o nome do contratado.

Resposta: Foram excluídos os dados pessoais da Minuta da ATA de Registro de Preço e da Minuta do Contrato, Fls. 521 e 526.

3.9. Levando em consideração o conhecimento de um homem médio em Tecnologia da Informação chamou a atenção o valor e as quantidades estimadas do item 10 Notebook, **(Quantidade 60 e valor R$ 15.598,50)**, os demais quantitativos e valores não tenho conhecimento técnico consequentemente foi questinado o Setor Demandante por meio do DIEx constante da Fl. 436, sendo respondido por mei do DIEx contante da Fl. 437 contendo anexos constante nas Fls. 438 a 449 e 479 a 520.

3.9.1. Os valores totais dos itens 4, 8, 16, 17 e 26 estavão equivocados e foram corrigidos;

3.9.2. O valor e o quantitativo do Notebook foram reajustados; e

3.9.3. Consequentemente o valor total também teve que ser corrigidos.

3.10. Não foi encontrado a documentação referente ao Órgão Participante, consequentemente foram impressos e incluídos no Processo, conforme Fls. 450/459.

Brasília-DF, 7 de junho de 2024

ADELSON PEDRO DA SILVA – 1° Ten QAO
Chefe SALC

Resposta da Equipe de planejamento

3.11. Item 15. "Na especificação técnica do objeto a ser adquirido, recomenda-se utilizar o CATMAT Sustentável que permite identificar itens de materiais sustentáveis que poderão ser adquiridos em substituição a itens similares.

Resposta: Conforme Fl. 438.

3.12. Item 23. "No caso dos autos, não se identificou manifestação expressa quanto ao enquadramento do objeto da licitação como solução de TIC - não obstante a redação da Introdução ao Mapa de Gerenciamento de Riscos mencionar de passagem o fato de se tratar de "processo de contrafação de soluções de Tecnologia da Informação e Comunicação - TIC' (Seq. 3, fl. 44) -, fazendo-se necessária a respectiva correção do feito. No que se relaciona às vedações, compete à área técnica do assessorado atestar a respectiva observância quando da confecção dos documentos."

Resposta: Conforme Fl. 438.

3.12. Item 28. "No presente caso, não se localizou manifestação do órgão assessorado de que a pretendida contratação está em consonância com o PDTIC; está alinhada à Estratégia do Governo Digital; e que consta do Plano de Contratações Anual. Considerando a dispensabilidade de cumprimento ao disposto no Decreto n° 10.9472022 para o órgão assessorado, recomenda-se a correção instrutória apenas quanto à manifestação de alinhamento da contratação ao PDTIC e à Estratégia do Governo Digital."

Resposta: Conforme Fl. 438.

3.13. Item 32. " Recomenda-se que o órgão, sempre quando da realização do planejamento da contratação, consulte a página do Governo Digital - Contratações TI, que, dentre outras orientações, contempla um tópico específico denominado "Dúvidas sobre contratações de bens e serviços de TIC" (https://www.gov.br/governodigital/pt-becontratacoes/perguntas-e-respostas).

Resposta: Conforme Fl. 438V.

3.14. Item 38. "No presente caso, os servidores da área técnica e requisitante (devidamente designados) elaboraram o ETP, não tendo sido, contudo, **aprovado e assinado pela autoridade máxima da área de TIC**, o que deve ser corrigido. No que concerne ao conteúdo, apesar de se tratar de documento extremamente técnico, cuja avaliação cabe, em última instância, ao próprio órgão assistido, aparentemente o ETP contém as previsões necessárias, relacionadas no art. 18, § 1°, da Lei n° 14.133/2021 e especialmente no art. 11 da IN SGD/ME n° 94/2022.

Resposta: Conforme Fl. 438V.

3.15. Item 48. "No presente caso, apesar de o órgão ter realizado a pesquisa de preços, não parecem ter sido atendidas as exigências dos incisos V, VI e VIII do art. 30 da IN SEGES/ME n° 65/2021, o que se recomenda.

Resposta: Conforme Fl. 438V.

3.16. Item 55. "No caso dos autos, observa-se que o órgão assessorado, embora tenha adotado o procedimento do SRP, não consignou a hipótese de cabimento que fundamentou o respectivo enquadramento. Apesar disso, considerando o disposto no art. 3° do referido decreto, entende-se possível a adoção do procedimento, recomendando-se, porém, que o órgão corrija a instrução do feito em razão do princípio da motivação dos atos administrativos, insculpido no art. 2° da Lei n° 9.784/1999.

Resposta: Conforme Fl. 438V.

3.17. No tocante ao questionamento do Chefe da SALC

Resposta: Conforme Fl. 438V.

COLÉGIO MILITAR DE BRASÍLIA - CMB
Fls. 533
Rub:

DESPACHO DO ORDENADOR DE DESPESAS

1. Aprovo as respectivas respostas do Chefe da Salc e da Equipe de Planejamento;
2. Aprovo o Edital e seus anexos constante das Fls. 461/530V;
3. Autorizo a publicação no Diário Oficial da União e Jornal.

Brasília 10 de junho de 2024

THALES MOTA DE ALENCAR – Cel

Ordenador de Despesas

EM BRANCO