PROCESSO Nº. 3548807.425.00007034/2025-90

PREGÃO ELETRÔNICO Nº 35/2026

1. PREÂMBULO

1.1. A Prefeitura Municipal de São Caetano do Sul - PMSCS através da Secretaria Municipal de Gestão e Governo Digital, por intermédio do Departamento de Planejamento de Compras, Licitações e Contratos, mediante Pregoeiro(a), designado pela Portaria nº 43.939 de 17 de março de 2026, torna público, para conhecimento dos interessados, que realizará **PREGÃO**, a ser realizada por intermédio do sistema eletrônico de contratações da Prefeitura Municipal de São Caetano do Sul, com utilização de recursos de tecnologia da informação, denominada **PREGÃO ELETRÔNICO**, do tipo **MENOR PREÇO**, nos termos da Lei Federal nº 14.133/21 e seus atos regulamentadores, do Decreto Municipal nº. 12.176/2025, Lei Complementar Federal nº. 123/2006 e posteriores alterações e Lei Municipal 4660/2008 no que couber, de demais normas pertinentes e, subsidiariamente, os Princípios Gerais de Direito**.**

1.2. Em quaisquer das menções à Lei Federal 14.133/21, ou outras Leis Federais, Estaduais e Municipais, entende-se, neste instrumento convocatório, que estão implícitas todas as alterações e regulamentações em vigor dessas mesmas leis, independente de expressa citação neste sentido, quando da indicação do texto legal.

1.3. A sessão pública de processamento do Pregão Eletrônico será realizada no endereço eletrônico https://pregaoeletronico.saocaetanodosul.sp.gov.br/, mediante condições de segurança - criptografia e autenticação, em todas as suas fases, no dia **19 de agosto de 2026 às 09:30 horas**, e será conduzida pelo(a) Pregoeiro(a) com o auxílio da equipe de apoio, designados nos autos do processo em epígrafe e indicados no sistema pela autoridade competente.

1.4. A realização do certame em formato eletrônico atende ao disposto no art. 17, § 2º da Lei 14.133/21 e o sistema de pregão eletrônico da Prefeitura Municipal de São Caetano do Sul é certificado digitalmente por autoridade certificadora credenciada no âmbito da Infraestrutura de Chaves Públicas Brasileiras – ICP Brasil.

1.5. As propostas deverão obedecer às especificações deste instrumento convocatório e seus anexos e ser encaminhadas por meio eletrônico após o registro dos interessados em participar do certame e o credenciamento de seus representantes no Portal de Pregão Eletrônico da Prefeitura de São Caetano do Sul: https://pregaoeletronico.saocaetanodosul.sp.gov.br/

1.6. As empresas licitantes que desejarem poderão realizar **VISITA TÉCNICA** através de seu representante legal ou técnico, devidamente credenciado pela empresa, a fim de tomar ciência de todas as condições locais para o cumprimento das obrigações objeto da licitação, objetivando a adequada formulação da proposta comercial, não podendo alegar futuramente, em sendo contratado, desconhecimento das condições do objeto.

1.6.1. As visitas acontecerão necessariamente durante o período de publicação do edital, cujo agendamento deverá ser efetuado previamente de segunda a sexta feiras, das 09hs às 17hs, através do telefone 11-4233-4125, ou pessoalmente na sede do Departamento de Tecnologia da Informação – DTI, localizado na Rua Serafim Carlos, nº 571, Bairro São José, Cidade de São Caetano do Sul, ou através do e-mail: "dti.agendamento@saocaetanodosul.sp.gov.br".

2. O B J E T O

2.1. Constitui o objeto deste Pregão o **REGISTRO DE PREÇOS PARA O FORNECIMENTO DE EQUIPAMENTOS DE REDE LÓGICA COM E SEM FIO PARA OS DEPARTAMENTOS MUNICIPAIS, INCLUINDO TODO MATERIAL E SERVIÇOS NECESSÁRIOS PARA SUA INSTALAÇÃO,** cujas especificações técnicas e quantitativos encontram-se descritas no Anexo I – deste Edital.

3. CONDIÇÕES DO FORNECIMENTO, PRAZO DE VALIDADE DO OBJETO E VIGÊNCIA.

3.1. O(s) objeto(s) deverá(ão) ser fornecido(s) na forma estabelecida no Anexo I do presente Edital – Especificações Técnicas.

3.2. O(s) produto(s) deverá(ão) ser acondicionado(s) conforme previsto do Anexo I – Termo de Referência - atendendo as exigências da legislação vigente.

3.3. Se durante o prazo de garantia, o produto fornecido apresentar quaisquer problemas técnicos, vícios e/ou defeitos, a Detentora deverá providenciar o prazo de 05 (cinco) dias úteis, sem quaisquer ônus para a Contratante a substituição do produto, a partir do recebimento da comunicação emitida pela Contratante, sem prejuízo da aplicação de penalidade cabível conforme item 17 do Edital.

3.4. O prazo de vigência da presente Ata de Registro de Preços será de 12 (doze) meses, contados a partir da assinatura do instrumento contratual, podendo ser prorrogado, a critério das partes, nos termos do artigo 84 da Lei Federal nº 14.133/21.

3.4.1. Na hipótese de prorrogação da vigência da Ata de Registro de Preços, as quantidades inicialmente registradas serão renovadas, na sua totalidade, independentemente do quantitativo utilizado no período de vigência, não sendo possível cumular com as quantidades não utilizadas.

4. DOS ESCLARECIMENTOS OU DA IMPUGNAÇÃO AO ATO CONVOCATÓRIO

4.1. Qualquer pessoa é parte legítima para impugnar o edital de licitação por irregularidade na aplicação da Lei ou para solicitar esclarecimento sobre os seus termos, devendo protocolar o pedido até **3 (três) dias úteis** antes da data de abertura do certame.

4.2. Quaisquer pedidos de esclarecimentos em relação a eventuais dúvidas na interpretação deste edital, ou impugnações ao mesmo, deverão ser encaminhados à Diretoria de Planejamento de Compras, Licitações e Contratos desta Prefeitura, inseridos na plataforma de pregão eletrônico https://pregaoeletronico.saocaetanodosul.sp.gov.br/.

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

4.4. Todas as perguntas e respostas serão numeradas sequencialmente e serão consideradas como aditamentos a este instrumento convocatório, sendo juntadas ao respectivo processo licitatório.

4.5. Caberá ao agente de contratação designado responder os pedidos de esclarecimentos e julgar eventuais impugnações apresentadas em face do edital, subsidiado por manifestação da área técnica demandante.

4.5.1. O agente de contratação poderá solicitar manifestação técnica dos órgãos de assessoramento jurídico, do controle interno ou de outros setores do órgão ou da entidade, a fim de subsidiar sua decisão.

4.6. Acolhida a petição contra o ato convocatório, será designada nova data para a realização do certame.

4.7. Em caso de não solicitação, pelas empresas licitantes, de esclarecimentos ou informações, pressupõe-se que os elementos fornecidos são suficientemente claros e precisos, não cabendo, posteriormente, o direito a qualquer reclamação.

4.8. Não serão aceitas consultas, reclamações, impugnações ou questionamentos efetivados através de ligação telefônica ou consulta verbal.

5. CRITÉRIO DE JULGAMENTO E LANCE

5.1. O critério de julgamento adotado será o de **Menor Valor Total Global do Lote.**

5.2. Serão admitidos preços unitários expressos com até duas casas decimais, desprezando-se as demais.

6. DAS CONDIÇÕES PARA PARTICIPAÇÃO NA LICITAÇÃO

6.1. As licitantes interessadas em participar do presente certame, poderão retirar o Edital Completo e seus anexos por meio eletrônico, através do site da Administração (http://licitacao.saocaetanodosul.sp.gov.br/web/ e https://pregaoeletronico.saocaetanodosul.sp.gov.br) ou no Departamento de Planejamento de Compras, Licitações e Contratos da Prefeitura Municipal de São Caetano do Sul.

6.1.1. Os interessados em adquirir o Edital pessoalmente deverão, na ocasião da aquisição, disponibilizar mídia removível (pen drive).

6.1.2. É importante o acesso frequente à página eletrônica da Prefeitura, tendo em vista que eventuais questionamentos sobre edital e os devidos esclarecimentos serão divulgados por meio eletrônico, no endereço indicado, junto ao respectivo edital, não sendo aceitas alegações de desconhecimento.

6.2. O presente Edital se submete ao disposto na Lei Complementar 123/2006 e suas posteriores alterações, e aos termos da Lei Municipal 4660/08.

6.3. Poderão participar da presente licitação, as pessoas físicas e jurídicas que atenderem as exigências deste Edital.

6.4. Poderão participar do certame todos os interessados em contratar com a Administração Municipal que estejam cadastrados do Portal de Pregão Eletrônico de São Caetano do Sul, que atuem em atividade econômica compatível com o seu objeto, e tenham credenciado os seus representantes.

6.4.1. O registro no Portal de Pregão Eletrônico de São Caetano do Sul, o credenciamento dos representantes que atuarão em nome da licitante no sistema de pregão eletrônico e a senha de acesso deverão ser obtidos anteriormente à abertura da sessão pública e autorizam a participação em qualquer pregão eletrônico realizado por intermédio do Portal de Pregão Eletrônico de São Caetano do Sul.

6.4.2. O registro no Portal de Pregão Eletrônico de São Caetano do Sul é gratuito.

6.5. Poderão participar da licitação empresas brasileiras ou empresas estrangeiras pertencentes ao ramo do objeto licitado.

6.5.1. A participação de cooperativas obedecerá ao disposto no artigo 16 da Lei Federal nº

14.133, de 1º de abril de 2021.

6.6. Para a participação de consórcios, coloca-se a obrigatoriedade de observância aos seguintes termos:

6.6.1. Compromisso expresso, público ou particular, este com firma reconhecida por tabelião, de responsabilidade solidária de todos os consorciados pelos atos praticados pelo consórcio durante o processo licitatório e na execução do contrato, bem como pelos encargos fiscais e administrativos referentes ao objeto.

6.6.2. O nome da empresa líder e responsável pelo consórcio.

6.6.3. A proporção econômica e financeira da respectiva participação de cada consorciado.

6.6.4. Compromisso de que não haverá qualquer alteração na composição e constituição do consórcio, sem prévia anuência da Prefeitura de São Caetano do Sul, durante toda vigência do contrato a ser firmado.

6.6.5. Duração do consórcio por período equivalente ao contrato.

6.6.6. Fica vedada a participação de empresa consorciada, na mesma licitação, por meio de mais um consórcio ou isoladamente.

6.6.7. O licitante vencedor, quando se tratar de consórcio, fica obrigado a promover, antes da celebração do contrato, a constituição e o registro do consórcio, devendo apresentá-lo quando da convocação para assinatura desta.

6.6.8. Cada empresa consorciada deverá apresentar a documentação de habilitação.

6.7. Estão impedidos de participar de qualquer fase do presente processo os interessados que se enquadrarem em uma ou mais das seguintes condições:

a) Organizações Sociais;

b) Empresas estrangeiras que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

c) Pessoas físicas ou jurídicas que tenham sido declaradas inidôneas para licitar ou contratar nos termos dos §§ 4º e 5º do artigo 156 da Lei Federal 14.133/21. Se a punição vier a ocorrer durante o

andamento desse processo, esta Administração, assegurado o direito à ampla defesa, poderá excluir a empresa do certame;

c.1) O impedimento de que trata o item 'd' 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.

c.2) A idoneidade dos participantes será ser consultados os seguintes cadastros:

I - Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS);

II - Cadastro Nacional de Empresas Punidas (CNEP); e

III - Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa e Inelegibilidade (CNIA – CNJ).

IV – Relação de apenados do TCESP – Tribunal de Contas do Estado de São Paulo;

d) 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, devendo essa proibição constar expressamente do edital de licitação;

e) Empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

f) 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;

g) Autor do anteprojeto ou do projeto básico, pessoa física ou jurídica;

h) Empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico, 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.

i) Pessoa física ou jurídica, que estejam enquadradas nos termos do artigo 14 da Lei 14.133/21.

7. DA REPRESENTAÇÃO E DO CREDENCIAMENTO NO SISTEMA LICITAÇÕES

7.1. A participação da licitante no pregão eletrônico se dará por meio da Plataforma https://pregaoeletronico.saocaetanodosul.sp.gov.br na qual a licitante deverá manifestar, por meio de seu operador designado, em campo próprio do sistema, pleno conhecimento, aceitação e atendimento às exigências de habilitação previstas no edital.

7.1.1. A Plataforma de Licitações disponibilização para download e orientação dos fornecedores, o **"Manual do Fornecedor"**, que pode ser acessado por meio do site https://pregaoeletronico.saocaetanodosul.sp.gov.br **– ícone documentos – Pregão Eletrônico**

7.2. O acesso ao pregão, para efeito de encaminhamento de proposta de preço e lances sucessivos de preços, somente se dará mediante prévia definição de senha privativa.

7.3. A chave de identificação e a senha dos operadores poderão ser utilizadas em qualquer pregão eletrônico, salvo quando canceladas por solicitação do credenciado.

7.4. É de exclusiva responsabilidade do usuário o sigilo da senha, bem como seu uso em qualquer transação efetuada diretamente ou por seu representante, não cabendo a operadora da plataforma ou ainda a Prefeitura a responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

7.5. O credenciamento do fornecedor junto ao sistema eletrônico implica a responsabilidade legal pelos atos praticados e a presunção de capacidade técnica para realização das transações inerentes ao pregão eletrônico.

7.6. A licitante deverá promover a sua inscrição e credenciamento para participar do certame, através do Portal https://pregaoeletronico.saocaetanodosul.sp.gov.br, antes da data e do horário previsto no edital para o fim da inscrição e cadastramento da proposta de preços.

7.7. A participação no pregão está condicionada obrigatoriamente a inscrição e credenciamento do licitante e deverá ser requerido e acompanhado dos seguintes documentos:

7.7.1. Proposta de Preços, conforme modelo Anexo II.

7.7.2. Os licitantes enquadrados como ME / EPP deverão informar em campo próprio da plataforma, sob pena de perder o direito ao tratamento diferenciado.

7.7.3. O registro no Portal de Pregão Eletrônico de São Caetano do Sul é gratuito.

8. DA PROPOSTA DE PREÇOS

8.1. O encaminhamento de proposta para o sistema eletrônico pressupõe o pleno conhecimento e atendimento às exigências de classificação e habilitação previstas no edital.

8.2. O Licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.

8.3. Nos preços ofertados pelas licitantes deverão estar inclusos, entre outros, tributos (impostos, taxas, emolumentos, contribuições fiscais e parafiscais), encargos trabalhistas, previdenciárias, sociais, fiscais e comerciais, despesas operacionais, transporte, frete, carga e descarga, obrigações financeiras de qualquer natureza e demais componentes do custo da execução do objeto da presente licitação, de acordo com o Anexo II- Proposta Comercial.

8.4. A omissão de qualquer despesa necessária à perfeita realização do objeto será interpretada como não existente ou já incluída no preço, não podendo a empresa pleitear acréscimos. Da mesma forma, o preço apresentado deverá incluir todos os benefícios e despesas indiretos, os quais serão assim considerados. No caso de erros aritméticos, serão considerados pelo(a) Pregoeiro(a), para fins de seleção e contratação, os valores retificados.

8.5. A não apresentação da proposta comercial conforme exigido no item 8.2.1, a apresentação desta contendo vício insanável ou em caso de não adequação, poderá acarretar a DESCLASSIFICAÇÃO da licitante.

8.6. Serão corrigidos automaticamente quaisquer erros de soma e/ou multiplicação, bem como as divergências que porventura ocorrerem entre o preço unitário e o total do serviço, prevalecendo o unitário.

8.7. O operador credenciado deverá verificar a condição de enquadramento da empresa, nos termos da LCF 123/06 (ME/EPP), devendo informar em campo próprio da plataforma.

8.7.1. O licitante que não informar sua condição de enquadramento, antes do envio da proposta, perderá o direito ao tratamento diferenciado previsto na LCF 123/06.

8.7.2. O tratamento diferenciado dado à ME/EPP consta detalhado no item 10 deste edital.

8.8. O objeto ofertado deverá atender plenamente às especificações contidas nos Anexo I - Termo de Referência.

8.9. Não serão levadas em consideração quaisquer ofertas ou vantagens não previstas neste edital.

8.10. Serão desclassificadas as propostas que conflitem com as normas deste edital ou da legislação em vigor.

8.11. A validade da proposta será de no mínimo 60 (sessenta) dias, contados a partir da data limite para apresentação da proposta.

8.12. A inserção, pelo fornecedor, da proposta comercial, conforme o modelo do Anexo II do edital, no momento do cadastro para participação na licitação **não** configura identificação prévia da empresa, vez que este apenas será liberado para acesso do agente de contratação após a fase de lances, na etapa de negociação.

9. DA ABERTURA DAS PROPOSTAS, DOS LANCES E DO JULGAMENTO

9.1. A partir do horário previsto no edital e no sistema para cadastramento e encaminhamento da proposta inicial de preço, terá início à sessão pública do pregão eletrônico, com a divulgação das propostas de preços recebidas, passando o(a) Pregoeiro(a) a avaliar a aceitabilidade das propostas.

9.1.1. A análise das propostas pelo(a) Pregoeiro(a) se limitará ao atendimento das condições estabelecidas neste Edital e seus anexos e à legislação vigente, sendo desclassificadas e reprovadas as propostas que, respectivamente:

a) cujo objeto não atenda as especificações, prazos e condições fixados neste Edital;

b) apresentadas por licitante impedida de participar, nos termos do item 6 deste edital.

c) que apresentem preços unitários ou total simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos ou salários de mercado;

d) formuladas por licitantes participantes de cartel, conluio ou qualquer acordo colusivo voltado a fraudar ou frustrar o caráter competitivo do certame licitatório.

9.1.2. A desclassificação da proposta será fundamentada e registrada no sistema, acompanhado em tempo real por todos os participantes.

9.1.3. O sistema ordenará automaticamente as propostas classificadas pelo(a) Pregoeiro(a).

9.1.4. O licitante que tiver sua proposta desclassificada e desejar recorrer da decisão deverá observar o item 13 deste edital.

9.2. Classificadas as propostas, o(a) Pregoeiro(a) dará início à fase competitiva, oportunidade em que os licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico. A cada lance ofertado o participante será imediatamente informado de seu recebimento e respectivo horário de registro e valor.

9.2.1. **O valor de redução mínima entre os lances será de 1% e incidirá sobre o valor total global do lote.**

9.2.2. O licitante poderá oferecer valores iguais ou superiores ao menor já ofertado e registrado pelo sistema, observado o 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.

9.3. Com o intuito de conferir celeridade à condução do processo licitatório, quando houver, será permitido ao(a) Pregoeiro(a) a abertura e gerenciamento simultâneo da disputa de vários itens da mesma licitação.

9.3.1. Em regra, a disputa simultânea de itens obedecerá à ordem sequencial dos mesmos. Entretanto, o(a) Pregoeiro(a) poderá efetuar a abertura da disputa de lotes selecionados fora da ordem sequencial.

9.4. Nos termos do Inciso I do artigo 56 da Lei 14.133/21, será adotado o **modo disputa aberto**, o qual terá etapa de lances com duração de 15 (quinze) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 02 (dois) minutos do período de duração da sessão pública. A prorrogação automática da etapa de lances será de 02 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários. Não havendo novos lances no período de prorrogação a etapa de lances encerrar-se-á automaticamente, o(a) Pregoeiro(a) poderá, assessorado pela equipe de apoio, admitir o reinício da etapa de envio de lances, na situação prevista pelo § 4º do artigo 56 da Lei 14.133/21.

9.4.1. A situação prevista no item anterior e no § 4º do artigo 56 da Lei 14.133/21 se destina apenas a definir as posições posteriores a proposta melhor classificada, ou seja, nessa situação não serão admitidos lances menores do que o valor da proposta melhor classificada. Os demais licitantes poderão formular outros lances, inclusive intermediários entre si.

9.4.2. O(a) Pregoeiro(a) tem a ação de iniciar a fase de lances, depois todo processo é automático, conforme explanado acima.

9.4.3. O não oferecimento de lances no prazo específico destinado a cada licitante produz a preclusão do direito de apresentá-los. Os lances apresentados em momento inadequado, antes do início do prazo específico ou após o seu término serão considerados inválidos.

9.5. Durante o transcurso da sessão pública os participantes serão informados, em tempo real, do valor do menor lance registrado. O sistema não identificará o autor dos lances aos demais participantes.

9.6. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão Eletrônico, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances, retornando o Pregoeiro, quando possível, sua atuação no certame, sem prejuízos dos atos realizados.

9.7. Quando a desconexão persistir por tempo superior a dez minutos, a sessão do Pregão Eletrônico será suspensa e terá reinício somente após comunicação expressa aos operadores representantes dos participantes, através de mensagem eletrônica na caixa de mensagem (chat) ou e-mail divulgando data e hora da reabertura da sessão.

9.8. Devido a imprevisão de tempo extra, as Empresas participantes deverão estimar o seu valor mínimo de lance a ser ofertado, evitando assim, cálculos de última hora, que poderá resultar em uma disputa frustrada por falta de tempo hábil.

9.9. Para julgamento será adotado o critério de menor preço, observado o prazo para fornecimento, as especificações técnicas, parâmetros mínimos de desempenho e de qualidade e demais condições definidas neste edital.

9.10. O sistema informará, na ordem de classificação, todas as propostas, partindo da proposta de menor preço (ou melhor proposta) imediatamente após o encerramento da etapa de lances.

9.10.1. Em caso de empate entre duas ou mais propostas, serão utilizados os critérios de desempate estabelecidos pelo art. 60 da Lei 14.133/21.

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

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

9.12. O(a) Pregoeiro(a) anunciará a licitante detentora da proposta ou lance de menor valor, imediatamente após o encerramento da etapa de lances da sessão pública ou, quando for o caso, após negociação e decisão pelo(a) Pregoeiro(a) acerca da aceitação do lance de menor valor.

9.13. Com base na classificação a que alude o item 9.10, será assegurada às licitantes microempresas, empresas de pequeno porte e cooperativas que preencham as condições estabelecidas no artigo 34, da Lei Federal n° 11.488/2007, preferência à contratação, observadas as seguintes regras:

9.13.1. A microempresa, empresa de pequeno porte ou cooperativa que preencha as condições estabelecidas no artigo 34, da Lei Federal n° 11.488/2007, detentora da proposta de menor valor, dentre aquelas cujos valores sejam iguais ou superiores até 5% (cinco por cento) ao valor da proposta melhor classificada, será convocada pelo Pregoeiro para que apresente preço inferior ao da melhor classificada no prazo de 5 (cinco) minutos, sob pena de preclusão do direito de preferência. Caso haja propostas empatadas, a convocação recairá sobre a licitante vencedora de sorteio.

9.13.2. Não havendo a apresentação de novo preço, inferior ao preço da proposta melhor classificada, serão convocadas para o exercício do direito de preferência, respeitada a ordem de classificação, as demais microempresas, empresas de pequeno porte e cooperativas que preencham as condições estabelecidas no artigo 34, da Lei Federal n° 11.488/2007, cujos valores das propostas se enquadrem nas condições indicadas no item 9.13.1.

9.13.3. Caso a detentora da melhor oferta, de acordo com a classificação de que trata o item 9.10, seja microempresa, empresa de pequeno porte ou cooperativa que preencha as condições estabelecidas no artigo 34, da Lei Federal n° 11.488/2007, não será assegurado o direito de preferência, passando-se, desde logo, à negociação do preço.

9.14. Considerada aceitável a proposta de menor preço, obedecidas às exigências fixadas neste edital, o(a) Pregoeiro(a) passará para a etapa habilitação do licitante que a tiver formulado, para confirmação das suas condições habilitatórias.

10. DO TRATAMENTO DIFERENCIADO ÀS MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

10.1. O tratamento diferenciado conferido às empresas de pequeno porte e às microempresas de que tratam a Lei Complementar 123, de 14 de dezembro de 2006 alteradas pelas Leis Complementares 147/14 e 155/16, obedecerá ao disposto no art. 4º da Lei 14.133/21 e deverá seguir o procedimento descrito a seguir:

10.1.1. Os licitantes deverão indicar no sistema eletrônico de licitações, antes do encaminhamento da proposta eletrônica de preços, a sua condição de microempresa ou empresa de pequeno porte.

10.1.1.1. O licitante que não informar sua condição antes do envio das propostas perderá o direito ao tratamento diferenciado.

10.1.2. Ao final da sessão pública de disputa de lances, o sistema eletrônico detectará automaticamente as situações de empate a que se referem os §§ 1° e 2º do art. 44 da Lei Complementar 123/2006, de 14 de dezembro de 2006.

10.1.2.1. Considera-se empate aquelas situações em que as propostas apresentadas pelas microempresas e empresas de pequeno porte sejam iguais ou até 5% (cinco por cento) superiores à proposta mais bem classificada, quando esta for proposta de licitante não enquadrado como microempresa ou empresa de pequeno porte.

10.1.2.2. Não ocorre empate quando a detentora da proposta mais bem classificada possuir a condição de microempresa ou empresa de pequeno porte.

10.1.2.3. Caso ocorra a situação de empate descrita no item 10.1.2.1, o(a) Pregoeiro(a) convocará o representante da empresa de pequeno porte ou da microempresa mais bem classificada, imediatamente e por meio do sistema eletrônico, a ofertar lance inferior ao menor lance registrado para o item no prazo de 5 (cinco) minutos.

10.1.2.4. Caso a licitante convocada não apresente lance inferior ao menor valor registrado no prazo acima indicado, as demais microempresas ou empresas de pequeno porte que porventura possuam lances ou propostas na situação do item 10.1.2.1 deverão ser convocadas, na ordem de classificação, a ofertar lances inferiores à menor proposta.

10.1.2.5. A microempresa ou empresa de pequeno porte que primeiro aceitar apresentar lance inferior ao menor lance ofertado na sessão de disputa será considerada arrematante pelo(a) Pregoeiro(a), que encerrará a disputa do item na sala virtual, e que deverá apresentar a documentação de habilitação, conforme item 12 e subitens deste edital.

10.1.2.6. O não oferecimento de lances no prazo específico destinado a cada licitante produz a preclusão do direito de apresentá-los. Os lances apresentados em momento inadequado, antes do início do prazo específico ou após o seu término serão considerados inválidos.

10.1.2.7. Caso a proposta inicialmente mais bem classificada, de licitante não enquadrado como microempresa ou empresa de pequeno porte, seja desclassificada pelo(a) Pregoeiro(a), por desatendimento ao edital, essa proposta não é mais considerada como parâmetro para o efeito do empate de que trata esta cláusula.

10.1.2.8. Para o efeito do empate, no caso da desclassificação de que trata o item anterior, a melhor proposta passa a ser a da próxima licitante não enquadrada como microempresa, empresa de pequeno porte, observado o previsto no item 10.1.2.2.

10.2. O julgamento da habilitação das microempresas ou empresas de pequeno porte obedecerá aos critérios gerais definidos neste edital, observadas as particularidades de cada pessoa jurídica.

10.3. Havendo alguma restrição na comprovação da regularidade fiscal e trabalhista, será assegurado às microempresas ou empresas de pequeno porte um prazo adicional de 05 (cinco) dias úteis para a regularização da documentação, contados a partir do momento que o proponente for declarado vencedor e/ou comunicado pelo(a) Pregoeiro(a). O prazo de 05 (cinco) dias úteis poderá ser prorrogado por igual período se houver manifestação expressa do interessado antes do término do prazo inicial, devidamente justificada e autorizada pelo(a) Pregoeiro(a).

10.4. A não regularização da documentação, no prazo previsto no subitem anterior, implicará decadência do direito à contratação, sem prejuízo das sanções previstas no artigo 156, da Lei Federal

14.133/21, sendo facultado ao(a) Pregoeiro(a) convocar os licitantes remanescentes, na ordem de classificação, para a apresentar os documentos de habilitação, ou fracassar a licitação.

11. APRESENTAÇÃO DE CATÁLOGOS OU DATASHEET

11.1. Encerrada a fase de lances e negociação, o(a) Pregoeiro(a) convocará a licitante detentora da melhor oferta para anexar **no sistema** as documentações relacionadas a seguir, no prazo de **até 10 (dez) dias úteis**, sob pena de desclassificação:

11.1.1. **Deverão ser apresentados os catálogos ou datasheet dos equipamentos: switches, firewall, pontos de acesso indoor e outdoor, nobreaks e rack para comprovação dos equipamentos em atendimento ao Termo de Referência.**

11.1.2. Justifica-se a exigência de catálogos, para a comprovação de que os equipamentos fornecidos atendam as especificações técnicas mínimas desejadas para o projeto, podendo a licitante ofertar equipamento superior ao descrito para atendimento do objeto.

11.1.3. A exigência de apresentação de catálogos dos itens descritos, são considerados os mais importantes tecnicamente, sendo que a qualidade destes podem definir o resultado do projeto como bom ou ruim, sendo relevantes principalmente nos quesitos de especificação técnica, compatibilidade, funcionalidades e tecnologia desejada. Ainda que os equipamentos de fornecimento deste projeto visam a ampliação dos sistemas de rede logica municipal que é amplamente utilizada em todas as partições publica, neste caso, a execução incorreta da implantação e gerenciamento poderá afetar e paralisar a rede logica, dificultando a análise e resolução de problemas.

11.1.4. Assim, garantir que as licitantes ofertem os equipamentos que atendam tecnicamente ao exigido no Termo de Referência, além de uma necessidade é uma obrigação desta administração, corroborando assim, para a minimizar os riscos relacionados à segurança da informação e vazamentos de informações sensíveis e prejuízos à Administração.

11.1.5. O catálogo deverá possuir informações que permitam concluir que estes correspondem às especificações técnicas contidas no Anexo I, deste edital, não podendo conter emendas ou rasuras, sob pena de desclassificação da licitante.

11.1.6. O(s) catálogo(s) e similar(es) deverá(ão) ser preferencialmente em original, podendo ser impresso ou xerocopiado (legível) ou extraído da internet, contendo as características técnicas do produto ofertado.

11.1.7. O(s) catálogo(s) deverá(ão) estar escrito(s) em português.

11.1.8. Será desclassificada a licitante que deixar de inserir a documentação exigida dentro do prazo estabelecido.

11.1.9. A documentação anexada será submetida à análise pela área requisitante, que irá deliberar sobre sua aprovação ou reprovação, conforme os critérios técnicos definidos.

11.1.10. **Não serão recebidos documentos enviados após os respectivos prazos, bem como, encaminhados por correio, e-mail ou outro meio que não seja através da plataforma de licitações.**

12. DA HABILITAÇÃO

12.1. Considerada aceitável a oferta de menor preço, o (a) Pregoeiro(a) convocará a licitante detentora da melhor oferta para anexar no sistema os documentos de habilitação, nos termos do inciso II do artigo 63 da Lei 14.133/2021, no prazo de até 02 (duas) horas. Após, proceder-se-á análise os documentos de habilitação da licitante.

12.1.1. O prazo poderá ser prorrogado mediante solicitação ou a critério do agente de contratação.

12.2. Para fins de habilitação no presente pregão o(s) licitante(s) vencedor(es) deverá(ão) apresentar os documentos a seguir especificados, válidos na data de apresentação dos documentos de habilitação. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

12.3. Caso o licitante pretenda que um de seus estabelecimentos, que não o participante desta licitação, execute o futuro contrato, deverá apresentar toda documentação de habilitação de ambos os estabelecimentos. No momento do recebimento do objeto deste certame, as respectivas notas fiscais deverão ser da mesma empresa/CNPJ/endereço da que participou desse certame ou de seu estabelecimento (filial) que executou o contrato. Caso o licitante vencedor abra uma filial posteriormente ao certame para prestar o serviço no Município da contratante em razão do objeto contratual, aplicar-se-ão as regras citadas acima.

12.4. **HABILITAÇÃO JURÍDICA**

a) Registro comercial, no caso de empresa individual;

b) Ato constitutivo, estatuto social, contrato social ou sua consolidação e posteriores alterações contratuais, devidamente registradas na junta comercial e, em vigor e, no caso de sociedade por ações, ata do atual capital social acompanhado da ata de eleição de sua atual administração, registrados e publicados;

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

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

e) Declaração de comprovação de regularidade perante o Ministério do Trabalho, conforme modelo Anexo IV deste edital.

12.5. **REGULARIDADE FISCAL E TRABALHISTA**

a) Prova de inscrição no Cadastro Nacional de Pessoa Jurídica do Ministério da Fazenda (CNPJ/MF);

b) Prova de regularidade para com a Fazenda Federal, compreendendo certidão expedida pela Secretaria da Receita Federal – RFB e pela Procuradoria Geral da Fazenda Nacional – PGFN, referente a todos os tributos federais e à Dívida Ativa da União por elas administrados, abrangendo inclusive as contribuições sociais previstas nas alíneas ‘a’ a ‘d’ do parágrafo único do art. 11 da Lei nº 8.212, de 24 de julho de 1991;

c) Prova de regularidade para com a Fazenda Estadual, consistente na apresentação de certidão que comprove regularidade fiscal junto ao Estado ou Distrito Federal;

d) Prova de regularidade para com a Fazenda Municipal da sede da empresa licitante, consistente na apresentação de certidão de regularidade de débitos municipais mobiliários.

e) Certidão que comprove a regularidade relativa ao Fundo de Garantia por Tempo de Serviço (FGTS);

f) Certidão Negativa de Débitos Trabalhistas – CNDT, de acordo com a Lei Federal nº 12.440/2011, emitida pelo site http://www.tst.jus.br/certidao/ .

12.5.1. As provas de regularidades elencadas nas alíneas “b”, “c” e “d” acima, são exclusivamente relativas aos tributos pertinentes ao objeto licitado.

12.5.2. Serão aceitas certidões positivas com efeito de negativas.

12.5.3. As certidões que não trouxerem em seu conteúdo o prazo de validade, será considerado de 180 (cento e oitenta) dias.

12.6. **QUALIFICAÇÃO ECONÔMICA-FINANCEIRA**

a) Certidão negativa de feitos sobre falência, expedida pelo distribuidor da sede da licitante (TCs 00015330.989.25-2 e 00015441.989.25-8).

b) Capital social mínimo correspondente a R$ 822.365,60 (Oitocentos e vinte e dois mil, trezentos e sessenta e cinco reais e sessenta centavos) nos termos do artigo 69, §4º, da Lei Federal 14.133/2021, cuja comprovação será feita por meio do Contrato Social ou a última alteração contratual;

b.1) Para esta contratação, solicitaremos o percentual de capital social de 05% da estimativa do valor da contratação, com valor base proveniente das cotações previas que antecedem a licitação, estando de acordo com a legislação vigente, o valor será readequado conforme proposta vais vantajosa para cada lote na confecção do contrato final.

b.2) Para a contratação do objeto desejado, a Administração Pública deve adotar todas as cautelas necessárias para assegurar que a empresa contratada possua plena capacidade de executar o objeto em sua totalidade. Neste contexto, a exigência de comprovação de saúde financeira é um pilar para a mitigação de riscos e para a garantia do sucesso do projeto, evitando desabastecimento e prejuízos ao Município.

b.3) Desta forma, justifica-se a exigência de comprovação de Patrimônio Líquido Mínimo correspondente a 05% (cinco por cento) do valor estimado da contratação, sendo o percentual razoável e suficiente, sem prejudicar a participação das licitantes menores, porém baseada em fundamentos legais que estipula exigência de percentual de comprovação de capital social de até 10% da contratação.

b.4) Eventuais vistas do processo poderão ser solicitadas através da Lei de Acesso à Informação, mediante requerimento a ser protocolado junto ao Atende Fácil, sito à Rua Major Carlo Del Prete, nº 651, de segunda à sexta – feira, das 08:00 às 18:00, ou de forma eletrônica através do site: http://esic.saocaetanodosul.sp.gov.br/.

12.7. **QUALIFICAÇÃO TÉCNICA**

a) A comprovação de aptidão técnica para o presente fornecimento deverá ter quantidades e prazos compatíveis com aqueles estabelecidos neste Edital. A comprovação deverá ser feita por meio de atestado (s) fornecido(s) por pessoas jurídicas de direito público ou privado, competentes para tanto, sendo que os quantitativos mínimos de prova de execução obedecerão ao percentual mínimo de 50% (cinquenta por cento), nos termos da Súmula 24 do TCESP, **das seguintes parcelas de maior relevância:**

- **Fornecimento e instalação de Rede WiFi, com no mínimo 215 (duzentos e quinze) access points;**
- **Fornecimento e instalação de 01 (um) firewall de alta capacidade;**
- **Fornecimento e instalação de no mínimo 100 (cem) switches;**
- **Fornecimento e instalação de 01 (um) Solução de Gerenciamento;**
- **Fornecimento e instalação de 01 (um) Solução de análise de log;**

a.1) O(s) quantitativo(s), quando não mencionado(s) no(s) atestado(s), poderá(ão) ser comprovado(s) por quaisquer documentos, tais como: contrato(s), nota(s) fiscal(ais) ou outro(s) documento(s) equivalente(s).

12.8. Justificativa: A exigência de atestados de capacidade técnica, com comprovação de 50% do quantitativo desejado para contratação, dos itens de maior relevância e valor do projeto solicitados acima, baseia-se na necessidade de garantir que a contratada possua experiência real na implantação de sistemas equivalente aos desejados nesta contratação.

12.9. Ao comprovar tais fornecimentos anteriores através de tais atestados, os emissores atestam que os serviços foram prestados de acordo, minimizando a possibilidade de implantações mal executadas que podem prejudicar o resultado final desejado, considerando a qualidade almejada e o valor da contratação, minimizando eventuais prejuízos à esta administração.

12.10. Os itens a serem comprovados são considerados os mais importantes tecnicamente, estes que podem definir o resultado final do projeto como bom ou ruim, sendo relevantes principalmente nos quesitos de especificação técnica, compatibilidade, funcionalidades, tecnologia desejada.

12.11. A licitante poderá suprir eventuais omissões ou sanear falhas relativas ao cumprimento dos requisitos e condições de habilitação estabelecidos neste Edital mediante a apresentação de documentos, preferencialmente por correio eletrônico a ser fornecido pelo Pregoeiro no chat do sistema, desde que os envie no curso da própria sessão pública e antes de ser proferida decisão sobre a habilitação.

12.12. A verificação será certificada pelo(a) Pregoeiro(a) e deverá ser anexada aos autos os documentos passíveis de obtenção por meio eletrônico, salvo impossibilidade devidamente justificada.

12.12.1. A Administração não se responsabilizará pela eventual indisponibilidade dos meios eletrônicos no momento da verificação, ressalvada a indisponibilidade de seus próprios meios. Na hipótese de ocorrerem essas indisponibilidades e/ou não sendo supridas ou saneadas as eventuais omissões ou falhas, a licitante será inabilitada, mediante decisão motivada;

12.13. Os Documentos de Habilitação deverão estar devidamente autenticados, nos termos do artigo 12, inciso IV, da Lei 14.133/2021 ou por autenticação digital.

12.14. Para aferição da autenticidade e veracidade dos documentos de habilitação apresentados sem autenticação eletrônica, os mesmos deverão ser apresentados, na forma original ou cópia autenticada por tabelião de notas, no **DEPARTAMENTO DE PLANEJAMENTO DE COMPRAS, LICITAÇÕES E CONTRATOS, sito à Rua Eduardo Prado, nº 201, Bairro Santo Antônio, CEP 09581- 900, na cidade de São Caetano do Sul/SP**, em até **02 (dois) dias úteis** após o encerramento da sessão pública, sob pena de invalidade do respectivo ato de habilitação e aplicação das penalidades cabíveis;

12.14.1. Os documentos poderão ser apresentados mediante publicação em órgão da imprensa oficial, ou por cópia simples, desde que acompanhados dos originais para que sejam autenticados por servidor da administração, por cartório competente, por autenticação digital;

12.15. Caso a licitante classificada com o menor preço venha a desatender as exigências para a habilitação, o(a) Pregoeiro(a) examinará a melhor oferta subsequente e negociará com o seu autor, decidindo sobre sua aceitabilidade e, em caso positivo, verificando as condições de habilitação e assim sucessivamente, até a apuração de uma oferta aceitável cuja autora atenda aos requisitos de habilitação, caso em que será declarada vencedor.

13. DOS RECURSOS ADMINISTRATIVOS

13.1. Declarada(s) vencedora(s), o(a) Pregoeiro(a) informará às licitantes por meio de mensagem lançada no sistema que poderão manifestar imediata, sua intenção de interpor recurso, que deverá ser realizada por meio eletrônico, utilizando exclusivamente o campo próprio disponibilizado no sistema.

13.2. Havendo manifestação da intenção de interposição de recurso, será concedido o prazo de 03 (três) dias úteis para apresentação das razões recursais, ficando as demais licitantes, desde logo, convocados para apresentar contrarrazões em igual número de dias úteis (03), que contarão a partir do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos autos.

13.3. A formalização de recursos, observados os prazos legais, será dirigida à Diretoria do Departamento de Planejamento de Compras, Licitações e Contratos e será efetivada por meio de documento com identificação do Processo e número do Pregão devendo ser redigido ou anexado em campo específico do sistema, sob pena de decadência do direito de recorrer.

13.4. **A falta de manifestação imediata da licitante, bem como a não apresentação das razões recursais no prazo estabelecido no item 13.2, importará na decadência do direito de recurso e adjudicação do objeto pelo(a) Pregoeiro(a) à vencedora.**

13.5. O recurso contra decisão do(a) Pregoeiro(a) terá efeito suspensivo.

13.6. O acolhimento do recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

13.7. Não serão conhecidos os recursos interpostos após os respectivos prazos legais, bem como os encaminhados por correio, e-mail ou em desacordo com o estabelecido no item 13.1.

13.8. Decididos os recursos e constatada a regularidade dos atos praticados, a autoridade competente adjudicará e homologará o procedimento e determinará a convocação da(s) vencedora(s) para a assinatura do contrato/retirada da Autorização de Fornecimento ou Ordem de início de serviços.

14. DO CONTRATO

14.1. Para atendimento ao objeto desse certame licitatório será firmado instrumento contratual, se caso for, ou instrumento equivalente, com a empresa vencedora, sendo o adjudicatário chamado via telefone ou por e-mail, a celebrá-lo em até 05 (cinco) dias úteis, contados do recebimento do chamamento, sob pena de decair o direito ao fornecimento, sem prejuízo das sanções previstas no artigo 156 da Lei Federal 14.133/21.

14.2. **Como condição à contratação será realizada consulta para comprovação que a empresa não possui pendências junto ao Cadastro Informativo Municipal – CADIN MUNICIPAL, em atendimento ao disposto no artigo 3º, inciso I e parágrafo primeiro da Lei 5.581/2017, que disciplinam que a inclusão no CADIN impedirá a empresa de contratar com a Administração, inclusive daquelas que não se encontram sediadas neste município.**

14.2.1. **Comprovadas irregularidades perante o CADIN Municipal de São Caetano do Sul, a licitante deverá proceder a regularização, antecedendo a assinatura do instrumento contratual ou emissão da Autorização de Fornecimento / Ordem de Serviços, caso seja declarada vencedora.**

14.3. **Na assinatura do contrato, a licitante deverá apresentar/comprovar que possui em seu quadro de pessoal:**

14.3.1. **Relação do pessoal técnico especializado que executará os serviços nas dependências da CONTRATANTE.**

14.3.2. **01(um) Engenheiro de Engenharia Elétrica ou de Telecomunicações. Conhecimentos em operação e gerenciamento de serviços e redes de telecomunicações, sistemas de telefonia privada e pública. Registro profissional: inscrição no Conselho Regional de Engenharia e Arquitetura (CREA-SP) ou equivalente, com registro vigente e livre de impedimentos ou restrições para o exercício profissional. Experiência requerida: profissional sênior.**

14.3.3. **02(dois) Analistas Sênior: Recurso com sólida formação técnica em Elétrica ou Telecomunicações, especializado no planejamento, operação e manutenção de redes LAN, WAN e Wi-Fi de alta disponibilidade. Possuir experiência em redes IP multisserviços (Dados, Voz e Vídeo), protocolos de roteamento, switching e QoS,. Experiência requerida: profissional sênior com certificação em pelo menos uma das seguintes certificações: CCNP, FCP, ACMP, CWNP, HCIP ou equivalentes.**

14.3.4. **01 (um) Gerente de Projetos; O gerente de projetos será o ponto de contato com a equipe da Contratante, com certificado na modalidade Project Management Certificate – PMP ou certificação equivalente;**

14.3.5. **01(um) Profissional certificado na solução ofertada;**

14.4. **Na assinatura do contrato, a licitante deverá apresentar as seguintes certificações:**

1- ISO20000 - Gerenciamento de Qualidade de Serviços de Tecnologia da Informação;

2- ISO27001 - Segurança da Informação;

14.4.1. **Ambas as certificações deverão ser entregues na assinatura do contrato e deverão estar dentro do prazo de validade;**

14.5. Justifica-se a exigência das certificações ISO 20000 e ISO 27001 em serviços de manutenção de rede WiFi para as unidades da Administração Municipal, certificações diretamente ligadas a qualidade e

segurança dos serviços desejados.

14.6. A certificação ISO/IEC 20000 é o padrão internacional reconhecido para o gerenciamento de serviços de TI, e sua adoção assegura que a contratada disponha:

-Processos estruturados e avançados para planejamento, entrega, operação e melhoria contínua do serviço, garantindo alta disponibilidade e desempenho da rede WiFi.

-Gerencia adequadamente incidentes, mudanças e liberações, minimizando riscos de falhas que poderiam comprometer o acesso dos alunos e professores.

-Oferece transparência e controle por meio de acordos de níveis de serviço (SLAs), assegurando cumprimento das responsabilidades e expectativa exigidas se tratando de unidades educacionais.

-Aumenta a confiabilidade do serviço, fator decisivo para um ambiente educacional onde a conectividade contínua é fundamental para o aprendizado e uso de plataformas digitais.

14.7. Proteção e confidencialidade dos dados (ISO 27001):

A certificação ISO/IEC 27001 estabelece um sistema de gestão de segurança da informação (SGSI) que:

-Identifica e controla riscos relacionados à segurança da rede e dos dados trafegados, sobretudo dados pessoais sensíveis de alunos e funcionários.

-Implementa medidas técnicas e organizacionais para proteger a confidencialidade, integridade e disponibilidade da informação, alinhadas às melhores práticas globais.

-Garante a conformidade com a Lei Geral de Proteção de Dados (LGPD), que exige proteção rigorosa dos dados pessoais, evitando vazamentos e uso indevido.

-Confere credibilidade e segurança jurídica para a prestadora de serviço e para as unidades escolares, reduzindo o impacto de incidentes de segurança e protegendo direitos dos titulares dos dados.

14.8. Conformidade legal e reputacional:

A LGPD impõe obrigações claras para o tratamento seguro dos dados pessoais no ambiente educacional. A ISO 27001 fornece uma estrutura certificada para cumprir essas obrigações.

14.9. O uso do padrão ISO 20000 complementa a segurança com qualidade do serviço, criando um ambiente tecnológico robusto e confiável.

14.10. A exigência dessas certificações demonstra compromisso institucional com a qualidade e segurança, elevando a confiança dos pais, alunos e órgãos públicos.

14.11. Desta forma, dada a criticidade do serviço de manutenção de redes WiFi nas Escolas Municipais, onde o sigilo dos dados pessoais e a qualidade do serviço são primordiais, a exigência das certificações

ISO 20000 e ISO 27001, assegura a gestão eficaz e a excelência na prestação do serviço, promove a proteção integral dos dados sensíveis em conformidade com a LGPD e contribui para reduzir riscos operacionais, técnicos e jurídicos, agregando diferencial competitivo e confiabilidade ao serviço prestado.

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

14.13. Será facultado à Administração, quando o convocado não assinar o termo de contrato ou não aceitar ou não retirar o instrumento equivalente no prazo e nas condições estabelecidas, convocar os licitantes remanescentes, na ordem de classificação, para apresentar os documentos de habilitação nos termos definidos neste edital.

14.14. Até a assinatura do instrumento contratual a vencedora poderá ser desclassificada se a Prefeitura tiver conhecimento de fato desabonador à sua habilitação, conhecido após o julgamento, nos termos da Lei de Licitações.

14.14.1. Ocorrendo a desclassificação da proposta da licitante vencedora por fato referido no item anterior, a Prefeitura poderá convocar as licitantes remanescentes observando o disposto no item 14.4, supra.

15. DAS OBRIGAÇÕES DA DETENTORA E DA CONTRATANTE E DO RECEBIMENTO E FISCALIZAÇÃO DO OBJETO

15.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei 14.133/21, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

15.2. As obrigações da Contratante e da Detentora são as estabelecidas no Contrato.

15.3. Os critérios de recebimento e aceitação dos serviços ou materiais e de fiscalização, bem como as condições de pagamento, estão previstos no Contrato.

15.4. O recebimento dos bens e materiais será realizado pelos membros indicados pelas Portarias nº. 37.975/2022, em conformidade com o estabelecido no Decreto Municipal nº 10.728 de 24/01/2014;

15.5. A atestação do objeto contratado, somente ocorrerá se não houver a constatação de qualquer irregularidade. Em havendo irregularidades ou caso os itens apresentem qualquer problema de fabricação, ou estejam fora dos padrões determinados, a contratante solicitará a troca dos itens em até 10 (dez) dias

úteis, sem quaisquer ônus à Administração. O atraso na regularização acarretará as penalidades previstas no Edital.

15.6. O acompanhamento e a fiscalização da execução do contrato consistirão na verificação da conformidade da execução do objeto, dos materiais, técnicas e equipamentos empregados, de forma a assegurar o perfeito cumprimento do ajuste, que serão exercidos por representantes da CONTRATANTE, especialmente designados, na forma do art. 117 da Lei 14.133/21.

16. CONDIÇÕES DE PAGAMENTO E DA DOTAÇÃO ORÇAMENTÁRIA

16.1. Os pagamentos serão efetivados em até 30 dias contados da data em que for protocolada, na Secretaria Municipal da Fazenda, a certidão de autorização da liquidação e pagamento devidamente assinados pelo(a) Secretário(a) da unidade requisitante, conforme disposições contidas no Decreto 11.092/2017 e suas alterações.

16.1.1. Somente haverá a liberação, pela Secretaria Municipal da Fazenda, do pagamento devido à Detentora, quando da apresentação, pela Unidade Requisitante, de certidão devidamente assinada pelo Secretário, conforme disposições contidas na Portaria nº 18.279, de 06 de janeiro de 2005.

16.2. Havendo divergência ou erro na emissão do documento fiscal, fica interrompido o prazo para o pagamento, sendo iniciada a nova contagem somente após a regularização dessa documentação.

16.2.1. A pessoa jurídica pode possuir vários estabelecimentos comerciais que são partes integrantes de uma mesma empresa. Contudo, para fins de execução do contrato, a emissão das notas fiscais deve sempre considerar o estabelecimento que efetivamente executou o contrato, não sendo lícito adotar conduta distinta a esta.

16.3. Ocorrendo atraso na liberação do pagamento por motivo injustificado, a Contratante poderá incorrer em multa de mora correspondente a 0,01% (um centésimo de percentual), do valor a ser pago, por dia de atraso até seu efetivo pagamento.

16.4. Ocorrendo atraso na liberação do pagamento por motivo injustificado, poderá ser feita a correção monetária, calculada pelo IPCA, aplicada sobre os valores da parcela devida, por dia de atraso até seu efetivo pagamento.

16.5. Ocorrendo atraso na liberação por motivo injustificado, poderá ser feita a atualização monetária, calculada pelo IPCA, aplicada sobre os valores da parcela devida, por dia de atraso até seu efetivo pagamento.

16.6. Não será efetuado qualquer pagamento a CONTRATADA enquanto houver pendência de liquidação da obrigação financeira em virtude de penalidade ou inadimplência contratual.

16.7. Os pagamentos serão efetuados através de ordem de pagamento bancário para o qual deverão constar os dados bancários no corpo da nota fiscal.

16.8. Os preços ofertados serão fixos e irreajustáveis, observando o disposto da Lei Federal nº 10.192/2001, sendo que na hipótese de prorrogação contratual, após o período de 12(doze) meses, os preços poderão ser reajustados com base no índice do IPCA, ou outro índice que viera substituí-lo, mediante requerimento da Contratada.

16.8.1. A data-base a ser considerada para o reajustamento dos preços será a data de apresentação do orçamento estimados, nos termos do §7º do artigo 25 da Lei 14.133/2021.

16.9. Eventuais alterações contratuais serão regidas pela Lei Federal nº 14.133/202, bem como por normas regulamentadoras.

16.10. O procedimento de recomposição do equilíbrio econômico-financeiro disposto na alínea “d” do inciso II, do artigo 124 da Lei Federal nº 14.133/2021 poderá ser iniciado por requerimento da CONTRATADA/DETENTORA ou por determinação da CONTRATANTE.

16.11. As despesas com a execução do presente onerarão as dotações orçamentárias de n.º: **02.24.03.04.126.0170.2.063.3.3.90.30.00; 02.24.03.04.126.0170.2.063.3.3.90.39.00; 02.24.03.04.126.0170.2.063.4.4.90.52.00 - VERBAS DO TESOURO MUNICIPAL.**

17. **DAS SANÇÕES**

17.1. O licitante que, convocado dentro do prazo de validade da sua proposta, não celebrar ou não retirar o contrato; deixar de entregar ou apresentar documentação falsa exigida para o certame; ensejar o retardamento da execução de seu objeto; não mantiver a proposta; falhar ou fraudar na execução do objeto; comportar-se de modo inidôneo; cometer fraude fiscal; praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013; ou desatender aos prazos do item 6.1.6 deste instrumento convocatório - se micro empresa ou empresa de pequeno porte, garantido o direito prévio da citação e da ampla defesa, poderá sofrer as sanções previstas no artigo 156 da Lei 14.133/21, sem prejuízo das multas enumeradas abaixo e das demais cominações legais:

17.1.1. Multa de 10,5% (dez vírgula cinco por cento) sobre o valor total do contrato, pela recusa injustificada do adjudicatário em assinar, aceitar ou retirar o contrato, dentro do prazo estabelecido neste instrumento.

17.1.2. Multa de 10,5% (dez vírgula cinco por cento) sobre a parcela não executada do ajuste decorrente deste certame; ou por material não aceito pela contratante e não substituído no prazo fixado por esta, prazo este que não excederá 15 (quinze) dias úteis, contados da intimação.

17.1.3. Multa de 0,5% (zero vírgula cinco por cento) ao dia, por dia de atraso da obrigação não cumprida, até o trigésimo dia, configurando-se, após esse prazo, a hipótese de rescisão unilateral da avença por parte dessa Administração pela inexecução, parcial ou total, de seu objeto.

17.1.4. O pagamento dessas multas não exime a adjudicatária da reparação de eventuais danos, perdas ou prejuízos que seu ato punível venha a acarretar à contratante.

17.1.5. As multas, calculadas como acima, deverão ser recolhidas no prazo de 10(dez) dias corridos, a contar da data do recebimento da comunicação enviada por esta Administração.

17.1.6. As multas, calculadas como acima, poderão ser deduzidas, até seu valor total, de quaisquer pagamentos devidos à adjudicatária, mesmo que referentes a outras avenças, ou deduzidas de eventual garantia de contrato. Poderão, alternativamente, ser inscritas em Dívida Ativa para cobrança executiva ou cobradas judicialmente.

17.1.7. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

17.2. As decisões relacionadas a multas, penalidades e advertências, bem como as notificações dessas decisões, serão publicadas em diário oficial do município e encaminhadas via correios para as empresas sancionadas, garantindo o direito de ampla defesa, a contar da confirmação de recebimento da decisão.

18. DAS DISPOSIÇÕES GERAIS

18.1. A simples participação na presente licitação, caracterizada pela inscrição e credenciamento para participar do pregão, implica para a licitante a observância dos preceitos legais e regulamentares em vigor, bem como a integral e incondicional aceitação de todos os termos e condições deste edital, e de seus anexos, aos quais se submete; implica, também, no reconhecimento de que este instrumento convocatório, e seus anexos, caracterizaram perfeitamente o objeto do certame, sendo os mesmos

suficientes para a exata compreensão do objeto e para seu perfeito atendimento, não cabendo, posteriormente, o direito a qualquer indenização.

18.2. A fidelidade e legitimidade de todos os documentos, informações e declarações prestadas em atendimento às normas deste instrumento editalício sujeitam-se às penas da lei. A falsidade de qualquer documento ou a inverdade das informações nele contidas implicará na imediata desclassificação da licitante que o tiver apresentado, ou, caso tenha sido a vencedora, na rescisão do ajuste, sem prejuízo das demais sanções cabíveis.

18.3. Cada proponente arcará com todos os custos diretos ou indiretos para a preparação e apresentação de sua proposta, independentemente do resultado deste procedimento licitatório.

18.4. As comunicações decorrentes de eventuais recursos, bem como quaisquer outras comunicações, poderão ser disponibilizadas aos proponentes por qualquer meio de comunicação que comprove o recebimento ou ainda, dar-se-ão por meio de publicações em Diário Oficial do Município, ou ainda no site oficial desta Prefeitura, ou ainda, diretamente para cada uma das empresas participantes do certame.

18.5. Os casos omissos serão regulados pela legislação citada em 1.1 e 1.2, sendo apreciados e decididos pelo(a) Pregoeiro(a) ou Agente de Contratação, submetendo-os, conforme o caso, à apreciação da Autoridade Competente.

18.6. Para que o interessado proceda com “vistas” ao processo, deverá apresentar requerimento por escrito, assinado por quem de direito, além de documento de identificação pessoal, sendo que nesse ato será lavrado “termo de vistas ao processo”, o qual será devidamente datado e assinado pelo interessado e pelo funcionário que o recepcionou. Vistas aos autos ocorrerão sem retirada dos mesmos das dependências da Prefeitura.

18.7. O(a) Pregoeiro(a) ou Agente de Contratação e sua Equipe de Apoio, se entenderem conveniente ou necessário, poderão utilizar-se de assessoramento técnico e específico para tomar decisões relativas ao presente certame licitatório, o qual se efetivará através de parecer formal que integrará o respectivo processo.

18.8. As normas disciplinadoras deste pregão serão interpretadas em favor da ampliação da disputa, observada a igualdade de oportunidades entre as proponentes, sem comprometimento do interesse público, da finalidade e da segurança do procedimento e dos futuros ajustes dele decorrentes.

18.9. Em caso de dúvidas quanto à comprovação de horário de quaisquer eventos marcados para

este certame licitatório, prevalecerá o horário oficial de Brasília.

18.9.1 - Da contagem dos prazos estabelecidos neste edital e seus anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento e considerar-se-ão os dias consecutivos, exceto quando for explicitamente disposto em contrário. Só se iniciam e vencem os prazos em dias de expediente na Prefeitura.

18.10. Muito embora os documentos estejam apresentados de forma individualizada, todos eles se completam, sendo que cada proponente deve, para a apresentação de PROPOSTA DE PREÇOS e DOCUMENTOS DE HABILITAÇÃO, bem como eventuais outros documentos, ao se valer do edital, inteirar-se de sua composição, tomando conhecimento, assim, das condições administrativas e técnicas que nortearão o desenvolvimento do certame e a formalização da contratação, de sorte que todos os aspectos mencionados em cada documento deverão ser observados, ainda que não repetidos em outros.

18.11. O(a) Pregoeiro(a) ou Agente de Contratação conforme o caso poderá relevar aspectos puramente formais nas propostas e nos documentos de habilitação apresentados pelas licitantes, desde que não comprometa a lisura e o caráter competitivo desta licitação.

18.12. Será eleito o Foro da Comarca desta Administração, com renúncia a qualquer outro, por mais privilegiado que seja, para qualquer procedimento relacionado com o processamento desse certame licitatório, assim como ao cumprimento das obrigações dele decorrente.

Anexo I – Termo de Referência;
Anexo IA – Endereços da Prestação dos Serviços;
Anexo II – Proposta Comercial;
Anexo III – Modelo de Declaração de Microempresa e Empresa de Pequeno Porte;
Anexo IV – Modelo de Declarações de Regularidade Perante o Ministério do Trabalho e Relativas aos Artigos 63, Inciso IV e 68, Inciso VI da Lei Federal 14.133/21;
Anexo V – Modelo de Declaração de Adequação da Cooperativa a lei Federal 12.690/2012;
Anexo VI – Termo de Ciência e Notificação;
Anexo VII – Minuta de Contrato;
Anexo VIIA – Endereços da Prestação dos Serviços;

São Caetano do Sul, 31 de julho de 2026.

Carolina Morales Duwe
Diretora do Departamento de Planejamento
de Compras, Licitações e Contratos

PROCESSO Nº. 3548807.425.00007034/2025-90

PREGÃO ELETRÔNICO Nº 35/2026

ANEXO I – TERMO DE REFERÊNCIA

1. OBJETO:

1.1. Constitui o objeto deste Pregão o **REGISTRO DE PREÇOS PARA O FORNECIMENTO DE EQUIPAMENTOS DE REDE LÓGICA COM E SEM FIO PARA OS DEPARTAMENTOS MUNICIPAIS, INCLUINDO TODO MATERIAL E SERVIÇOS NECESSÁRIOS PARA SUA INSTALAÇÃO,** cujas especificações técnicas e quantitativos encontram-se descritas no Anexo I – deste Edital.

LOTE ÚNICO				
ITEM	**CÓDIGO**	**QUANTIDADE**	**UNIDADE**	**ESPECIFICACAO**
1	1.14.01.2228-0	123	UN	NOBREAK TIPO 1 - 1500VA . MAIORES INFORMAÇÕES NO MEMORIAL DESCRITIVO.
2	1.14.01.2384-7	400	UN	PROPAGADOR DE SINAL SEM FIO PARA TRANSMISSÃO E RECEPÇÃO TIPO I, CONFORME TERMO DE REFERÊNCIA
3	1.14.01.2385-5	30	UN	PROPAGADOR DE SINAL SEM FIO PARA TRANSMISSÃO E RECEPÇÃO TIPO II, CONFORME TERMO DE REFERÊNCIA
4	1.14.01.2387-1	200	UN	SWITCH TIPO I, CONFORME TERMO DE REFERÊNCIA
5	1.14.01.2393-6	123	UN	RACK 19" 8US, CONFORME TERMO DE REFERÊNCIA
6	1.14.01.2443-6	8.600	M	INFRAESTRUTURA TUBULAR COMPLETA INCLUSO ACESSORIOS PARA FIXACAO
7	1.14.01.2491-6	2	UN	FIREWALL NGF DE ALTA CAPACIDADE
8	1.14.01.2819-9	1	UN	PLATAFORMA DE AUTENTICAÇÃO E GERENCIAMENTO DA SOLUÇÃO DE SEGURANÇA
9	1.14.01.2820-2	1	UN	PLATAFORMA DE ANÁLISE DE LOG CENTRALIZADO DA SOLUÇÃO DE SEGURANÇA.
10	2.09.03.0187-7	2	XX	LICENCIAMENTO DO FIREWALL ALTA CAPACIDADE TIPO I - ATIVA AS FUNCIONALIDADES AVANÇADAS DO NGFW E ATIVA SUPORTE PELO PERÍODO DE 24 MESES.
11	2.09.03.0188-5	400	XX	LICENCIAMENTO DE SUPORTE JUNTO O FABRICANTE - PROPAGADOR DE SINAL TIPO I

12	2.09.03.01 89-3	30	XX	LICENCIAMENTO DE SUPORTE JUNTO O FABRICANTE - PROPAGADOR DE SINAL TIPO II
13	2.09.03.01 90-7	1	XX	LICENCIAMENTO DE SUPORTE JUNTO O FABRICANTE - PLATAFORMA DE AUTENTICAÇÃO E GERENCIAMENTO DA SOLUÇÃO DE SEGURANÇA
14	2.09.03.01 91-5	1	XX	LICENCIAMENTO DE SUPORTE JUNTO O FABRICANTE - PLATAFORMA DE ANÁLISE DE LOG CENTRALIZADO DA SOLUÇÃO DE SEGURANÇA
15	2.09.03.01 97-4	2	XX	INSTALACAO FIREWALL DE ALTA CAPACIDADE TIPO I
16	2.09.03.01 98-2	400	XX	INSTALACAO PROPAGADOR DE SINAL SEM FIO TIPO I - INDOOR
17	2.09.03.01 99-0	30	XX	INSTALACAO PROPAGADOR DE SINAL SEM FIO TIPO II - OUTDOOR
18	2.09.03.02 00-8	200	XX	INSTALACAO SWITCH GERENCIAVEL TIPO I
19	2.09.03.02 01-6	1	XX	INSTALACAO PLATAFORMA DE AUTENTICACAO E GERENCIAMENTO DA SOLUCAO DE SEGURANCA
20	2.09.03.02 02-4	1	XX	INSTALACAO PLATAFORMA DE ANÁLISE DE LOG CENTRALIZADO DA SOLUCAO DE SEGURANCA
21	2.09.03.02 03-2	123	XX	INSTALACAO RACK 19 POLEGADAS 8US
22	2.09.03.02 04-0	123	XX	INSTALACAO NOBREAK TIPO I - 1500VA
23	2.09.03.02 05-9	8.600	XX	INSTALACAO INFRAESTRUTURA DE COMUNICACAO LOGICA COMPLETA
24	2.09.03.02 31-8	12	XX	SERVICOS DE SUPORTE E MANUTENCAO PREVENTIVA E CORRETIVA

1.2. Este projeto contempla o fornecimento e instalação dos equipamentos, de forma que seja possível sua utilização logo após implantação.

1.3. Deverá ser contemplando todos os materiais e serviços necessários para a instalação e configuração dos equipamentos.

1.4. Após implantação, os equipamentos deverão estar prontos para o uso, devidamente instalados e configurados.

1.5. ESPECIFICAÇÕES TÉCNICAS DOS EQUIPAMENTOS E SISTEMAS DA REDE DE COMUNICAÇÃO

As configurações descritas são as mínimas solicitadas, sendo que a licitante poderá ofertar equipamento superior para atender o edital.

Os equipamentos ativos deverão estar em linha de produção pelo fabricante na data de entrega da proposta.

1.6. PROPAGADOR DE SINAL PARA TRANSMISSÃO E RECEPÇÃO TIPO I

Equipamento de Propagação de sinal para rede local sem fio, devidamente licenciado e configurável via software;
Deverá ser do mesmo fabricante da Controladora de fornecimento deste projeto;
Possuir no mínimo uma porta Ethernet 100M/1000M/2.5G/5.0G Multigigabit Ethernet (RJ45;
Possuir botão de Reset ou possibilitar reset através do injetor PoE;
Possuir Bluethoot integrado;
Possuir porta USB;
Possuir porta RS-232 RJ45 Serial Port;
Suportar ao menos as tecnologias 802.11 a/b/g/n/ac;
Suportar a tecnologia 802.11ax;
Suportar UL MU-MIMO; DL UM MIMO; BBS Coloring;
Possui recurso de economia de energia “Enhanced Target Wake Time(TWT)”;
Suportar OFDMA;
Possui recursos de monitoramento sem fio de varredura de APs não autorizados (Rogue Scan Radio), Varredura de pacotes (Packet Sniffer) e analisador de espectro (Spectrum Analyser);
O equipamento deve possuir 6 antenas, distribuídas da seguinte forma:

- 2 antenas Wi-Fi Dual Band (2.4GHz/5GHz)
- 2 antenas Wi-Fi na banda de 6GHz
- 1 antena BLE/ZigBee
- 1 antena GPS

Operar em Triband (2.4 Ghz, 5 Ghz e 6Ghz);

Radio 1: Frequência: 2.4GHz: Largura de canais: 20/40MHz / Modulação: BPSK, QPSK, 64/256/1024 QAM / MIMO 2x2;
Radio 2: Frequência: 5.0GHz: Largura de canais: 20/40/80/160MHz / Modulação: BPSK, QPSK, 16/64/256/1024/4096 QAM / MIMO: 2x2;
Radio 3: Frequency: 6.0Ghz: Largura de canais: 20/40/80/160/320mhz / BPSK, QPSK, 16/64/256/1024/4096 QAM / MIMO 2x2;

Taxa de dados: Radio 1 de até 688Mbps / Radio 2 até 2800Mbps e Radio 3 até 5700Mbps
Suportar 2x2 MIMO em 2.4Ghz, 5Ghz e 6Ghz;
Possuir ganho mínimo em 2,4 Ghz de 4.5 dBi;
Possuir ganho mínimo em 5 Ghz e 6Ghz de 5.0 dBi;
Suportar até 512 usuários por rádio (radio 1, radio 2 e radio 3);
Possuir suporte até 8 SSIDs;
Suporta SSID do tipo Local-Bridge, Mesh e Tunnel;
Suportas modulação 1024QAM;
Ser compatível com o padrão IEEE 802.3at PoE;
Conformidade com a IEEE 802.1q;
Suportar 802.11k;
Suportar 802.11v;
Suportar 802.11r;
Suportar WEP;
Suportar WPA2;
Suportar WPA3;
Suportar Autenticação IEEE 802.1X;
Suportar Autenticação por MAC Address;
Suportar Autenticação por Portal;
Suportar 802.11w;
Acompanha acessórios para fixação na parede e teto;
Acompanha injetor PoE bivolt automático, compatível com IEEE 802.3at, homologado pelo fabricante do access point.
Possui Led de indicação de funcionamento. A led pode ser mantida apagada;
Possuir homologação da ANATEL válida no momento da entrega dos equipamentos;
Certificação RoHS (materiais livre de substâncias perigosas) ou equivalente;
Certificação FCC (utiliza frequências dentro dos limites regulatórios) ou equivalente;
Atende certificação “UL2043 Plenum Material” de utilização de materiais não propagante a chamas ou equivalente;
Possibilita dispositivos habilitados se conectarem automaticamente no ponto de acesso próximo (Wi-Fi aliance Certified – Passpoint);
MTBF aproximado de 10 anos;
Temperatura de operação de 0ºC à 50ºC e armazenamento de -10ºC à 70ºC;
Humidade de 5% a 90% não condensado;
Consumo máximo de 16w em POE e 15w 12V DC;
Fornecido com licenciamento do tipo permanente para todas as funcionalidades solicitadas em nome da contratante.
Possui 24 meses de garantia, sendo 3 meses garantia legal mais 21 meses garantia estendida.

1.7. **PROPAGADOR DE SINAL PARA TRANSMISSÃO E RECEPÇÃO TIPO II (outdoor)**

Equipamento de Propagação de sinal para rede local sem fio, devidamente licenciado e configurável via software;

Deverá ser do mesmo fabricante da Controladora de fornecimento deste projeto;

Possuir no mínimo uma porta Ethernet 100/1000/ Base-T RJ45;

Possuir botão de Reset ou possibilitar reset através do injetor PoE;

Possuir Bluethoot integrado;

Possuir porta RS-232 Rj45 Serial Port;

Suportar ao menos as tecnologias 802.11 a/b/g/n/ac;

Suportar a tecnologia 802.11ax;

Suportar UL MU-MIMO; DL UM MIMO; BBS Coloring;

Possui recurso de economia de energia “Enhanced Target Wake Time(TWT)”;

Suportar OFDMA;

Possui recursos de monitoramento sem fio de varredura de APs não autorizados (Rogue Scan Radio), Varredura de pacotes (Packet Sniffer) e analisador de espectro (Spectrum Analyser);

Possuir 3 antenas internas + BLE, sendo 2 antenas dual band (WiFi) e antena BLE + 2.4ghz;;

Operar em Dual-Band (2.4 Ghz e 5 Ghz);

Radio 1: Frequência: 2.4GHz: Largura de canais: 20/40MHz / Modulação: BPSK, QPSK, 64/256/1024 QAM / MIMO 2x2;

Radio 2: Frequência: 5.0GHz: Largura de canais: 20/40/80MHz / Modulação: BPSK, QPSK, 64/256/1024 QAM / MIMO: 2x2;

Radio 3: Frequency: 2.4GHz, 5.0GHz, MIMO varredura frequência;

Taxa de dados: Radio 1 de até 574Mbps / Radio 2 até 1200Mbps e radio 3 varredura de frequência;

Suportar 2x2 MIMO em 2.4Ghz;

Suportar 2X2 em MIMO 5Ghz;

Possuir ganho mínimo em 2,4 Ghz de 10 dBi;

Possuir ganho mínimo em 5 Ghz de 10 dBi;

Suportar até 512 usuários por rádio (radio 1, radio 2);

Possuir suporte até 16 SSIDs;

Suporta SSID do tipo Local-Bridge, Mesh e Tunnel;

Suportas modulação 1024QAM;

Ser compatível com o padrão IEEE 802.3at PoE;

Conformidade com a IEEE 802.1q;

Suportar 802.11k;

Suportar 802.11v;

Suportar 802.11r;

Suportar WEP;

Suportar WPA2;

Suportar WPA3;
Suportar Autenticação IEEE 802.1X;
Suportar Autenticação por MAC Address;
Suportar Autenticação por Portal;
Suportar 802.11w;
Acompanha acessórios para fixação na parede e teto;
Acompanha injetor PoE bivolt automático, compatível com IEEE 802.3at, homologado pelo fabricante do access point.), tipo Gigabit Ethernet (GE);
Possui Led de indicação de funcionamento. A led pode ser mantida apagada;
Possuir homologação da ANATEL válida no momento da entrega dos equipamentos;
Certificação RoHS;
Possibilita dispositivos habilitados se conectarem automaticamente no ponto de acesso próximo (Wi-Fi aliance Certified – Passpoint);
MTBF aproximado de 10 anos;
Proteção contra surtos;
Proteção IP67;
Temperatura de operação de 0ºC à 60ºC e armazenamento de -10ºC à 70ºC;
Humidade de 10% a 90% não condensado;
Consumo máximo 17w;
Fornecido com licenciamento do tipo permanente para todas as funcionalidades solicitadas em nome da contratante.
Possui 24 meses de garantia, sendo 3 meses garantia legal mais 21 meses garantia estendida.

1.8. **SWITCH TIPO I**

Switch gerenciável, POE com no mínimo, 24 portas 1000Base-T e 4 portas 1GE SFP;
Possuir capacidade de associação das portas compatível com a norma IEEE 802.3ad.
Possuir, 24 portas UTP (RJ45) PoE+ e, pelo menos, 4 portas óticas (podendo ser combo) com suporte a módulos de fibra multimodo e monomodo (SFP).
Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);
Deve ser capaz de alimentar as 24 portas com IEEE 802.3af e IEEE 802.3at.
As interfaces 10/100/1000 devem obedecer às normas técnicas IEEE802.3, IEEE802.3u (100BaseTX) e 802.3ab (1000BaseT);
Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas.
Implementar VLANs por porta.
Implementar VLANs compatíveis com o padrão IEEE 802.1q.
Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk 802.1q.

Possuir porta de console para gerenciamento e configuração via linha de comando CLI com conector RJ-45 ou conector padrão RS-232 ou USB;
Possuir interface USB para conexão de flash drive que permita cópias de arquivos de configuração e imagens de software para upgrades.
Possuir capacidade de empilhamento de até 9 unidades.
Possuir fonte de alimentação AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz).
Deverá ser fornecido cabo de alimentação padrão Brasil;
Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.
Deve possuir no máximo 1 Rack Unit (RU).
Possuir LEDs para a indicação do status das portas.
Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.
Possuir suporte a MIB II, conforme RFC 1213.
Possuir armazenamento interno das mensagens de log;
Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU;
Implementar nativamente RMON (History, Statistcs, Alarms e Events);
Implementar os protocolos LLDP (IEEE 802.1AB) e LLDP-MED, com auto negociação de energia para PoE.
O equipamento deve suportar para gerência e administração o uso dos protocolos: SNMP, NTP, HTTPS, SSH, Telnet e RADIUS;
Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet.
Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP.
Permitir a gravação de log externo (syslog).
Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
Permitir o espelhamento do tráfego de uma porta;
Implementar funcionalidade de QoS;
Deve permitir configuração de Vlan centralizado;
Implementar o protocolo NTP (Network Time Protocol);
Implementar DHCP Relay e DHCP Server;
Implementar roteamento estático IPv4;
Implementar roteamento estático IPv6;
Implementar roteamento entre VLANs
Possuir capacidade para pelo menos 32.000 endereços MAC.
Implementar, no mínimo, 4000 VLANS simultaneamente.

Deve possuir capacidade de comutação de no mínimo 128Gbps.
Deve possuir taxa de encaminhamento de no mínimo 190Mpps.
Suportar Jumbo frames.
Implementar filtragem de pacotes (ACL - Access Control List) IPv4 e IPv6.
Implementar o protocolo SSH para acesso à interface de linha de comando.
Implementar mecanismos de autenticação RADIUS Accounting;
Possuir controle de broadcast, multicast e unicast.
Possuir suporte a mecanismo de proteção “Spanning-Tree”;
Implementar padrão IEEE 802.1d;
Implementar padrão IEEE 802.1q;
Implementar padrão IEEE 802.1p;
Implementar padrão IEEE 802.3ad;
Implementar controle de acesso por porta, usando o padrão IEEE 802.1x;
Suportar a autenticação 802.1x via endereço MAC;
Implementar padrão IEEE 802.1w
Implementar padrão IEEE 802.1s
Implementar o protocolo IGMP Snooping;
Implementar interface do switch o protocolo MLD (Multicast Listener Discovery).
Implementar DSCP;
Suporte aos mecanismos de QoS WRR (Weighted Round Robin) ou SRR (Shaped Round Robin).
Implementar IPv6.
Implementar ICMPv6;
Possuir os seguintes protocolos: Ping e Traceroute
HTTP sobre IPv6.
Implementar funcionalidade de provisionamento simplificado do tipo zero-touch.
Implementar funcionalidade OPS (Open Programmability System) ou similar que permita o uso de scripts python para funções de operação e manutenção.
Implementar Sflow ou Netstream ou Netflow Lite ou protocolo equivalente.
Implementar QinQ.
Implementar os protocolos de roteamento RIPv2 e OSPF.
Implementar no mínimo 16.000 rotas em IPv4.
Implementar no mínimo 2.000 ACLs.
Fornecido com licenciamento do tipo permanente para todas as funcionalidades solicitadas em nome da contratante.
Acompanha fonte instalada dimensionada para alimentar simultaneamente todas as 24 portas PoE (802.3af/802.3at) totalizando até 370w;
Consumo máximo de 452w;
Temperatura de funcionamento de 0°C até +45°C.

Fluxo de ar Lateral para traseira;
Peso aproximado de 3,9Kg;
Nível de barulho até 45.8dBA;
Certificação RoHS2 / FCC ou equivalente;
Deve possuir homologação ANATEL válida.
Possui 24 meses de garantia, sendo 3 meses garantia legal mais 21 meses garantia estendida.

1.9. **FIREWALL DE ALTA CAPACIDADE TIPO I**

Firewall de nova geração (NGFW), deverá ser instalado na localidade DTI – Departamento de Tecnologia da Informação.

Especificações técnicas:
Deverá possuir as seguintes interfaces:
-1 porta de 2.5/GE RjJ45 HA Port;
-1 porta GE RJ45 para gerenciamento;
-16 portas GE RJ45;
-8 portas GE SFP (Slots);
-4 slots 10GE/GE (slots SFP+/SFP);
-4 slots de baixa latência de 25GE/10GE (SFP28/SFP+);
-2 portas USB;
-Acompanha 8 transceivers de 1GE SFP instalado;
-Acompanha 4 transceivers de 10GE SFP+ instalado;
-Possui 2 (duas) fontes instaladas do tipo Hot Swap;
-Possui 2 (dois) ventiladores internos instalados;
-Possui armazenamento interno com no mínimo 2 unidades armazenamento com capacidade de 480GB cada;
-Possui modulo TPM instalado;
-Possui Bluetooth Low Energy (BLE);

O Firewall deverá implementar a seguinte performance:
-Throughput do Firewall (pacotes por segundo)– 229Mbps
-Throughput do Firewall IPV4 (1518/512/64 bytes em UDP) 164/163/153Gbps;
-Latência de 3.8/2.5us (64 bytes/UDP)
-Sessões simultâneas – 16 milhões;
-Novas sessões por segundo – 720.000;
-Throughput do IPS (us misto) – 42Gbps
-Throughput de proteção NGFW: 30Gbps.(com log habilitado, firewall, application control e proteção de malware habilitados)

-Throughput contra ameaças (Threat): 30Gbps.
-Politicas de Firewall: 50.000;
-IPSEC VPN Throughput (512 byte): 55Gbps.
-Ipsec túneis VPN – 2000;
-Usuários VPN SSL simultâneos: 10.000;
-Inspeção SSL Throughput: 16.7Gbps;

Possui funcionalidade de controladora de pontos de acesso integrado;
A solução ofertada deve permitir o gerenciamento de até 2.048 pontos de acesso, garantindo escalabilidade para o ambiente.
Possibilitar controlador e gerenciar a rede sem fio e os equipamentos de rede sem fio de fornecimento deste projeto.
Possibilita configuração em alta disponibilidade nos modos ativo-ativo/ cluster ou Ativo-passivo;
Equipamento específico para montagem em rack de telecomunicação padrão 19 polegadas com altura de no máximo 2Us de rack;
Alimentação bivolt automático;
Acompanha cabo de alimentação elétrica padrão brasileiro;
Consumo médio /máximo aproximado: 184w/323w;
Possui duas fontes instaladas padrão 80Plus ou superior;
Temperatura de operação: 0ºC a 45ºC;
Humidade: 10% a 90% não condensado;
Deverá possuir Certificação ANATEL válida;
Possui 24 meses de garantia, sendo 3 meses garantia legal mais 21 meses garantia estendida.

Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;

Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.

CARACTERÍSTICAS GERAIS
A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open source (produto montado);

Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

Deve possuir garantia do fabricante com validade mínima de 24 (vinte e quatro) meses;

As funcionalidades de segurança que compõem a solução podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação, acompanhem os mesmos termos de garantia, atualizações e manutenção, e suportem gerenciamento centralizado;

A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
Todos os equipamentos fornecidos não devem ultrapassar a medida máxima de 1U cada;
O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
Os dispositivos de proteção de rede devem possuir suporte a Vlans;
Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

Recursos
Deve possibilitar melhorar a qualidade e disponibilidade de aplicações de voz;
Deve suportar BGP, OSPF, RIP e roteamento estático;
Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
Deve suportar NAT dinâmico (Many-to-Many);
Deve suportar NAT estático (1-to-1);
Deve suportar NAT estático bidirecional 1-to-1;
Deve suportar Tradução de porta (PAT);
Deve suportar NAT de Origem;
Deve suportar NAT de Destino;
Deve suportar NAT de Origem e NAT de Destino simultaneamente;
Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
Deve suportar NAT64;
Deve implementar o protocolo ECMP;
Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
Enviar log para sistemas de monitoração externos;
Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
Proteção anti-spoofing;
Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo layer 3;
A configuração em alta disponibilidade deve sincronizar: Sessões;
A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;
A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;
O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
Deve possuir suporte à criação de sistemas virtuais (VDOMs) no mesmo appliance;
Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
Controle, inspeção e descriptografia de SSL para tráfego de Saída (Outbound), devendo suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);

Políticas
Deverá suportar controles por zonas de segurança;
Deverá suportar controles de políticas por porta e protocolo;
Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);
Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2;
Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
Suporte a objetos e regras IPV6;
Suporte a objetos e regras multicast;
Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

Aplicações
Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
Reconhecer pelo menos 5.500 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
Deve suportar a decriptografia do tráfego SSL (IPv4 e IPv6) e espelhar este tráfego para uma interface específica.
Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;
Identificar o uso de táticas evasivas via comunicações criptografadas;
Atualizar a base de assinaturas de aplicações automaticamente;
Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
Deve permitir exceções de aplicações caso uma regra de controle de aplicação seja configurada para permitir ou bloquear uma categoria de aplicação.
O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
Deve alertar o usuário quando uma aplicação for bloqueada;

Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts e bloquear a chamada de vídeo;
Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação e categoria da aplicação;
Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.

Controladora Wireless;
Solução que deverá administrar e controlar de maneira centralizada os pontos de acesso wireless do mesmo fabricante da solução ofertada, caso seja necessário alguma solução como complemento a mesma deve ser fornecida em conjunto com o Firewall e os valores inclusos no seu valor final.
Deve ser fornecido na forma de appliance físico composto pelo conjunto de hardware e software;
Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;
Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;
A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;
A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;
O contradora wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless.

Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso;
Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;
Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;
Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;
Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;
A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;
A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;
A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;
A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;
A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;
A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o

MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;
A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;
A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexbilidade no design da rede wireless;
A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;
A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;
A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;
A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;
A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;
A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual

está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;
Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;
A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;
A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;
A solução deve suportar a configuração do BLE (Blueooth Low Energy) nos pontos de acesso que tenham este recurso;
A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;
A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;
A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;
A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;
A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;
A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;
A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;
A solução deve implementar recurso para controle de URLs acessadas na rede wireless através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários e SSID;
A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede wireless;
O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria;
A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas;

A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução;
A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento;
A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e para websites/domínios específicos;
A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS;
A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede wireless com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig;
O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6;
A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução;
A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede wireless;
A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução;
A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações;
A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI;
A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada SSID;
A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS;
A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless;
"A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:
Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);
Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;
ASLEAP;
Null Probe Response or Null SSID Probe Response;

Long Duration;
Ataques contra Wireless Bridges;
Weak WEP;
Invalid MAC OUI.
A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;
A solução deve implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede wireless;
Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;
Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS;
Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
A solução deve permitir a configuração de múltplas chaves de autenticação PSK para utilização em um determinado SSID;
Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;
A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;
Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;
A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
A solução deve permitir a configuração do captive portal com endereço IPv6;
A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;

A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;
A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;
A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;
A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;
A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;
A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;
A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;
A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;
A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;
A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);
A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;
A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;
A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;
A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;
A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;
A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;

A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;
A solução deve possuir ferramentas de diagnósticos e debug;
A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;
A solução deve suportar comunicação com elementos externos através de REST API;
A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;

Prevenção de ameaças
Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e colocar em quarentena o IP do atacante por um intervalo de tempo;
As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
Deve ser possível criar uma assinatura de IPS utilizando o identificador CVE assim como um “wildcard” do CVE para abranger mais de um identificador.
Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
Deve permitir o bloqueio de vulnerabilidades;
Deve permitir o bloqueio de exploits conhecidos;
Deve incluir proteção contra-ataques de negação de serviços;
Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
Detectar e bloquear a origem de portscans;
Bloquear ataques efetuados por worms conhecidos;
Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
Possuir assinaturas para bloqueio de ataques de buffer overflow;
Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
Identificar e bloquear comunicação com botnets;
Registrar no console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
Os eventos devem identificar o país de onde partiu a ameaça;
Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;
A solução de sandbox deve ser capaz de criar assinaturas e ainda inclui-las na base de antivírus do firewall, prevenindo a reincidência do ataque;
A solução de sandbox deve ser capaz de incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas (Block list), impedindo que esses endereços sejam acessados pelos usuários de rede novamente;
Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;
A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado;

Filtro de URLs

Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall;
Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
Possuir pelo menos 60 categorias de URLs;
Deve possuir a função de exclusão de URLs do bloqueio;

Permitir a customização de página de bloqueio;

Identificação de usuários
Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 e mais atuais;
Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;
Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
Deve 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);
Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

Filtro de dados
Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

Geolocalização

Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

VPN

Suportar VPN Site-to-Site e Cliente-To-Site;

Suportar IPSec VPN;

Suportar SSL VPN;

A VPN IPSec deve suportar 3DES;

A VPN IPSec deve suportar Autenticação MD5 e SHA-1;

A VPN IPSec deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

A VPN IPSec deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

A VPN IPSec deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

A VPN IPSec deve suportar Autenticação via certificado IKE PKI;

Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB ou agente VPN;

A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente de VPN;

Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

Atribuição de DNS nos clientes remotos de VPN;

Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

Suportar autenticação via AD/LDAP, certificado e base de usuários local;

Suportar leitura e verificação de CRL (certificate revocation list);

Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

Deve suportar que a conexão com a VPN seja estabelecida das seguintes formas: Antes do usuário autenticar na estação;

Deve suportar que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;

Deve suportar que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;

Deverá manter uma conexão segura com o portal durante a sessão;

O agente de VPN deve ser compatível com pelo menos: Windows10/11 e Mac OS 10.14 e superior.

Funcionalidades de gerenciamento avançado NGFW:
O equipamento deverá ser licenciado com todas as funcionalidades NGFW para o período de 24 meses, sendo possível sua renovação recorrentemente através de renovação de licença.

1.10. PLATAFORMA DE AUTENTICAÇÃO E GERENCIAMENTO

A solução deve ser baseada em appliance físico do mesmo fabricante da solução de NGFW e ter como objetivo a coleta, armazenamento e análise automatizada de registros e gestão WLAN em modo centralizado de todos os equipamentos a partir de uma única console de administração;
Deverá estar devidamente licenciada para:
Suportar a coleta de, no mínimo, 100 GB de logs diários;
Possuir e permitir espaço de armazenamento de, no mínimo, 10 TB;
O apliance deve suportar:
Pelo menos duas interfaces 2x GE RJ-45
Suportar a configuração de RAID 0 e 1 para os discos internos;
Possuir 2 fontes de alimentação interna, redundante e hot-swap;
Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
Possui 24 meses de garantia, sendo 3 meses garantia legal mais 21 meses garantia estendida.
Realizar o backup das configurações para permitir o retorno de uma configuração salva;
Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;
Deve suportar a definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.
A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;
Através da análise de tráfego de rede, web e DNS, deve suportar a verificação de máquinas potencialmente comprometidas ou usuários com uso de rede suspeito;
Realizar agregação via pontuação, para geração de um veredito sobre máquinas comprometidas na rede e atividades suspeitas;
Utilizar técnicas de machine learning para a captura de índices de comprometimento, através de URLs, domínios e endereços IPs maliciosos;
Deve possuir um painel com as informações de máquinas comprometidas indicando informações de endereço IP dos usuários, veredito, número de incidentes etc.;
Deve oferecer um portal do cliente fácil de usar, permitindo acesso às capacidades seguras de SD-WAN, como monitoramento e modelos SD-WAN, políticas e objetos, painéis analíticos, visualizações e relatórios, auditoria e recursos adicionais, como documentação e links;

Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;
Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;
Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;
Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;
Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;
Deve possuir mecanismos de remoção automática para logs antigos;
Permitir importação e exportação de relatórios
Deve ter a capacidade de criar relatórios no formato HTML, PDF, XML e CSV;
Deve permitir exportar os logs no formato CSV;
Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;
Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;
A solução deve ter relatórios predefinidos;
Deve permitir o envio automático dos logs para um servidor FTP externo a solução;
Deve ter a capacidade de personalizar a capa dos relatórios obtidos;
Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;
Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;
Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;
Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;
Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;
Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;
Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;
Permitir o envio por e-mail relatórios automaticamente;
Deve permitir que o relatório seja enviado por e-mail para o destinatário específico;
Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;
Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;
Deve permitir o uso de filtros nos relatórios;
Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;
Permitir especificar o idioma dos relatórios criados;

Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;
Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;
Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;
Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;
Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;
Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;
Deve permitir visualizar em tempo real os logs recebidos;
Deve permitir o encaminhamento de log no formato syslog;
Deve permitir o encaminhamento de log no formato CEF (Common Event Format);
Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;
Deve ser capaz de visualizar alertas de surtos e baixar automaticamente manipuladores de eventos e relatórios relacionados;
Deve permitir o time de resposta a incidentes identificar se um artefato malicioso de "Zero Day" encontrado na rede faz parte de alguma campanha específica de malware, se foi visto até o momento somente na rede da instituição;
Caso o malware faça parte de alguma campanha, deve ser detalhado qual o objetivo dela, tipos de indústria que já foram alvo do malware, comportamento malicioso conhecido sobre o malware e quais são os autores;
Deve permitir gerar alertas de eventos a partir de logs recebidos;
Deve suportar o serviço de Indicadores de Compromisso (IoC) do mesmo fabricante, que mostra as suspeitas de envolvimento do usuário final na Web e deve relatar pelo menos: endereço IP do usuário, nome do host, sistema operacional, veredito (classificação geral da ameaça), o número de ameaças detectadas;
A solução deve possuir garantia, suporte e atualizações ao software durante a vigência do contrato;

Solução de Identificação e Autenticação Centralizada
Características mínimas da Solução de Identificação e Autenticação Centralizada.
A solução deverá ser do mesmo fabricante da solução de NGFW de fornecimento deste projeto;
Poderá ser entregue em equipamento único ou com composição de equipamentos. para atender as funcionalidades exigidas.
Deverá possuir licenciamento para pelo menos 9000 usuários locais;
Deverá possuir licenciamento para até 1.000 grupos de usuários,

Deverá possuir licenciamento para até 500 certificados de usuários.
Deverá possuir licenciamento para até 50 tokens para dispositivos móveis, compatíveis com sistemas Android e iOS.

Suportar administração em interface gráfica (GUI) por HTTP e/ou HTTPS;
Suporta administração em interface baseada em linhas de comando (CLI) por TELNET e/ou SSH;
Permitir definir perfis de administradores para a solução, de modo que possa segmentar a responsabilidade dos administradores por tarefas operativas;
Possuir indicador visual, centralizado, de informações críticas (estado da licença, versão de firmware, consumo de CPU/Memória/Disco, quantidade de usuários criados e licenciados);
Suportar a atualização do firmware via interface gráfica, por processo simplificado e intuitivo;
Suportar customização de mensagens padrão da solução como páginas de erro, portais de autenticação, auto registro, reset de senha e outros. Suportar também a inclusão, alteração e remoção de imagens nas mensagens/páginas sem a necessidade de recursos ou conectividade externa;
Suportar configuração de Alta Disponibilidade (HA), reduzindo ao máximo os períodos de interrupção;
Suportar implementações de HA como "Ativo-Passivo" ou sincronizando configurações entre duas caixas ativas;
Permitir sincronismo automático de configurações entre todos os equipamentos que componham a solução em HA;
Suportar implementação de HA sincronizando configurações com appliances em localidades geograficamente separadas;
Suportar a opção de backup criptografado;
Suportar backup automatizado (agendados por critérios pré-definidos), não somente sob demanda;
Suportar o backup completo da configuração, incluindo base de usuários, grupos, tokens, certificados, configurações de single-sign-on e etc. A solução deve também permitir a restauração de toda configuração diretamente da interface gráfica;
Suportar NTP (Network Time Protocol), visando o sincronismo de hora/data;
Suportar SNMP v1, v2 e v3 permitindo consultar MIB própria e envio de Traps;
Suportar nativamente Trap SNMP indicando mudança de status de HA;
Suportar captura de pacotes através da interface gráfica para Troubleshoot avançado em ferramentas de análise de pacotes (ex.: Wireshark);
O equipamento deve permitir o envio de e-mails relacionados a reset de senha, aprovação de novos usuários, auto-registro de usuários e autenticação de segundo fator (token);
Deve suportar o envio de mensagens SMS para os usuários através de gateways SMS de terceiros ou seu próprio serviço de envio de SMS, sendo este segundo licenciado ou não;
Deve suportar o registro de todos os eventos que os usuários de sua base de dados local realizem com suas contas, tais como criação de um usuário, troca de senha de um usuário e alteração de informação gerais;

AUTENTICAÇÃO:

A solução deve efetuar autenticação para a gerência de identidade dos usuários da rede, ajudando a simplificar a administração dos mesmos sendo um ponto central de controle de autenticação, onde múltiplos métodos de autenticação possam ser consolidados;

Deve suportar autenticação em dois fatores (two-factor authentication);

Deve possuir suporte a autenticação de dois fatores em pelo menos tokens lógicos como software para dispositivos móveis, e-mail e SMS, permitindo que seja dada a escolha de qual dos tipos utilizar para cada usuário e situação;

A solução deve permitir que se defina um perfil de complexidade mínimo para as senhas de todos os usuários cadastrados na base de dados local, possibilitando a definição de número mínimo de letras minúsculas, letras maiúsculas, caracteres numéricos, caracteres especiais e etc;

A solução deve permitir a criação de política de bloqueio automático de usuários após uma quantidade de falhas de autenticação, assim evitando ataques de força bruta;

A solução deve suportar a criação de usuários em base local, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade;

A solução deve permitir a criação em massa de usuários na base de dados local através da importação de lista de usuários a serem criados contida em arquivos externos;

A solução deve permitir a criação de novos usuários na base de dados local e que o criador/administrador possa definir uma senha no momento de criação;

A solução deve permitir a criação de novos usuários na base de dados local sem a definição de senha, exigindo que o mesmo utilize o token como único fator de autenticação;

Deve permitir associar os tokens aos usuários criados localmente na base de dados;

Deve permitir que os próprios usuários façam o registro dos seus tokens e relatem a perda de um token automaticamente, sem necessidade de envolver um administrador;

Remoção automática em massa de usuários desabilitados, baseado em critérios definidos;

A solução deve possuir formas que permitam que os usuários locais possam fazer o reset de suas senhas de forma segura sem a intervenção de administradores, através de correio eletrônico ou pergunta de segurança;

Deve suportar a criação de grupos de usuários, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade;

Os tokens deverão gerar códigos com no mínimo 6 dígitos e intervalos não superiores à 60 segundos

Suportar autenticação em dois fatores por aplicativo mobile (iOS e Android);

Suportar autenticação em dois fatores por envio de mensagem SMS;

Suportar autenticação em dois fatores por envio de e-mail;

Deve permitir desabilitar um token quando este seja roubado ou extraviado, permitindo sua reativação posterior quando/se for recuperado (Celulares / Tablets e contas de e-mail);

Deve prover um portal web para o auto-registro dos usuários, de forma que o mesmo acesse, preencha os seus dados e submeta o registro. Após o usuário efetuar o registro, o administrador deverá ser notificado automaticamente para aprovar ou negar o cadastro do mesmo antes de que ele seja ativado;
A solução deve funcionar como servidor RADIUS (Remote Authentication Dial-In User Server), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;
A solução deve suportar a integração com servidor RADIUS remoto;
A solução pode funcionar como servidor LDAP (Lightweight Directory Access Protocol), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;
A solução deve suportar a integração com servidor LDAP remoto (como Microsoft Active Directory);
A solução deve suportar autenticação de usuários com credenciais de mídias sociais de terceiros como Facebook, Twitter, LinkedIn e Google+;
A solução deve permitir que usuários que não possuam uma conta local ou em mídias sociais se autentiquem através de um rápido cadastro, que garanta o mínimo de rastreabilidade, através da validação de endereços de e-mail ou número de telefone;
A solução deve permitir o login automático de usuários visitantes depois de se registrarem com sucesso;
A solução deve permitir configurar os parâmetros de rede (como as configurações de WiFi) em um endpoint baixando um script ou um executável através do portal de visitantes;
Deve suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Indentity Provider - IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider -SP);
Deve permitir integração com bases do Azure Directory e GSuite;
Por meio do SAML, deve permitir integrações com SPs variados, tais como Office 365;
Deve suportar FIDO;
A solução deve apontar a última vez (data) em que um token foi utilizado;
A solução deve suportar OpenID Connect (OIDC);
Deve suportar autenticação adaptativa;
Deve suportar regras granulares no processo de autenticação. Ex: usuários se autenticando na VPN precisam utilizar MFA, mas, o mesmo usuário, em portal web, não precise informar o token;
Deve suportar push notification;

CONTROLE BASEADO EM PORTA:
A solução deve suportar nativamente (sem redirecionamentos) a integração e autenticação de switches e outros dispositivos compatíveis com o padrão 802.1X;
Suportar os seguintes métodos 802.1X EAP: PEAP (MSCHAPv2), EAP-TTLS, EAP-TLS e EAP-GTC;
Suportar interoperabilidade com equipamentos de acesso (switches) de outros fabricantes, para autenticação de portas junto a solução, através dos padrões 802.1X;

Deve suportar bypass de autenticação 802.1X para dispositivos conhecidos que não suportem 802.1X, a liberação deverá ser feita baseada no endereço MAC dos equipamentos previamente cadastrados, estes terão acesso a rede sem necessidade de autenticação ou ação do usuário ou dispositivo.

CERTIFICADOS:

A solução deve atuar como Autoridade Certificadora (CA);
Deve permitir a administração de certificados digitais, com emissão e revogação;
Deve permitir o uso de CA's confiáveis para validação de certificados emitidos por CA's externas;
Deve suportar OCSP para que se possa fornecer uma lista de certificados revogados (CRL);
Deve prover repositório para autenticação de VPN Site-to-Site através de Certificados;
Deve suportar SCEP Server (Simple Certificate Enrollment Protocol), permitindo a assinatura de requisições de certificados digitais (CSR) automaticamente ou com interação do administrador;
Deve ser capaz de importar outros certificados de CA's assim como a lista de certificados revogados;
Deve ser capaz de permitir ao administrador do sistema gerar, assinar e revogar certificados digitais para os usuários;
Suportar ao protocolo ACME para geração de certificados.

SERVIÇO DE AUTENTICAÇÃO ÚNICA (SINGLE SIGN-ON)

A solução deve prover capacidade de serviço SSO (Single Sign-On), com autenticação transparente (passiva) de usuários em sistemas compatíveis
Deve ser capaz de integrar-se a um diretório ativo (Windows AD) e poder oferecer a funcionalidade se SSO, onde a autenticação automática/transparente via SSO para os serviços necessários é baseada na autenticação prévia feita pelo usuário no domínio
Deve permitir definir uma lista de usuários de SSO que serão ignorados, evitando assim interferência de contas de serviços tais como antivírus ou scripts via GPO
Deve suportar análise de arquivos syslog enviados de fonte remota, para uso pelo serviço de SSO
Deve suportar Security Assertion Markup Language (SAML), agindo como autenticador de um Provedor de Serviços (Service Provider - SP) solicitando informações de identidade de usuários a Provedores de Identidade (Indentity Providers - IDP's) de terceiros
Deve suportar SSO baseado em Radius (RSSO - RADIUS Single Sign-On)
Deve suportar RSSO Accounting Proxy permitindo a recepção de pacotes radius de accouting, a modificação destes pacotes e o encaminhamento dos mesmos para vários outros pontos

SEGUNDO FATOR DE AUTENTICAÇÃO PARA REDES PRIVADAS VIRTUAIS

Permitir o download gratuito do seu provisionamento.
Instalado no dispositivo móvel sem que haja a necessidade de alteração de sua configuração, ou mesmo a capacidade de formatar o dispositivo móvel de forma remota.
Garantir a privacidade do dispositivo móvel.

Deve requerer a permissão do proprietário para envio de notificações ou qualquer tipo de alteração nas configurações.
Deve suportar, no mínimo, as principais plataformas de mobile do mercado: iOS, Android e Windows
Suportar ativação através da utilização de QR Codes e manual.
Criptografar o armazenamento de sementes utilizadas na geração do token.
Ter a capacidade de proteger abertura do aplicativo através de PIN, Impressão Digital ou Face Security.
Suportar que a senha gerada possa ser copiada para a área de transferência.
Suportar detalhes de login enviados ao telefone para aprovação com um toque.
Suportar à sua utilização como segundo fator de autenticação para acesso VPN via SSL ou IPSEC, sem a necessidade de utilização de um servidor RADIUS.

1.11. **PLATAFORMA DE ANÁLISE DE LOG CENTRALIZADO DA SOLUÇÃO**

Plataforma composta por hardware e software, específico para analisar os logos coletados dos equipamentos firewall e plataforma de autenticação.
Deve ser totalmente compatível com os itens de fornecimento deste projeto.
Armazenamento interno mínimo de 24TB;
Deve possuir 8 baias para discos rígidos;
Formato para montagem em rack com altura máxima de 2Us;
Raid por Hardware;
Possui duas fontes redundantes do tipo hot swap;
Possui 2 portas de 2.5gbps RJ45 e 2 portas 25GbE SFP28
Alimentação 100-240Vac, 50~60Hz
Consumo Máximo aproximado de 302W
Possui 24 meses de garantia, sendo 3 meses garantia legal mais 21 meses garantia estendida.

1.12. **RACK 19”**

O Rack 19” deverá ser instalado nos Próprios e atender no mínimo as especificações abaixo:
Possuir 8U de altura, por 570mm de profundidade;
Deverá ser do tipo “Rack de parede”;
Possuir laterais e porta em aço;
Porta frontal com fechadura e acrílico cristal;
Acompanha uma calha de tomadas com 4 tomadas devidamente fixada ao rack;
Acompanha um organizador de cabos U cor preta com fechamento frontal devidamente fixada ao rack;
Acompanha um patch pannel de 24 portas categoria 6 devidamente fixada ao rack;
Pintura em cor preta.

Deverá ser previsto a fixação do Rack com no mínimo 4 parafusos e buchas metálicas especiais para suportar o peso do rack mais o peso dos equipamentos de fornecimento deste projeto, considerando 1

nobreak / 2 Switches / 2 organizadores de cabos / 2 patch pannels / Cabeamento Cat 6 / Cabos elétricos / conversores de fibra optica).

1.13. **NOBREAK**

O Nobreak deverá possuir as características técnicas mínimas:
Tensão nominal de entrada Bivolt Automático (115/127/220v);
Sistema senoidal por aproximação retangular PWM;
Frequência de entrada 60 Hz ±4;
Variação máxima: 89 a 140V (em rede 115V) e 175 a 260 (em rede 220V);
Plugue do cabo de força no padrão NBR14136;
Capacidade de Potência de Saída 1500VA;
Fator de potência 0,7;
Tensão nominal de saída bivolt com seleção manual 115/220v;
Frequência de saída 60hz ±4% (Para operação em bateria);
Permite carregar as baterias mesmo com pouca carga;
Conexões de Saída 8 tomadas padrão NBR14136;
Rendimento: até 96% (para operação rede);
Bateria interna: 2 baterias 12Vdc/7Ah;
Bateria externa opcional: até 80ah / 24vDC;
Dimensões aproximadas: (AxLxP) 233x140x386 / Peso Aproximado bruto: 12,5kg;
Possui 24 meses de garantia, sendo 3 meses garantia legal mais 21 meses garantia estendida.

1.14. **INFRAESTRUTURA DE COMUNICAÇÃO LÓGICA COMPLETA**

Toda infraestrutura a ser criada entre o rack de distribuição aos propagadores de sinal, deverão ser do tipo metálica, de 1 polegada, possuir proteção contra corrosão, devidamente fixada e dimensionado conforme norma ABNT vigente.

A disposição e fixação da infraestrutura seca, deverá ser efetuada da melhor forma possível, de forma organizada, para que fique visualmente harmoniosa e sem fios aparente durante toda sua extensão.

A infraestrutura necessária (tubulação metálica e acessórios) para passagem de cabos lógicos e/ou elétricos a ser criada, será de responsabilidade da CONTRATADA, dimensionada conforme normas técnicas e de segurança vigentes.

CARACTERÍSTICAS GERAIS

Os equipamentos deverão ser instalados conforme diretrizes do Departamento de Tecnologia da Informação.

Os equipamentos deverão ser instalados de forma cobrir a extensão principal do departamento contemplado com sinal de rede sem fio.

Na proposta apresentada, deverá ser previsto todos os serviços e materiais necessários para possibilitar a instalação e utilização dos equipamentos de fornecimento deste projeto.

O sistema de comunicação prevê a implantação de equipamentos e sistemas de acesso Wi-Fi que possibilite:
-Uma conexão mais confiável;
-Performance otimizada;
-Implementação simplificada e transparente;
-Minimizar as zonas de sombra dentro das unidades;
-Gerenciamento centralizado;

Para tingir o objetivo esperado, o sistema a ser ofertado, deverá permitir a conexão simultânea de grandes quantidades de equipamentos gerenciados de forma centralizada, permitindo uma comunicação estável nas localidades contempladas neste projeto.

Os equipamentos principais servidores, controladores e sistemas, deverão ser instalados no CPD Municipal sito no Departamento de Tecnologia da Informação – DTI, Rua Serafim Carloçs 571, Bairro São José, São Caetano do Sul – São Paulo.

Os controladores secundários e/ou switches de distribuição, devem ser instalados nos racks existentes ou em novos Racks que devem ser instalados em local estratégico que facilite a distribuição do cabeamento necessário.

Devem ser fornecidos e utilizados guias organizadores de cabos para os racks, etiquetas térmicas e outros materiais para a correta organização e identificação dos cabos, portas de rede e pontos de dados envolvidos neste projeto. A identificação deve seguir norma ABNT de identificação de cabeamento estruturado.

Para a interligação lógica entre os propagadores de sinal e os racks de ativos de rede, deverá ser previsto a correta conectorização e identificação.

Os propagadores de sinal, deverão ser instalados dentro das salas indicadas pela administração, preferencialmente nas paredes laterais, fixados por parafuso e bucha adequados.

A alimentação elétrica dos equipamentos se dará através de porta POE do switch a ser fornecido.

Os equipamentos conectados à rede wireless objeto de implantação deste edital, acessarão à internet através de link de acesso fornecido pela CONTRATANTE interligado à controladora a ser instalada no CPD Municipal, sendo de responsabilidade da contratada configurar VLANS, endereçamentos de IPS, roteamentos, ACLs e demais configurações necessárias, que devem ser definidas em conjunto coma equipe técnica do DTI.

A interligação logica (backbone e interconects) deverão ser criados com velocidade gigabit, devendo ser utilizado cabeamento e conectores categoria 6, devidamente homologada pela ANATEL, com suporte à POE, em lances máximos de 100(cem) metros.

O cabeamento categoria 6 a ser utilizado deverá possuía as características mínimas abaixo:
-Categoria 6;
- Cabeamento Estruturado para transmissão de voz, dados e imagens, segundo requisitos da norma - ANSI/TIA-568-C.2 Categoria 6;
-O cabo utilizado deverá possuir certificação Anatel;
-O cabo deve ser composto por condutores de cobre sólido 23 AWG;
-Capa externa em composto retardante à chama, com baixo nível de emissão de fumaça e livre de halogênios;
-Possuir impresso na capa externa nome do fabricante, marca do produto, e sistema de rastreabilidade que permita identificar a data de fabricação dos cabos.
-Deve suportar velocidade de 1Gbps em lances de 100 metros;

Deverão ser fornecidos todos equipamentos e licenças necessárias para implantação e funcionamento deste projeto.

Os equipamentos ofertados deverão pertencer a linha corporativa do fabricante, não sendo aceito equipamentos destinados ao uso doméstico.

Deverão ser novos, sem uso anterior, não remanufaturados e estar em linha de produção pelo fabricante no momento da entrega da proposta.

Na eventualidade do equipamento não estar mais em linha de produção no ato da entrega, a licitante deverá comunicar formalmente a equipe técnica que analisará as especificações do equipamento substituto em aderência ao solicitado em edital.

A licitante deverá trocar produtos defeituosos em garantia, em até 5 dias uteis após solicitação de reparo.

1.15. **SERVIÇO DE SUPORTE E MANUTENÇÃO PREVENTIVA**

1.15.1. A CONTRATADA, durante a vigência do contrato, deverá fornecer suporte técnico aos equipamentos e sistemas da solução sem fio ofertada de instalação neste projeto, com o objetivo de manter em perfeito funcionamento o sistema e atuar na resolução de problemas, reconfigurações, alterações de topologia, acompanhamento e melhoria de utilização da solução e ainda solucionar eventuais dúvidas operacionais e problemas que venham a ocorrer e/ou impeçam o uso de todos os equipamentos e softwares fornecidos e instalados. O legado é de responsabilidade da CONTRATANTE.

1.15.2. Fornecer toda assistência necessária à equipe de colaboradores da CONTRATANTE, sempre que acionada, para esclarecimentos de dúvidas e execução de ajustes nos equipamentos fornecidos pela mesma.

1.15.3. Realizar correções na solução ou execução de quaisquer medidas necessárias para solucionarem falhas de funcionamento e o restabelecimento da solução, dentro da sua responsabilidade.

1.15.4. O acionamento do suporte técnico da CONTRATADA poderá ser feito através das seguintes opções: telefônica (central de atendimento técnico) ou correio eletrônico (e-mail de suporte).

1.15.5. A CONTRATADA deverá possuir serviço de manutenção corretiva com atendimento 8x5, ou seja (oito) horas por dia, 5 (cinco) dias por semana.

1.15.6. A CONTRATADA deverá possuir Central de Atendimento para abertura dos chamados, comprometendo-se a manter registros dos mesmos constando a descrição do problema e solução aplicada.

1.15.7. Durante o prazo de garantia dos equipamentos, a parte ou peça defeituosa, deverá ser substituída sem ônus para o CONTRATANTE, salvo quando o defeito for provocado por uso inadequado, como quebra proposital, vandalismo ou alamentos provenientes de infiltrações no local de instalação do equipamento.

1.15.8. A CONTRATADA será responsável pelo atendimento de Nível 1, 2 e 3. Os Níveis de atendimento são qualificados da seguinte forma:

1° Nível:

Suporte realizado através de conexão remota, objetivando a verificação, o diagnóstico e correção de problema funcional do SISTEMAS, focando nos seguintes aspectos:

- Classes de alarme
- "Hardware" e "software"
- "Backup" do sistema
- Aplicativos do Sistema
- Falhas relatadas pelo cliente
- Corrigir configurações diversas

2° Nível:

Suporte On-Site

Este serviço deve ser prestado localmente, através de profissionais técnicos qualificados. Este serviço será responsável por prestar suporte ao cliente em atividades de manutenção corretiva, atendimentos em situações emergenciais, interrupções ou funcionamento inadequado dos sistemas, tendo como objetivo principal obter um serviço de suporte técnico presencial que garanta ou reestabeleça a operacionalidade e o bom desempenho dos equipamentos e ambientes envolvidos no contrato, bem como uma resposta rápida e emergencial às solicitações do cliente para os problemas identificados.

Atividades relacionadas ao Suporte On-Site:

- Corrigir configurações diversas;
- Atualizar software devido a falhas reconhecidas como bugs;
- Efetuar a troca de hardware devido a falhas e solicitar à troca ao fabricante dentro do período de garantia;

3° Nível:

Caso o problema não seja solucionado de acordo com os Níveis 1 e 2.

O atendimento será realizado pela equipe de profissionais especializados do Centro de Competência da CONTRATADA e se necessário com o acionamento do fabricante das soluções instaladas.

1.15.9. Quadro de SLA da CONTRATADA:

Classificação	**Tempo Máximo para Atendimento**
Alta	12 horas
Moderada	18 horas
Baixa	1 dia útil.

Alta: Problemas que prejudicam a operação da infraestrutura de rede/sistemas que a tornem inoperante.

Moderada: Problemas ou dúvidas que criam algumas restrições à operação da solução.

Baixa: Solicitações que não afetem o uso do sistema de forma imediata.

1.15.10. **SLA – SERVICE LEVEL AGREEMENT**

1.15.10.1. O ANS – Acordo de Níveis Serviço define as principais metas e responsabilidades da CONTRATADA no atendimento de chamados técnicos na execução e manutenção das redes de fibra óptica e de cabeamento estruturado;

1.15.10.2. Os chamados técnicos abertos serão classificados por grau de severidade, sendo que as Garantias Acessórias da Solução devem ser executadas dentro dos padrões mínimos de atendimento:

1.15.10.3. Severidade 1 (S1): o equipamento, acessório ou periférico apresenta pane, falha ou não conformidade técnica que o torna acima de 50% inoperante. O primeiro retorno telefônico da CONTRATADA deve ser realizado em no máximo 01 hora e a solução técnica, definitiva ou de contorno, não poderá exceder a 12 horas, contadas do chamado técnico;

1.15.10.4. Severidade 2 (S2): o equipamento, acessório, ou periférico apresenta pane, falha ou não-conformidade técnica que degrade a qualidade, prejudica a operação e o uso ou acesso de funções básicas. O primeiro retorno telefônico da CONTRATADA deve ser realizado em no máximo 02 horas e a solução técnica, definitiva ou de contorno, não poderá exceder a 18 horas, contadas do chamado técnico;

1.15.10.5. Severidade 3 (S3): o equipamento, acessório, ou periférico apresenta pane, falha ou não conformidade técnica que não afetem o rendimento do serviço. O primeiro retorno telefônico da CONTRATADA deve ser realizado em no máximo 02 horas e a solução técnica, definitiva ou de contorno, não poderá exceder a 24 horas, contadas do chamado técnico.

1.15.10.6. O serviço de manutenção descritos neste documento, serão faturados mensalmente conforme peso de importância do suporte em relação ao equipamento e cada peso com relação à quantidade de equipamentos efetivamente instalados neste projeto, conforme tabela a seguir:

DESCRIÇÃO	QTD	PESO PERCENTUAL DO SERVIÇO DE MANUTENÇÃO E SUPORTE
Firewall de alta capacidade Tipo I	2	30%
Propagador de sinal sem fio Tipo I (indoor)	400	20%
Propagador de sinal sem fio Tipo II (outdoor)	30	5%
Switch Gerenciável Tipo I	200	5%
Plataforma de autenticação e gerenciamento da Solução de Segurança	1	15%
Plataforma de Análise de Log Centralizado da Solução de Segurança	1	15%
Rack 19" 8Us	123	0%
Nobreak Tipo I - 1500VA	123	5%
Infraestrutura de comunicação lógica completa	8600	5%
		100%

2. PRAZOS, CONDIÇÕES E LOCAL DE ENTREGA DOS MATERIAIS E/OU PRESTAÇÃO DOS SERVIÇOS, VIGÊNCIA DO CONTRATO.

2.1. O prazo de vigência da presente Ata de Registro de Preços será de 12 (doze) meses, contados a partir da assinatura do instrumento contratual, podendo ser prorrogado, a critério das partes, nos termos do artigo 84 da Lei Federal nº 14.133/21.

2.1.1. Na hipótese de prorrogação da vigência da Ata de Registro de Preços, as quantidades inicialmente registradas serão renovadas, na sua totalidade, independentemente do quantitativo utilizado no período de vigência, não sendo possível cumular com as quantidades não utilizadas.

2.2. A Autorização de Fornecimento será encaminhada por quaisquer meios de comunicação que possibilitem a comprovação do respectivo recebimento por parte da Detentora, inclusive correio eletrônico.

2.3. O fornecimento deverá ser realizado de acordo com as especificações técnicas constantes do edital, na forma prevista na proposta, naquilo que não o contrariar, dentro dos prazos estabelecidos sob pena de a(s) futura(s) Detentora (s) incorrer(em) nas sanções previstas neste Edital.

2.4. Os equipamentos deverão ser entregues e instalados, no endereço constante da Autorização de Fornecimento, conforme o **ANEXO IA - Endereços da Prestação dos Serviços,** de segundas às sextas-feiras, no prazo de até 30 (trinta) dias corridos, contados a partir do recebimento da mesma.

2.4.1. Qualquer alteração de local de entrega será previamente informada à Detentora.

2.5. Os equipamentos serão solicitados sob demanda, conforme necessidades e disponibilidade orçamentária.

2.6. Todas as despesas decorrentes de carga, descarga, transporte ocorrerão por conta da empresa Detentora.

2.7. O material deve ser entregue em sua embalagem original, sem estar violada ou fracionada e em condições de transporte e acondicionamento indicados pelo fabricante.

2.8. No momento do recebimento, haverá avaliação para aferir conformidade com o solicitado.

2.9. Ao apresentar qualquer irregularidade na qualidade do produto, a Unidade requisitante entrará em contato com o fornecedor para que faça a troca do produto.

2.10. Todos os equipamentos fornecidos pela Detentora, deverão ter garantia de 24 (vinte e quatro) meses.

2.11. As garantias solicitadas terão início a partir da data de emissão da Nota Fiscal de entrega dos equipamentos.

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

3.1. O recebimento dos bens e materiais será realizado pelos membros indicados pelas Portarias nº. 37.975/2022, em conformidade com o estabelecido no Decreto Municipal nº 10.728 de 24/01/2014;

3.2. A atestação do objeto contratado, somente ocorrerá se não houver a constatação de qualquer irregularidade, em havendo irregularidades ou caso os aparelhos estejam fora dos padrões determinados, à contratante solicitará a regularização no prazo de 03 (dez) dias úteis, o atraso na regularização acarretará as penalidades previstas no Edital;

4. **OBRIGAÇÕES DA DETENTORA**

4.1. Fornecer os produtos na quantidade e prazos estabelecidos no Edital, de acordo com as especificações técnicas constantes neste instrumento.

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

4.3. Compromete-se a fornecer os produtos na forma de sua apresentação na proposta, comprovando a marca, validade, procedência e demais características dos produtos, os quais serão conferidos pela Contratante;

4.4. Substituir, no local de entrega e no prazo ajustado, após notificação, o serviço recusado.

4.5. Todas as despesas decorrentes de seguros, transporte, tributos, embalagem, correrão por conta exclusiva da empresa Detentora.

4.6. A Detentora está obrigada a aceitar nas mesmas condições contratuais os acréscimos e supressões até 25% do valor inicial atualizado do contrato ou da nota de empenho.

4.7. Comunicar à Contratante toda e qualquer irregularidade ocorrida ou observada durante o fornecimento dos materiais.

4.8. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à Administração.

4.9. Obedecer às normas e rotinas da CONTRATANTE em especial as que disserem respeito à proteção de dados pessoais, à segurança, à guarda, à manutenção e a integridade das informações coletadas, custodiadas, produzidas, recebidas, classificadas, utilizadas, acessadas, reproduzidas, transmitidas, processadas arquivadas eliminadas ou avaliadas durante a execução do objeto a que se refere a Cláusula Primeira deste Contrato, observando as normas legais e regulamentares aplicáveis.

4.10. Atender às determinações da fiscalização do Gestor do Contrato e providenciar a imediata correção das deficiências apontadas pela fiscalização quanto a entrega dos produtos.

4.11. A Detentora deverá cumprir a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, nos termos do art. 116 da lei 14.133/2021.

4.12. Nomear preposto para representá-la na execução deste contrato durante o período de vigência.

4.13. Manter, durante a vigência do contrato, as condições de habilitação exigidas na licitação, devendo comunicar a contratante a superveniência de fato impeditivo da manutenção dessas condições.

4.14. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto deste contrato em que se verificarem vícios, defeitos ou incorreções, e terão o prazo de 48 horas para substituir o material rejeitado.

4.15. Comunicar à Contratante, no prazo máximo de 48 (quarenta e oito) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.

4.16. Comunicar à Contratante toda e qualquer irregularidade ocorrida ou observada durante a entrega do material.

4.17. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão, dentre outras, as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade.

4.18. Orientar tecnicamente os responsáveis pela operação dos bens, fornecendo os esclarecimentos necessários ao seu perfeito funcionamento.

4.19. Proceder a entrega dos bens, devidamente embalados, de forma a não serem danificados durante a operação de transporte e de carga e descarga, assinalando na embalagem a marca, destino e, quando for o caso, número da Licença de Importação ou documento equivalente, com as especificações detalhadas ou documento equivalente, para conferência.

4.20. Realizar testes e corrigir defeitos nos bens, inclusive com a sua substituição quando necessário, sem ônus para a CONTRATANTE, durante o período de garantia. A troca de produtos defeituosos deverá ser em até 5 dias uteis.

4.21. Responder por todos os ônus referentes a entrega dos bens ora contratados, desde os salários dos seus empregados, como também os encargos trabalhistas, previdenciários, fiscais e comerciais, que venham a incidir sobre o Contrato.

4.22. A Detentora deverá designar profissional qualificado que atuará como gerente de projeto, coordenando os demais profissionais envolvidos na execução do objeto, garantindo a sintonia das diversas atividades e o bom andamento do cronograma de trabalho.

4.23. O gerente de projeto também será o ponto de contato com os representantes do Município, para os quais reportará as atividades, fatos e eventuais dificuldades que deverão ser comunicadas ao gestor do contrato.

4.24. Entregar os bens no local indicado pela CONTRATANTE.

4.25. Responsabilizar-se:

a) Por quaisquer acidentes na entrega dos bens.

b) Pelo pagamento de seguros, impostos, taxas e serviços, encargos sociais e trabalhistas, e quaisquer despesas referentes aos bens.

4.26. Executar o objeto em conformidade com as condições deste instrumento.

4.27. Responsabilizar-se pelos danos causados diretamente a CONTRATANTE ou a terceiros, decorrentes da sua culpa ou dolo, quando da execução do objeto, não podendo ser arguido para efeito de exclusão ou redução de sua responsabilidade o fato de a CONTRATANTE proceder a fiscalização ou acompanhar a execução contratual.

4.28. Responder por todas as despesas diretas e indiretas que incidam ou venham a incidir sobre a execução do contrato, inclusive as obrigações relativas a salários, previdência social, impostos, encargos sociais e outras providencias, respondendo obrigatoriamente pelo fiel cumprimento das leis trabalhistas e especificas de acidentes do trabalho e legislação correlata, aplicáveis ao pessoal empregado na execução contratual.

4.29. Prestar imediatamente as informações e os esclarecimentos que venham a ser solicitados pela CONTRATANTE, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidas no prazo de 24 (vinte e quatro) horas.

4.30. Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta comercial, observando o prazo mínimo exigido pela Administração.

4.31. Providenciar a substituição de qualquer profissional envolvido na execução do objeto contratual, cuja conduta seja considerada indesejável pela fiscalização da CONTRATANTE.

4.32. A equipe de trabalho da contratada, deverá orientar a equipe de funcionários municipais sempre que necessário, no que tange operação, funcionalidades e configurações do sistema contratado, sem custos à CONTRATANTE.

5. OBRIGAÇÕES DA CONTRATANTE

5.1. Cumprir o prazo fixado para realização do pagamento;

5.2. Indicar o funcionário responsável pelo acompanhamento do instrumento contratual;

5.3. Comunicar à Detentora sobre quaisquer irregularidades dos produtos entregues;

5.4. Fiscalizar o fornecimento dos materiais, zelando pelo fiel cumprimento do presente contrato, promovendo seu recebimento, conferindo a qualidade, especificação exigida dos mesmos, assim como os preços apresentados;

5.5. Prestar as informações e os esclarecimentos que venham a ser solicitados pelo Fornecedor Contratado, durante o prazo vigente do Contrato;

5.6. Receber o objeto no dia previamente agendado, no horário de funcionamento da unidade responsável pelo recebimento.

5.7. Solicitar o reparo ou a substituição do objeto em que se verificarem vícios, defeitos ou incorreções.

5.8. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes deste Termo de Referência e da proposta, para fins de aceitação e recebimento definitivos.

5.9. Proporcionar a Detentora todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do objeto contratual.

5.10. Designar um funcionário como gestor do contrato e que servirá de contato junto à CONTRATADA

para gestão, acompanhamento e esclarecimentos que porventura se fizerem necessários durante a vigência contratual.

5.11. Comunicar à Detentora, toda e qualquer orientação acerca dos serviços, excetuados os entendimentos orais determinados pela urgência, que deverão ser confirmados, por escrito, no prazo de 1 (um) dia útil.

5.12. Fornecer e colocar à disposição da Detentora todos os elementos e informações que se fizerem necessários à execução dos serviços.

5.13. Acompanhar, fiscalizar e auditar a execução dos serviços prestados, nos aspectos técnicos, de segurança, de confiabilidade e quaisquer outros de seu interesse, através de pessoal próprio ou de terceiros designados para este fim.

5.14. A CONTRATANTE deverá assegurar acesso aos técnicos credenciados pela CONTRATADA, a todos equipamentos para a execução dos serviços de manutenção, prestando os esclarecimentos que eventualmente venham a ser solicitados.

5.15. A CONTRATANTE deverá designar um funcionário responsável, que acompanhará o pessoal técnico da CONTRATADA em todas as visitas, para a comprovação de eventuais irregularidades.

5.16. Caso a CONTRATANTE substitua o funcionário responsável pelo atendimento, deverá informar por escrito à Detentora.

5.17. É expressamente vedado à CONTRATANTE em qualquer hipótese, utilizar-se de serviços de terceiros ou próprio, para intervir no conserto, alteração do equipamento ou acessórios sem prévia e expressa autorização da Detentora.

5.18. Notificar, formal e tempestivamente, a Detentora sobre as irregularidades observadas no cumprimento do contrato.

5.19. Efetuar os pagamentos devidos a Detentora nas condições estabelecidas neste Termo.

5.20. Aplicar as penalidades previstas em lei e neste instrumento.

6. GESTOR DO CONTRATO

6.1. O gestor da presente contratação será o servidor indicado e, na sua ausência, a Secretária Municipal de Gestão e Governo Digital, nos termos do Decreto Municipal nº 12.176/2025 e Portaria nº 44.004/2026

o qual será responsável pelo acompanhamento e fiscalização da execução do termo contratual objeto do presente certame, procedendo ao registro das ocorrências e adotando as providências necessárias ao fiel cumprimento do ajuste, bem como, responsabilizar-se á pela vigência, com o consequente controle dos prazos de início e término contratual, aditamentos e instauração de novo processo de licitação, caso seja deliberado pela continuidade dos serviços ou fornecimento.

6.2. Compreenderá na fiscalização aludida no item anterior, a atestação e aprovação dos serviços prestados, de que os mesmos atendem as especificações e finalidades contratuais, de forma a ser concretizado o acompanhamento.

6.3. O Gestor responderá administrativamente, civil e penalmente pelo cumprimento do contrato ou instrumento equivalente, quando verificado a não observância dos requisitos acima causando prejuízo à Administração ou comprometimento das atividades procedimentais.

ANEXO- IA

ENDEREÇOS DA PRESTAÇÃO DOS SERVIÇOS

LOCAIS DE INSTALAÇÃO DOS EQUIPAMENTOS.

Os equipamentos poderão ser instalados nos seguintes endereços relacionados abaixo, visto que as quantidades serão definidas conforme necessidade de cobertura de rede sem fio em cada localidade bem como disponibilidade orçamentária de cada departamento.

Os equipamentos Enterprise (firewall, plataforma de autenticação e plataforma de análise de log) serão instalados do Rack de equipamento existente no Departamento de Tecnologia da Informação, situado na Rua Serafim Carlos, 571, Bairro São José, São Caetano do Sul.

Possíveis endereços de instalação dos equipamentos:

ENDEREÇO	BAIRRO
AL CASSAQUERA 00227	BARCELONA
AL JOAO GALEGO 00001	SANTA MARIA
AL PORTO ALEGRE,CDE 00800	STA MARIA
AL PORTO ALEGRE,CDE 00820	STA MARIA
AL PORTO ALEGRE,CDE 01540	STA MARIA
AV ANTONIO PRADO,CONS 00000	CENTRO
AV ANTONIO PRADO,CONS 00250	CENTRO
AV ANTONIO PRADO,CONS 00307	CENTRO
AV AUGUSTO DE TOLEDO,DR 00000	OSWALDO CRUZ
AV AUGUSTO DE TOLEDO,DR 00195	SANTA PAULA
AV AUGUSTO DE TOLEDO,DR 00255	SANTA PAULA
AV AUGUSTO DE TOLEDO,DR 00350	SANTA PAULA
AV FERNANDO SIMONSEN 00130	SANTA PAULA
AV FERNANDO SIMONSEN 00160	CERAMICA
AV FERNANDO SIMONSEN 00566	CERAMICA
AV GOIAS 00340	CERAMICA
AV GOIAS 00600AN 3	BARCELONA
AV GOIAS 00950	BARCELONA
AV GOIAS 02000	BARCELONA
AV GOIAS 02101	BARCELONA
AV GOIAS 03400	BARCELONA
AV GUIDO ALIBERTI 00020	BARCELONA
AV GUIDO ALIBERTI 01610	BARCELONA

AV GUIDO ALIBERTI 01651	CENTRO
AV JOAO XXIII,PAPA 00601	CENTRO
AV KENNEDY,PRES 02100	CENTRO
AV KENNEDY,PRES 02300	JD S CAETANO
AV KENNEDY,PRES 02400	BOA VISTA
AV LIBERO BADARO 00000	BOA VISTA
AV PARAISO 00600	BOA VISTA
AV PARAISO 00831	JD S CAETANO
AV PARANAPANEMA 00670	OLIMPICO
AV PROSPERIDADE 00441	OLIMPICO
AV PROSPERIDADE 00671	NOVA GERTY
AV ROBERTO SIMONSEN,SEN 00282+AN 1	PROSPERIDADE
AV RODRIGUES ALVES,DR 00093+	PROSPERIDADE
AV TIETE 00301	CENTRO
AV TIJUCUSSU 00800	FUNDACAO
AV VITAL BRASIL FILHO 00300	NOVA GERTY
AV VITAL BRASIL FILHO 00361	OLIMPICO
AV VITAL BRASIL FILHO 00600+ESCOLA SYLVIOROMERO	OSVALDO CRUZ
AV WALTER THOME 00064	OSVALDO CRUZ
ETRLAGRIMAS 00320	OSVALDO CRUZ
ETRLAGRIMAS 00515	OSVALDO CRUZ
ETRLAGRIMAS 00579	OSVALDO CRUZ
ETRLAGRIMAS 01165	OLIMPICO
ETRLAGRIMAS 01630	MAUA
ETRLAGRIMAS 01656	MAUA
PCABADEN POWELL 00001	MAUA
R ALEGRE 00497	MAUA
R ANGELO APARECIDO RADIM 00090+GUARITA GCMS	MAUA
R ANTONIO BENTO 00140	MAUA
R ANTONIO BENTO 00180	CENTRO
R ANTONIO JOAO,TTE 00413	SANTA PAULA
R ANTONIO,STO 00050+FARMACIA POP GOV	SAO JOSE
R ANTONIO,STO 00117	SANTA PAULA
R ARARAQUARA 00063	SANTA PAULA
R ARLINDO MARCHETTI 00508	SANTA PAULA
R ARMANDO DE A PEREIRA,ENG 00000	CERAMICA
R ARMANDO DE A PEREIRA,ENG 00120	CENTRO

R ARMANDO DE A PEREIRA,ENG 01470	CENTRO
R ARNALDO SANTE LOCOSELLI 00158	FUNDACAO
R AURELIA 00257	SANTA MARIA
R AURELIA 00257+HOSP EMERG ALBERT S	CERAMICA
R BELL ALLIANCE 00000+ESQ R WINSTON CHUR	CERAMICA
R BELL ALLIANCE 00225	CERAMICA
R BERILOS 00113	CERAMICA
R BERTOLINO CUNHA 00100	STA PAULA
R BOA VISTA 00150	STA PAULA
R BOA VISTA 00200	STA PAULA
R BUSCH 00042FR	JD S CAETANO
R CAMISAO,CEL 00320	JD SAO CAETANO
R CAPIVARI 00500	PROSPERIDADE
R CAPIVARI 00624	OSWALDO CRUZ
R CARLO DEL PRETE,MAJ 00651	BOA VISTA
R CASEMIRO DE ABREU 00560	BOA VISTA
R CASTORES 00060	NOVA GERTI
R CEARA 00509+CRE FUDA??O	OSWALDO CRUZ
R CLOVIS BEVILACQUA 00075	NOVA GERTY
R CORAL 00155	NOVA GERTY
R DEODORO,MAL 00000+FRENTE TRAV PEDESTR	CENTRO
R DEODORO,MAL 00300	CENTRO
R DEODORO,MAL 00445	CENTRO
R DEODORO,MAL 00830	CERAMICA
R DEODORO,MAL 01111	MAUA
R DESIREE MALATEAUX 00129	FUNDACAO
R DIONIZIO MERCADO 00199	CERAMICA
R DOMENICO BOTAN 00091	PROSPERIDADE
R DURVAL VILALVA,DR 00135	STA PAULA
R EDUARDO PRADO 00000	SANTA PAULA
R EDUARDO PRADO 00001	SANTA PAULA
R EDUARDO PRADO 00201	SANTA PAULA
R ERNESTO GIULIANO,CAV 00849+ESCOLA ANACLETO C	SANTA PAULA
R ERNESTO GIULIANO,CAV 01050	MAUA
R ERNESTO GIULIANO,CAV 01301	VL GERTI
R ESPIRITO SANTO 00277	OSWALDO CRUZ
R ESPIRITO SANTO 01330	FUNDACAO

R ESTILAC LEAL,GAL 00058	SAO JOSE
R ETERNIDADE 00013	SAO JOSE A
R ETERNIDADE 00261	SAO JOSE
R ETERNIDADE 00263	SAO JOSE
R FATIMA,N S 00497	SAO JOSE
R FLAQUER,SEN 00134	SAO JOSE
R FLORIDA 00295+POSTO SAUDE	OSVALDO CRUZ
R FLORIDA 00525	OSVALDO CRUZ
R FLORIDA 00960	OSVALDO CRUZ
R FLORIDA 00975	BAIRRO CERAMICA
R GARCA 00121	BAIRRO CERAMICA
R GARCA 00323	BAIRRO CERAMICA
R GIOVANI PERUCCHI 00190+ESCOLA OSWALDO S M	BAIRRO CERAMICA
R GOITACAZES 00301	BAIRRO CERAMICA
R GONZAGA 00241	BAIRRO CERAMICA
R HELOISA PAMPLONA 00180+ESCOLA S FLAQUER	MAUA
R HELOISA PAMPLONA 00269+NGA-43 SAMUEL KLEIN	MAUA
R HELOISA PAMPLONA 00304	MAUA
R HELOISA PAMPLONA 00316	MAUA
R HELOISA PAMPLONA 00402	SANTA PAULA
R HERCULANO DE FREITAS 00200	SAO JOSE
R HERCULANO DE FREITAS 00265	BARCELONA
R HUMBERTO DE CAMPOS 00000	BARCELONA
R HUMBERTO DE CAMPOS 00550	BARCELONA
R HUMBERTO DE CAMPOS 00600	BARCELONA
R INHAUMA DE,VISC 00905	PROSPERIDADE
R IVAI 00063+ESCOLA EDA MONTOANE	PROSPERIDADE
R JOAO RAMALHO 00100	OSWALDO CRUZ
R JOAQUIM NABUCO 00172	CENTRO
R JOSE BENEDETTI 00550+ EMEF	OSWALDO CRUZ
R JURUA 00050+CER AGUIAS	FUNDACAO
R JUSTINO PAIXAO 00141	FUNDACAO
R LAFAYETTE,CONS 00619	FUNDACAO
R LISBOA 00399	FUNDACAO
R LOURDES 00460	FUNDACAO
R LOURDES 00525	FUNDACAO
R LUIZ LOUZA 00048	FUNDACAO

R LUIZ LOUZA 00170+CRE GONZAGA	SAO JOSE
R MARANHAO 00022+ESCOLA BARTOLOMEU B	SAO JOSE
R MARANHAO 00611	SAO JOSE
R MARIA MACEDO,PROF 00240	OSWALDO CRUZ
R MARTIM FRANCISCO 00177+ESCOLA BENEDITO P A	SANTA MARIA
R MAUA,BR 00133	BOA VISTA
R MAXIMILIANO LORENZINI 00122	SANTO ANTONIO
R MIGUEL GLEBOCCHI 00090+ESCOLA DECIO GAIA	SANTO ANTONIO
R MOGI GUASSU 00080	NOVA GERTY
R NELLY PELLEGRINO 00930	JD S CAETANO
R NELLY PELLEGRINO 00954	BARCELONA
R NELSON 00231	OSVALDO CRUZ
R NESTOR MOREIRA 00300	NOVA GERTY
R NESTOR MOREIRA 00360	NOVA GERTY
R ORIENTE 00333	OLIMPICO
R ORIENTE 00501	OLIMPICO
R OSWALDO CRUZ 01153+UBS NAIR SPINA	OLIMPICO
R OTAVIO MANGABEIRA 00017	OLIMPICO
R PARA 00080	SANTO ANTONIO
R PARA 00088	SANTO ANTONIO
R PARAIBA 00646	CENTRO
R PASTEUR 00430	SANTA PAULA
R PAULO,S 00230+CRE TAMAYO	SAO JOSE
R PAZ 00010	FUNDACAO
R PELEGRINO BERNARDO 00515	BOA VISTA
R PERI 00316	OLIMPICO
R PERI 00361	NOVA GERTY
R PERNAMBUCO 00100	NOVA GERTY R
R PERRELLA 00000	NOVA GERTY
R PIAUI 00420	NOVA GERTI
R PORTO CALVO 00205	CERAMICA
R PRATES 00430	CERAMICA
R PRESTES MAIA 00100	BARCELONA
R PRUDENTE DE MORAIS 00081	BARCELONA
R RAFAEL CORREA SAMPAIO 00584+ B	SANTA PAULA
R RAFAEL CORREA SAMPAIO 00600	OSWALDO CRUZ
R RIO DE JANEIRO 00018+18/28	CENTRO

R RIO GRANDE DO SUL 00083	CENTRO
R RIO GRANDE DO SUL 00790	CENTRO
R ROSA,STA 00079	JD SAO CAETANO
R SEBASTIAO DIOGO 00099	SANTO ANTONIO
R SÃO PAULO, 200 (TAMOYO)	OSWALDO CRUZ
R SERAFIM CARLOS 00571	MAUA
R SERAFIM CONSTANTINO 00000+COMJUV	OLIMPICO
R SILVIA 00160	OSWALDO CRUZ
R SILVIA 00670+ESCOLA ROSALVITO C	OSWALDO CRUZ
R SILVIA 01743	CENTRO
R TAPAJOS 01085	FUNDACAO R
R TEFFE 00460	STO ANTONIO
R TEODORO SAMPAIO 00201	OSWALDO CRUZ
R TIRADENTES 00000	OSWALDO CRUZ
R TOMASO TOME 00270	NOVA GERTY
R TUPI 00300	SANTA PAULA
R ULYSSES TORNINCASA 00160	SANTO ANTONIO
R VANDA 00011+NASF PSF	SANTO ANTONIO
R VANDA 00073	OSVALDO CRUZ
R VICTOR MEIRELLES 00066	SANTO ANTONIO
R VIEIRA DE CARVALHO 00525	SANTO ANTONIO
TR SEBASTIAO GOMES LIMA 00060	SANTA PAULA

E demais localidades que vierem a ser criadas durante vigência contratual.

ANEXO II

PROPOSTA COMERCIAL

PROCESSO Nº. 3548807.425.00007034/2025-90

PREGÃO ELETRÔNICO Nº 35/2026

Nome da Empresa: **Endereço eletrônico:**		
Endereço:	**Nº.**	**Bairro:**
Cidade:	**Estado:**	**CEP:**
CNPJ Nº:	**Fone:**	**Inscrição Estadual:**
Dados para pagamento: **Banco: _____ - nº ___ / Agência: _____/Conta Corrente: ____**		
Dados do Responsável que Assinará o Contrato: **Nome:** **Cargo:** **Estado Civil:** **RG nº** **CPF nº** **Data de Nascimento:** **__/__/____** **Endereço completo:** **E-mail corporativo:** **E-mail pessoal:** **Telefone Coml:** **Telefone Resid.:** **Celular**		
***Pregão nº:* 35/2026**	***Data Abertura: 19/08/2026***	***Horário: 09:30hs***

LOTE ÚNICO

ITEM	CÓDIGO	QUANTIDADE	UNIDADE	ESPECIFICACAO	MARCA/ MODELO	VALOR UNITÁRIO	VALOR TOTAL
1	1.14.01.2228-0	123	UN	NOBREAK TIPO 1 - 1500VA . MAIORES INFORMAÇÕES NO MEMORIAL DESCRITIVO.			
2	1.14.01.2384-7	400	UN	PROPAGADOR DE SINAL SEM FIO PARA TRANSMISSÃO E RECEPÇÃO TIPO I, CONFORME TERMO DE REFERÊNCIA			
3	1.14.01.2385-5	30	UN	PROPAGADOR DE SINAL SEM FIO PARA TRANSMISSÃO E RECEPÇÃO TIPO II, CONFORME TERMO DE REFERÊNCIA			
4	1.14.01.2387-1	200	UN	SWITCH TIPO I, CONFORME TERMO DE REFERÊNCIA			

5	1.14.01.2393-6	123	UN	RACK 19" 8US, CONFORME TERMO DE REFERÊNCIA			
6	1.14.01.2443-6	8.600	M	INFRAESTRUTURA TUBULAR COMPLETA INCLUSO ACESSORIOS PARA FIXACAO			
7	1.14.01.2491-6	2	UN	FIREWALL NGF DE ALTA CAPACIDADE			
8	1.14.01.2819-9	1	UN	PLATAFORMA DE AUTENTICAÇÃO E GERENCIAMENTO DA SOLUÇÃO DE SEGURANÇA			
9	1.14.01.2820-2	1	UN	PLATAFORMA DE ANÁLISE DE LOG CENTRALIZADO DA SOLUÇÃO DE SEGURANÇA.			
10	2.09.03.0187-7	2	XX	LICENCIAMENTO DO FIREWALL ALTA CAPACIDADE TIPO I - ATIVA AS FUNCIONALIDADES AVANÇADAS DO NGFW E ATIVA SUPORTE PELO PERÍODO DE 24 MESES.			
11	2.09.03.0188-5	400	XX	LICENCIAMENTO DE SUPORTE JUNTO O FABRICANTE - PROPAGADOR DE SINAL TIPO I			
12	2.09.03.0189-3	30	XX	LICENCIAMENTO DE SUPORTE JUNTO O FABRICANTE - PROPAGADOR DE SINAL TIPO II			
13	2.09.03.0190-7	1	XX	LICENCIAMENTO DE SUPORTE JUNTO O FABRICANTE - PLATAFORMA DE AUTENTICAÇÃO E GERENCIAMENTO DA SOLUÇÃO DE SEGURANÇA			
14	2.09.03.0191-5	1	XX	LICENCIAMENTO DE SUPORTE JUNTO O FABRICANTE - PLATAFORMA DE ANÁLISE DE LOG CENTRALIZADO DA SOLUÇÃO DE SEGURANÇA			
15	2.09.03.0197-4	2	XX	INSTALACAO FIREWALL DE ALTA CAPACIDADE TIPO I			
16	2.09.03.0198-2	400	XX	INSTALACAO PROPAGADOR DE SINAL SEM FIO TIPO I - INDOOR			
17	2.09.03.0199-0	30	XX	INSTALACAO PROPAGADOR DE SINAL SEM FIO TIPO II - OUTDOOR			

18	2.09.03.0200-8	200	XX	INSTALACAO SWITCH GERENCIAVEL TIPO I			
19	2.09.03.0201-6	1	XX	INSTALACAO PLATAFORMA DE AUTENTICACAO E GERENCIAMENTO DA SOLUCAO DE SEGURANCA			
20	2.09.03.0202-4	1	XX	INSTALACAO PLATAFORMA DE ANÁLISE DE LOG CENTRALIZADO DA SOLUCAO DE SEGURANCA			
21	2.09.03.0203-2	123	XX	INSTALACAO RACK 19 POLEGADAS 8US			
22	2.09.03.0204-0	123	XX	INSTALACAO NOBREAK TIPO I - 1500VA			
23	2.09.03.0205-9	8.600	XX	INSTALACAO INFRAESTRUTURA DE COMUNICACAO LOGICA COMPLETA			
24	2.09.03.0231-8	12	XX	SERVICOS DE SUPORTE E MANUTENCAO PREVENTIVA E CORRETIVA			
					VALOR TOTAL GLOBAL LOTE	**R$**	

Prazo de validade da proposta: no mínimo 60 (sessenta) dias.

Prazo para entrega: até 30 (trinta) dias corridos contados do recebimento da Autorização de Fornecimento.

Declaramos que estamos cientes e aceitamos todas as exigências, normas e prazos estabelecidos neste edital e nos seus Anexos, e que os produtos ofertados atendem às especificações contidas no Termo de Referência - Anexo I.

Local....., de..... de.....de 2026

Assinatura e carimbo da empresa

ANEXO III (MODELO)

DECLARAÇÃO DE MICROEMPRESA E EMPRESA DE PEQUENO PORTE

PROCESSO Nº. 3548807.425.00007034/2025-90

PREGÃO ELETRÔNICO Nº 35/2026

D E C L A R A Ç Ã O

(Razão Social da Empresa), estabelecida a Rua _____ nº. ____ , bairro _____, no município de _____, Estado de _____, inscrita no CNPJ/MF sob nº. _____, Inscrição Estadual nº. _____, neste ato representado por seu (sócio/procurador), Sr. _____, portador da Cédula de Identidade RG nº. _____, inscrito no CPF/MF sob o nº. _____, no uso de suas atribuições legais, DECLARA, sob as penas da Lei, que a receita bruta do exercício anterior (na forma da lei) não excedeu o limite fixado no artigo 3º da Lei Complementar 123/2006 e posteriores alterações e artigos 4º e 5º da Lei Municipal 4660/2008, no que couber, conforme o caso, e que não se enquadra em qualquer das hipóteses de exclusão relacionadas na legislação citada.

Declara, ainda, que não tem nenhum dos impedimentos do parágrafo 4º do art. 3º da Lei Complementar 123/2006, devidamente atualizada, ciente da obrigatoriedade de declarar ocorrências posteriores.

Era o que tinha a declarar, a fim de produzir os efeitos jurídicos e legais de direito.

_____, _____ de _____ de 2026.

_____

Razão Social da Empresa

Nome do Responsável/Procurador

Cargo do Responsável/Procurador

Nº. Documento identidade

ANEXO IV (MODELO)

DECLARAÇÃO DE REGULARIDADE PERANTE O MINISTÉRIO DO TRABALHO E EMPREGO, CONFORME PORTARIA 547, DE 11 DE ABRIL DE 2025 DO MINISTÉRIO DO TRABALHO E EMPREGO E RELATIVAS AOS ARTIGOS 63, INCISO IV E 68, INCISO VI, DA LEI FEDERAL 14.133/21

PROCESSO Nº.
PREGÃO ELETRÔNICO Nº

D E C L A R A Ç Ã O

(Razão Social da Empresa), estabelecida a Rua _____ nº. ____ - (bairro), no município de _____, Estado de _____, inscrita no C.N.P.J. sob nº. _____, Inscrição Estadual nº. _____, neste ato representada por seu (sócio/procurador), no uso de suas atribuições legais, vem, **DECLARAR,** para fins de participação no **Processo Licitatório nº _____ Pregão Eletrônico nº___/____,** sob as penas da Lei, que:

- Está em situação regular perante o Ministério do Trabalho, uma vez que cumpre as disposições impostas pelo inciso XXXIII, do Artigo 7º, da Constituição Federal;

- 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;

- Cumpre a reserva legal de contratação de pessoas com deficiência e reabilitados da Previdência Social e de contratação de aprendizes, conforme disposto na Portaria 547, de 11 de abril de 2025 do Ministério do Trabalho e Emprego;

- A proposta econômica 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 entrega da proposta.

_____, ____ de _____ de 2026.

Razão Social da Empresa
Nome do Responsável/Procurador
Cargo do Responsável/Procurador
Nº. Documento identidade

ANEXO V (MODELO)

DECLARAÇÃO DE ADEQUAÇÃO DA COOPERATIVA À LEI FEDERAL Nº 12.690/2012 E ENQUADRAMENTO COMO COOPERATIVA QUE PREENCHA AS CONDIÇÕES ESTABELECIDAS NO ART. 34, DA LEI FEDERAL Nº 11.488/2007.

PROCESSO Nº. 3548807.425.00007034/2025-90
PREGÃO ELETRÔNICO Nº 35/2026

Eu, _____, portador do RG nº _____ e do CPF nº _____, representante legal do licitante _____ (*nome empresarial*), interessado em participar do Pregão Eletrônico nº ___/___, Processo n° ___/___, **DECLARO**, sob as penas da Lei, que:

a) O Estatuto Social da cooperativa encontra-se adequado à Lei Federal nº 12.690/2012;
b) A cooperativa aufere Receita Bruta até o limite definido no inciso II do *caput* do art. 3º da Lei Complementar Federal n° 123/2006, a ser comprovado mediante Demonstração do Resultado do Exercício ou documento equivalente. *****

*** Para usufruir do tratamento diferenciado às microempresas e empresas de pequeno porte**

(Local e data).

_____
(Nome/assinatura do representante legal)

ANEXO VI

TERMO DE CIÊNCIA E DE NOTIFICAÇÃO

CONTRATANTE: _____

CONTRATADO: _____

CONTRATO Nº (DE ORIGEM): _____

OBJETO: _____

Pelo presente TERMO, nós, abaixo identificados:

1. Estamos CIENTES de que:

a) o ajuste acima referido, seus aditamentos, bem como o acompanhamento de sua execução contratual, estarão sujeitos a análise e julgamento pelo Tribunal de Contas do Estado de São Paulo, cujo trâmite processual ocorrerá pelo sistema eletrônico;

b) poderemos ter acesso ao processo, tendo vista e extraindo cópias das manifestações de interesse, Despachos e Decisões, mediante regular cadastramento no Sistema de Processo Eletrônico, em consonância com o estabelecido na Resolução nº 01/2011 do TCESP;

c) além de disponíveis no processo eletrônico, todos os Despachos e Decisões que vierem a ser tomados, relativamente ao aludido processo, serão publicados no Diário Oficial Eletrônico do Tribunal de Contas do Estado de São Paulo (https://doe.tce.sp.gov.br/), em conformidade com o artigo 90 da Lei Complementar nº 709, de 14 de janeiro de 1993, iniciando-se, a partir de então, a contagem dos prazos processuais, conforme regras do Código de Processo Civil;

d) as informações pessoais dos responsáveis pela contratante e interessados estão cadastradas no módulo eletrônico do "Cadastro Corporativo TCESP – CadTCESP", nos termos previstos no Artigo 2º das Instruções nº01/2024, conforme "Declaração(ões) de Atualização Cadastral" anexa (s);

e) é de exclusiva responsabilidade do contratado manter seus dados sempre atualizados.

2. Damo-nos por NOTIFICADOS para:

a) O acompanhamento dos atos do processo até seu julgamento final e consequente publicação;

b) Se for o caso e de nosso interesse, nos prazos e nas formas legais e regimentais, exercer o direito de defesa, interpor recursos e o que mais couber.

LOCAL e DATA: _____

AUTORIDADE MÁXIMA DO ÓRGÃO/ENTIDADE:

Nome:_____

Cargo:_____

CPF: _____

RESPONSÁVEIS PELA HOMOLOGACÃO DO CERTAME OU RATIFICACÃO DA DISPENSA/INEXIGIBILIDADE DE LICITACÃO:

Nome:_____

Cargo:_____

CPF: _____

Assinatura: _____

RESPONSÁVEIS QUE ASSINARAM O AJUSTE:

Pelo contratante:

Nome:_____

Cargo:_____

CPF: _____

Assinatura: _____

Pela Detentora:

Nome:_____

Cargo:_____

CPF: _____

Assinatura: _____

ORDENADOR DE DESPESAS DA CONTRATANTE:

Nome:_____

Cargo:_____

CPF: _____

Assinatura: _____

GESTOR(ES) DO CONTRATO:

Nome:_____

Cargo:_____

CPF: _____

Assinatura: _____

DEMAIS RESPONSÁVEIS (*):

Tipo de ato sob sua responsabilidade: _____

Nome:_____

Cargo:_____

CPF: _____

Assinatura: _____

(*) - O Termo de Ciência e de Notificação deve identificar as pessoas físicas que tenham concorrido para a prática do ato jurídico, na condição de ordenador da despesa; de partes contratantes; de responsáveis por ações de acompanhamento, monitoramento e avaliação; de responsáveis por processos licitatórios; de responsáveis por prestações de contas; de responsáveis com atribuições previstas em atos legais ou administrativos e de interessados relacionados a processos de competência deste Tribunal. Na hipótese de prestações de contas, caso o signatário do parecer conclusivo seja distinto daqueles já arrolados como subscritores do Termo de Ciência e de Notificação, será ele objeto de notificação específica.

ANEXO VII

MINUTA DA ATA DE REGISTRO DE PREÇOS

ATA DE REGISTRO DE PREÇOS PARA O FORNECIMENTO DE EQUIPAMENTOS DE REDE LÓGICA COM E SEM FIO PARA OS DEPARTAMENTOS MUNICIPAIS, INCLUINDO TODO MATERIAL E SERVIÇOS NECESSÁRIOS PARA SUA INSTALAÇÃO, QUE ENTRE SI FAZEM A PREFEITURA MUNICIPAL DE SÃO CAETANO DO SUL E A EMPRESA _____, ORIUNDA DO PROCESSO Nº. 3548807.425.00007034/2025-90- PREGÃO ELETRÔNICO Nº ____/2026

Aos ____ dias do mês de ____, do ano de 2026 (dois mil e vinte e seis), nesta cidade de São Caetano do Sul, no Gabinete do Senhor Prefeito, situado na Rua Eduardo Prado nº. 201, Bairro Cerâmica, Cidade de São Caetano do Sul, Estado de São Paulo, compareceram as partes entre si justas e pactuadas, a saber: de um lado a **PREFEITURA MUNICIPAL DE SÃO CAETANO DO SUL**, pessoa jurídica de direito público interno, inscrita no CNPJ/MF sob o nº. 59.307.595/0001-75, neste ato representada pela sua **Secretária Municipal de Gestão e Governo Digital** (devidamente qualificada no Termos de Ciências e de Notificação), doravante denominados simplesmente **"Contratante",** e, de outro lado, a empresa ____, com sede na ____, nº. ____, Bairro ____, Cidade ____, Estado ____, inscrita no CNPJ/MF sob o nº. ____, Inscrição Estadual nº. ____, neste ato representada por ____, portador da Cédula de Identidade RG nº. ____, inscrito no CPF/MF nº. ____, residente e domiciliado na ____, doravante denominada simplesmente "**Detentora"**, as quais, na presença das testemunhas adiante nomeadas e assinadas, resolvem firmar o presente contrato, em observância às disposições da Lei Federal 14.133/2021 e seus atos regulamentadores; da Lei Complementar Federal 123/06 em suas redações atuais; do Decreto Municipal nº. 12.176/2025; supletivamente aos princípios da teoria geral dos contratos e as disposições de direito privado e, mediante as cláusulas e condições a seguir enunciadas mediante as cláusulas e condições que mutuamente aceitam e outorgam, que seguem:

CLÁUSULA PRIMEIRA – DO OBJETO E DO VALOR

1.1. Constitui o objeto deste Pregão o **REGISTRO DE PREÇOS PARA O FORNECIMENTO DE EQUIPAMENTOS DE REDE LÓGICA COM E SEM FIO PARA OS DEPARTAMENTOS MUNICIPAIS, INCLUINDO TODO MATERIAL E SERVIÇOS NECESSÁRIOS PARA SUA INSTALAÇÃO,** conforme **especificações técnicas** descritas abaixo:

ITEM	CÓDIGO	QUANTIDADE	UNIDADE	ESPECIFICACAO	MARCA/ MODELO	VALOR UNITÁRIO	VALOR TOTAL
1	1.14.01.2228-0	123	UN	NOBREAK TIPO 1 - 1500VA . MAIORES INFORMAÇÕES NO MEMORIAL DESCRITIVO.			
2	1.14.01.2384-7	400	UN	PROPAGADOR DE SINAL SEM FIO PARA TRANSMISSÃO E RECEPÇÃO TIPO I, CONFORME TERMO DE REFERÊNCIA			
3	1.14.01.2385-5	30	UN	PROPAGADOR DE SINAL SEM FIO PARA TRANSMISSÃO E RECEPÇÃO TIPO II, CONFORME TERMO DE REFERÊNCIA			
4	1.14.01.2387-1	200	UN	SWITCH TIPO I, CONFORME TERMO DE REFERÊNCIA			
5	1.14.01.2393-6	123	UN	RACK 19" 8US, CONFORME TERMO DE REFERÊNCIA			
6	1.14.01.2443-6	8.600	M	INFRAESTRUTURA TUBULAR COMPLETA INCLUSO ACESSORIOS PARA FIXACAO			
7	1.14.01.2491-6	2	UN	FIREWALL NGF DE ALTA CAPACIDADE			
8	1.14.01.2819-9	1	UN	PLATAFORMA DE AUTENTICAÇÃO E GERENCIAMENTO DA SOLUÇÃO DE SEGURANÇA			
9	1.14.01.2820-2	1	UN	PLATAFORMA DE ANÁLISE DE LOG CENTRALIZADO DA SOLUÇÃO DE SEGURANÇA.			
10	2.09.03.0187-7	2	XX	LICENCIAMENTO DO FIREWALL ALTA CAPACIDADE TIPO I - ATIVA AS FUNCIONALIDADES AVANÇADAS DO NGFW E ATIVA SUPORTE PELO PERÍODO DE 24 MESES.			

11	2.09.03.0188-5	400	XX	LICENCIAMENTO DE SUPORTE JUNTO O FABRICANTE - PROPAGADOR DE SINAL TIPO I			
12	2.09.03.0189-3	30	XX	LICENCIAMENTO DE SUPORTE JUNTO O FABRICANTE - PROPAGADOR DE SINAL TIPO II			
13	2.09.03.0190-7	1	XX	LICENCIAMENTO DE SUPORTE JUNTO O FABRICANTE - PLATAFORMA DE AUTENTICAÇÃO E GERENCIAMENTO DA SOLUÇÃO DE SEGURANÇA			
14	2.09.03.0191-5	1	XX	LICENCIAMENTO DE SUPORTE JUNTO O FABRICANTE - PLATAFORMA DE ANÁLISE DE LOG CENTRALIZADO DA SOLUÇÃO DE SEGURANÇA			
15	2.09.03.0197-4	2	XX	INSTALACAO FIREWALL DE ALTA CAPACIDADE TIPO I			
16	2.09.03.0198-2	400	XX	INSTALACAO PROPAGADOR DE SINAL SEM FIO TIPO I - INDOOR			
17	2.09.03.0199-0	30	XX	INSTALACAO PROPAGADOR DE SINAL SEM FIO TIPO II - OUTDOOR			
18	2.09.03.0200-8	200	XX	INSTALACAO SWITCH GERENCIAVEL TIPO I			
19	2.09.03.0201-6	1	XX	INSTALACAO PLATAFORMA DE AUTENTICACAO E GERENCIAMENTO DA SOLUCAO DE SEGURANCA			
20	2.09.03.0202-4	1	XX	INSTALACAO PLATAFORMA DE ANÁLISE DE LOG CENTRALIZADO DA SOLUCAO DE SEGURANCA			
21	2.09.03.0203-2	123	XX	INSTALACAO RACK 19 POLEGADAS 8US			
22	2.09.03.0204-0	123	XX	INSTALACAO NOBREAK TIPO I - 1500VA			
23	2.09.03.0205-9	8.600	XX	INSTALACAO INFRAESTRUTURA DE COMUNICACAO LOGICA COMPLETA			

24	2.09.03.0231-8	12	XX	SERVICOS DE SUPORTE E MANUTENCAO PREVENTIVA E CORRETIVA			
VALOR TOTAL GLOBAL LOTE					**R$**		

1.2. Este projeto contempla o fornecimento e instalação dos equipamentos, de forma que seja possível sua utilização logo após implantação.

1.3. Deverá ser contemplando todos os materiais e serviços necessários para a instalação e configuração dos equipamentos.

1.4. Após implantação, os equipamentos deverão estar prontos para o uso, devidamente instalados e configurados.

1.5. **ESPECIFICAÇÕES TÉCNICAS DOS EQUIPAMENTOS E SISTEMAS DA REDE DE COMUNICAÇÃO**

As configurações descritas são as mínimas solicitadas, sendo que a licitante poderá ofertar equipamento superior para atender o edital.

Os equipamentos ativos deverão estar em linha de produção pelo fabricante na data de entrega da proposta.

1.6. **PROPAGADOR DE SINAL PARA TRANSMISSÃO E RECEPÇÃO TIPO I**

Equipamento de Propagação de sinal para rede local sem fio, devidamente licenciado e configurável via software;
Deverá ser do mesmo fabricante da Controladora de fornecimento deste projeto;
Possuir no mínimo uma porta Ethernet 100M/1000M/2.5G/5.0G Multigigabit Ethernet (RJ45;
Possuir botão de Reset ou possibilitar reset através do injetor PoE;
Possuir Bluethoot integrado;
Possuir porta USB;
Possuir porta RS-232 RJ45 Serial Port;
Suportar ao menos as tecnologias 802.11 a/b/g/n/ac;
Suportar a tecnologia 802.11ax;
Suportar UL MU-MIMO; DL UM MIMO; BBS Coloring;
Possui recurso de economia de energia “Enhanced Target Wake Time(TWT)”;
Suportar OFDMA;

Possui recursos de monitoramento sem fio de varredura de APs não autorizados (Rogue Scan Radio), Varredura de pacotes (Packet Sniffer) e analisador de espectro (Spectrum Analyser);
O equipamento deve possuir 6 antenas, distribuídas da seguinte forma:

- 2 antenas Wi-Fi Dual Band (2.4GHz/5GHz)
- 2 antenas Wi-Fi na banda de 6GHz
- 1 antena BLE/ZigBee
- 1 antena GPS

Operar em Triband (2.4 Ghz, 5 Ghz e 6Ghz);

Radio 1: Frequência: 2.4GHz: Largura de canais: 20/40MHz / Modulação: BPSK, QPSK, 64/256/1024 QAM / MIMO 2x2;
Radio 2: Frequência: 5.0GHz: Largura de canais: 20/40/80/160MHz / Modulação: BPSK, QPSK, 16/64/256/1024/4096 QAM / MIMO: 2x2;
Radio 3: Frequency: 6.0Ghz: Largura de canais: 20/40/80/160/320mhz / BPSK, QPSK, 16/64/256/1024/4096 QAM / MIMO 2x2;
Taxa de dados: Radio 1 de até 688Mbps / Radio 2 até 2800Mbps e Radio 3 até 5700Mbps
Suportar 2x2 MIMO em 2.4Ghz, 5Ghz e 6Ghz;
Possuir ganho mínimo em 2,4 Ghz de 4.5 dBi;
Possuir ganho mínimo em 5 Ghz e 6Ghz de 5.0 dBi;
Suportar até 512 usuários por rádio (radio 1, radio 2 e radio 3);
Possuir suporte até 8 SSIDs;
Suporta SSID do tipo Local-Bridge, Mesh e Tunnel;
Suportas modulação 1024QAM;
Ser compatível com o padrão IEEE 802.3at PoE;
Conformidade com a IEEE 802.1q;
Suportar 802.11k;
Suportar 802.11v;
Suportar 802.11r;
Suportar WEP;
Suportar WPA2;
Suportar WPA3;
Suportar Autenticação IEEE 802.1X;
Suportar Autenticação por MAC Address;
Suportar Autenticação por Portal;
Suportar 802.11w;
Acompanha acessórios para fixação na parede e teto;
Acompanha injetor PoE bivolt automático, compatível com IEEE 802.3at, homologado pelo fabricante do access point.

Possui Led de indicação de funcionamento. A led pode ser mantida apagada;
Possuir homologação da ANATEL válida no momento da entrega dos equipamentos;
Certificação RoHS (materiais livre de substâncias perigosas) ou equivalente;
Certificação FCC (utiliza frequências dentro dos limites regulatórios) ou equivalente;
Atende certificação “UL2043 Plenum Material” de utilização de materiais não propagante a chamas ou equivalente;
Possibilita dispositivos habilitados se conectarem automaticamente no ponto de acesso próximo (Wi-Fi aliance Certified – Passpoint);
MTBF aproximado de 10 anos;
Temperatura de operação de 0ºC à 50ºC e armazenamento de -10ºC à 70ºC;
Humidade de 5% a 90% não condensado;
Consumo máximo de 16w em POE e 15w 12V DC;
Fornecido com licenciamento do tipo permanente para todas as funcionalidades solicitadas em nome da contratante.
Possui 24 meses de garantia, sendo 3 meses garantia legal mais 21 meses garantia estendida.

1.7. PROPAGADOR DE SINAL PARA TRANSMISSÃO E RECEPÇÃO TIPO II (outdoor)

Equipamento de Propagação de sinal para rede local sem fio, devidamente licenciado e configurável via software;
Deverá ser do mesmo fabricante da Controladora de fornecimento deste projeto;
Possuir no mínimo uma porta Ethernet 100/1000/ Base-T RJ45;
Possuir botão de Reset ou possibilitar reset através do injetor PoE;
Possuir Bluethoot integrado;
Possuir porta RS-232 Rj45 Serial Port;
Suportar ao menos as tecnologias 802.11 a/b/g/n/ac;
Suportar a tecnologia 802.11ax;
Suportar UL MU-MIMO; DL UM MIMO; BBS Coloring;
Possui recurso de economia de energia “Enhanced Target Wake Time(TWT)”;
Suportar OFDMA;
Possui recursos de monitoramento sem fio de varredura de APs não autorizados (Rogue Scan Radio), Varredura de pacotes (Packet Sniffer) e analisador de espectro (Spectrum Analyser);
Possuir 3 antenas internas + BLE, sendo 2 antenas dual band (WiFi) e antena BLE + 2.4ghz;;
Operar em Dual-Band (2.4 Ghz e 5 Ghz);
Radio 1: Frequência: 2.4GHz: Largura de canais: 20/40MHz / Modulação: BPSK, QPSK, 64/256/1024 QAM / MIMO 2x2;
Radio 2: Frequência: 5.0GHz: Largura de canais: 20/40/80MHz / Modulação: BPSK, QPSK, 64/256/1024 QAM / MIMO: 2x2;
Radio 3: Frequency: 2.4GHz, 5.0GHz, MIMO varredura frequência;

Taxa de dados: Radio 1 de até 574Mbps / Radio 2 até 1200Mbps e radio 3 varredura de frequência;
Suportar 2x2 MIMO em 2.4Ghz;
Suportar 2X2 em MIMO 5Ghz;
Possuir ganho mínimo em 2,4 Ghz de 10 dBi;
Possuir ganho mínimo em 5 Ghz de 10 dBi;
Suportar até 512 usuários por rádio (radio 1, radio 2);
Possuir suporte até 16 SSIDs;
Suporta SSID do tipo Local-Bridge, Mesh e Tunnel;
Suportas modulação 1024QAM;
Ser compatível com o padrão IEEE 802.3at PoE;
Conformidade com a IEEE 802.1q;
Suportar 802.11k;
Suportar 802.11v;
Suportar 802.11r;
Suportar WEP;
Suportar WPA2;
Suportar WPA3;
Suportar Autenticação IEEE 802.1X;
Suportar Autenticação por MAC Address;
Suportar Autenticação por Portal;
Suportar 802.11w;
Acompanha acessórios para fixação na parede e teto;
Acompanha injetor PoE bivolt automático, compatível com IEEE 802.3at, homologado pelo fabricante do access point.), tipo Gigabit Ethernet (GE);
Possui Led de indicação de funcionamento. A led pode ser mantida apagada;
Possuir homologação da ANATEL válida no momento da entrega dos equipamentos;
Certificação RoHS;
Possibilita dispositivos habilitados se conectarem automaticamente no ponto de acesso próximo (Wi-Fi aliance Certified – Passpoint);
MTBF aproximado de 10 anos;
Proteção contra surtos;
Proteção IP67;
Temperatura de operação de 0ºC à 60ºC e armazenamento de -10ºC à 70ºC;
Humidade de 10% a 90% não condensado;
Consumo máximo 17w;
Fornecido com licenciamento do tipo permanente para todas as funcionalidades solicitadas em nome da contratante.
Possui 24 meses de garantia, sendo 3 meses garantia legal mais 21 meses garantia estendida.

1.8. **SWITCH TIPO I**

Switch gerenciável, POE com no mínimo, 24 portas 1000Base-T e 4 portas 1GE SFP;
Possuir capacidade de associação das portas compatível com a norma IEEE 802.3ad.
Possuir, 24 portas UTP (RJ45) PoE+ e, pelo menos, 4 portas óticas (podendo ser combo) com suporte a módulos de fibra multimodo e monomodo (SFP).
Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);
Deve ser capaz de alimentar as 24 portas com IEEE 802.3af e IEEE 802.3at.
As interfaces 10/100/1000 devem obedecer às normas técnicas IEEE802.3, IEEE802.3u (100BaseTX) e 802.3ab (1000BaseT);
Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas.
Implementar VLANs por porta.
Implementar VLANs compatíveis com o padrão IEEE 802.1q.
Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk 802.1q.
Possuir porta de console para gerenciamento e configuração via linha de comando CLI com conector RJ-45 ou conector padrão RS-232 ou USB;
Possuir interface USB para conexão de flash drive que permita cópias de arquivos de configuração e imagens de software para upgrades.
Possuir capacidade de empilhamento de até 9 unidades.
Possuir fonte de alimentação AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz).
Deverá ser fornecido cabo de alimentação padrão Brasil;
Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.
Deve possuir no máximo 1 Rack Unit (RU).
Possuir LEDs para a indicação do status das portas.
Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.
Possuir suporte a MIB II, conforme RFC 1213.
Possuir armazenamento interno das mensagens de log;
Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU;
Implementar nativamente RMON (History, Statistcs, Alarms e Events);
Implementar os protocolos LLDP (IEEE 802.1AB) e LLDP-MED, com auto negociação de energia para PoE.
O equipamento deve suportar para gerência e administração o uso dos protocolos: SNMP, NTP, HTTPS, SSH, Telnet e RADIUS;

Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet.
Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP.
Permitir a gravação de log externo (syslog).
Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
Permitir o espelhamento do tráfego de uma porta;
Implementar funcionalidade de QoS;
Deve permitir configuração de Vlan centralizado;
Implementar o protocolo NTP (Network Time Protocol);
Implementar DHCP Relay e DHCP Server;
Implementar roteamento estático IPv4;
Implementar roteamento estático IPv6;
Implementar roteamento entre VLANs
Possuir capacidade para pelo menos 32.000 endereços MAC.
Implementar, no mínimo, 4000 VLANS simultaneamente.
Deve possuir capacidade de comutação de no mínimo 128Gbps.
Deve possuir taxa de encaminhamento de no mínimo 190Mpps.
Suportar Jumbo frames.
Implementar filtragem de pacotes (ACL - Access Control List) IPv4 e IPv6.
Implementar o protocolo SSH para acesso à interface de linha de comando.
Implementar mecanismos de autenticação RADIUS Accounting;
Possuir controle de broadcast, multicast e unicast.
Possuir suporte a mecanismo de proteção “Spanning-Tree”;
Implementar padrão IEEE 802.1d;
Implementar padrão IEEE 802.1q;
Implementar padrão IEEE 802.1p;
Implementar padrão IEEE 802.3ad;
Implementar controle de acesso por porta, usando o padrão IEEE 802.1x;
Suportar a autenticação 802.1x via endereço MAC;
Implementar padrão IEEE 802.1w
Implementar padrão IEEE 802.1s
Implementar o protocolo IGMP Snooping;
Implementar interface do switch o protocolo MLD (Multicast Listener Discovery).
Implementar DSCP;
Suporte aos mecanismos de QoS WRR (Weighted Round Robin) ou SRR (Shaped Round Robin).
Implementar IPv6.

Implementar ICMPv6;
Possuir os seguintes protocolos: Ping e Traceroute
HTTP sobre IPv6.
Implementar funcionalidade de provisionamento simplificado do tipo zero-touch.
Implementar funcionalidade OPS (Open Programmability System) ou similar que permita o uso de scripts python para funções de operação e manutenção.
Implementar Sflow ou Netstream ou Netflow Lite ou protocolo equivalente.
Implementar QinQ.
Implementar os protocolos de roteamento RIPv2 e OSPF.
Implementar no mínimo 16.000 rotas em IPv4.
Implementar no mínimo 2.000 ACLs.
Fornecido com licenciamento do tipo permanente para todas as funcionalidades solicitadas em nome da contratante.
Acompanha fonte instalada dimensionada para alimentar simultaneamente todas as 24 portas PoE (802.3af/802.3at) totalizando até 370w;
Consumo máximo de 452w;
Temperatura de funcionamento de 0°C até +45°C.
Fluxo de ar Lateral para traseira;
Peso aproximado de 3,9Kg;
Nível de barulho até 45.8dBA;
Certificação RoHS2 / FCC ou equivalente;
Deve possuir homologação ANATEL válida.
Possui 24 meses de garantia, sendo 3 meses garantia legal mais 21 meses garantia estendida.

1.9. **FIREWALL DE ALTA CAPACIDADE TIPO I**

Firewall de nova geração (NGFW), deverá ser instalado na localidade DTI – Departamento de Tecnologia da Informação.

Especificações técnicas:
Deverá possuir as seguintes interfaces:
-1 porta de 2.5/GE RjJ45 HA Port;
-1 porta GE RJ45 para gerenciamento;
-16 portas GE RJ45;
-8 portas GE SFP (Slots);
-4 slots 10GE/GE (slots SFP+/SFP);
-4 slots de baixa latência de 25GE/10GE (SFP28/SFP+);
-2 portas USB;
-Acompanha 8 transceivers de 1GE SFP instalado;

-Acompanha 4 transceivers de 10GE SFP+ instalado;
-Possui 2 (duas) fontes instaladas do tipo Hot Swap;
-Possui 2 (dois) ventiladores internos instalados;
-Possui armazenamento interno com no mínimo 2 unidades armazenamento com capacidade de 480GB cada;
-Possui modulo TPM instalado;
-Possui Bluetooth Low Energy (BLE);

O Firewall deverá implementar a seguinte performance:
-Throughput do Firewall (pacotes por segundo)– 229Mbps
-Throughput do Firewall IPV4 (1518/512/64 bytes em UDP) 164/163/153Gbps;
-Latência de 3.8/2.5us (64 bytes/UDP)
-Sessões simultâneas – 16 milhões;
-Novas sessões por segundo – 720.000;
-Throughput do IPS (us misto) – 42Gbps
-Throughput de proteção NGFW: 30Gbps.(com log habilitado, firewall, application control e proteção de malware habilitados)
-Throughput contra ameaças (Threat): 30Gbps.
-Politicas de Firewall: 50.000;
-IPSEC VPN Throughput (512 byte): 55Gbps.
-Ipsec túneis VPN – 2000;
-Usuários VPN SSL simultâneos: 10.000;
-Inspeção SSL Throughput: 16.7Gbps;

Possui funcionalidade de controladora de pontos de acesso integrado;
A solução ofertada deve permitir o gerenciamento de até 2.048 pontos de acesso, garantindo escalabilidade para o ambiente.
Possibilitar controlador e gerenciar a rede sem fio e os equipamentos de rede sem fio de fornecimento deste projeto.
Possibilita configuração em alta disponibilidade nos modos ativo-ativo/ cluster ou Ativo-passivo;
Equipamento específico para montagem em rack de telecomunicação padrão 19 polegadas com altura de no máximo 2Us de rack;
Alimentação bivolt automático;
Acompanha cabo de alimentação elétrica padrão brasileiro;
Consumo médio /máximo aproximado: 184w/323w;
Possui duas fontes instaladas padrão 80Plus ou superior;
Temperatura de operação: 0ºC a 45ºC;
Humidade: 10% a 90% não condensado;

Deverá possuir Certificação ANATEL válida;
Possui 24 meses de garantia, sendo 3 meses garantia legal mais 21 meses garantia estendida.

Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;

Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.

CARACTERÍSTICAS GERAIS
A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open source (produto montado);

Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

Deve possuir garantia do fabricante com validade mínima de 24 (vinte e quatro) meses;

As funcionalidades de segurança que compõem a solução podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação, acompanhem os mesmos termos de garantia, atualizações e manutenção, e suportem gerenciamento centralizado;

A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
Todos os equipamentos fornecidos não devem ultrapassar a medida máxima de 1U cada;
O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
Os dispositivos de proteção de rede devem possuir suporte a Vlans;
Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

Recursos
Deve possibilitar melhorar a qualidade e disponibilidade de aplicações de voz;
Deve suportar BGP, OSPF, RIP e roteamento estático;
Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
Deve suportar NAT dinâmico (Many-to-Many);

Deve suportar NAT estático (1-to-1);
Deve suportar NAT estático bidirecional 1-to-1;
Deve suportar Tradução de porta (PAT);
Deve suportar NAT de Origem;
Deve suportar NAT de Destino;
Deve suportar NAT de Origem e NAT de Destino simultaneamente;
Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
Deve suportar NAT64;
Deve implementar o protocolo ECMP;
Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
Enviar log para sistemas de monitoração externos;
Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
Proteção anti-spoofing;
Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo layer 3;
A configuração em alta disponibilidade deve sincronizar: Sessões;
A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;
A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;
O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
Deve possuir suporte à criação de sistemas virtuais (VDOMs) no mesmo appliance;
Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
Controle, inspeção e descriptografia de SSL para tráfego de Saída (Outbound), devendo suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);

Políticas

Deverá suportar controles por zonas de segurança;
Deverá suportar controles de políticas por porta e protocolo;

Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);
Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2;
Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
Suporte a objetos e regras IPV6;
Suporte a objetos e regras multicast;
Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

Aplicações
Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
Reconhecer pelo menos 5.500 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
Deve suportar a decriptografia do tráfego SSL (IPv4 e IPv6) e espelhar este tráfego para uma interface específica.
Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;

Identificar o uso de táticas evasivas via comunicações criptografadas;
Atualizar a base de assinaturas de aplicações automaticamente;
Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
Deve permitir exceções de aplicações caso uma regra de controle de aplicação seja configurada para permitir ou bloquear uma categoria de aplicação.
O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
Deve alertar o usuário quando uma aplicação for bloqueada;
Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts e bloquear a chamada de vídeo;
Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação e categoria da aplicação;
Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.

Controladora Wireless;
Solução que deverá administrar e controlar de maneira centralizada os pontos de acesso wireless do mesmo fabricante da solução ofertada, caso seja necessário alguma solução como complemento a mesma deve ser fornecida em conjunto com o Firewall e os valores inclusos no seu valor final.
Deve ser fornecido na forma de appliance físico composto pelo conjunto de hardware e software;
Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;

Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;
A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;
A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;
O contradora wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso;
Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;
Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;
Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;
Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;
A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;
A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;
A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;
A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;
A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;
A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;
A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;
A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexbilidade no design da rede wireless;
A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;
A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;
A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;

A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;
A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;
A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;
A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;
Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;
A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;
A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;
A solução deve suportar a configuração do BLE (Blueooth Low Energy) nos pontos de acesso que tenham este recurso;
A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;
A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;
A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;
A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;
A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal

oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;
A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;
A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;
A solução deve implementar recurso para controle de URLs acessadas na rede wireless através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários e SSID;
A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede wireless;
O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria;
A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas;
A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução;
A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento;
A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e para websites/domínios específicos;
A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS;
A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede wireless com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig;
O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6;
A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução;
A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede wireless;
A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução;

A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações;
A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI;
A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada SSID;
A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS;
A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless;
"A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:
Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);
Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;
ASLEAP;
Null Probe Response or Null SSID Probe Response;
Long Duration;
Ataques contra Wireless Bridges;
Weak WEP;
Invalid MAC OUI.
A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;
A solução deve implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede wireless;
Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;
Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS;
Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
A solução deve permitir a configuração de múltplas chaves de autenticação PSK para utilização em um determinado SSID;
Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;
A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;
Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;
A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
A solução deve permitir a configuração do captive portal com endereço IPv6;
A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;
A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;
A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;
A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;
A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;
A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;
A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;
A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;

A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;
A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);
A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;
A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;
A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;
A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;
A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;
A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;
A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;
A solução deve possuir ferramentas de diagnósticos e debug;
A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;
A solução deve suportar comunicação com elementos externos através de REST API;
A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;

Prevenção de ameaças
Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e colocar em quarentena o IP do atacante por um intervalo de tempo;
As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
Deve ser possível criar uma assinatura de IPS utilizando o identificador CVE assim como um “wildcard” do CVE para abranger mais de um identificador.

Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
Deve permitir o bloqueio de vulnerabilidades;
Deve permitir o bloqueio de exploits conhecidos;
Deve incluir proteção contra-ataques de negação de serviços;
Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
Detectar e bloquear a origem de portscans;
Bloquear ataques efetuados por worms conhecidos;
Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
Possuir assinaturas para bloqueio de ataques de buffer overflow;
Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
Identificar e bloquear comunicação com botnets;
Registrar no console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
Os eventos devem identificar o país de onde partiu a ameaça;
Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;
A solução de sandbox deve ser capaz de criar assinaturas e ainda inclui-las na base de antivírus do firewall, prevenindo a reincidência do ataque;

A solução de sandbox deve ser capaz de incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas (Block list), impedindo que esses endereços sejam acessados pelos usuários de rede novamente;
Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;
A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado;

Filtro de URLs
Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall;
Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
Possuir pelo menos 60 categorias de URLs;
Deve possuir a função de exclusão de URLs do bloqueio;
Permitir a customização de página de bloqueio;

Identificação de usuários
Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 e mais atuais;
Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;
Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

Deve 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);
Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

Filtro de dados
Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

Geolocalização
Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

VPN
Suportar VPN Site-to-Site e Cliente-To-Site;
Suportar IPSec VPN;
Suportar SSL VPN;
A VPN IPSec deve suportar 3DES;
A VPN IPSec deve suportar Autenticação MD5 e SHA-1;
A VPN IPSec deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
A VPN IPSec deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
A VPN IPSec deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
A VPN IPSec deve suportar Autenticação via certificado IKE PKI;
Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB ou agente VPN;
A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente de VPN;
Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
Atribuição de DNS nos clientes remotos de VPN;
Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
Suportar autenticação via AD/LDAP, certificado e base de usuários local;
Suportar leitura e verificação de CRL (certificate revocation list);
Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
Deve suportar que a conexão com a VPN seja estabelecida das seguintes formas: Antes do usuário autenticar na estação;
Deve suportar que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;
Deve suportar que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;
Deverá manter uma conexão segura com o portal durante a sessão;
O agente de VPN deve ser compatível com pelo menos: Windows10/11 e Mac OS 10.14 e superior.

Funcionalidades de gerenciamento avançado NGFW:
O equipamento deverá ser licenciado com todas as funcionalidades NGFW para o período de 24 meses, sendo possível sua renovação recorrentemente através de renovação de licença.

1.10. PLATAFORMA DE AUTENTICAÇÃO E GERENCIAMENTO

A solução deve ser baseada em appliance físico do mesmo fabricante da solução de NGFW e ter como objetivo a coleta, armazenamento e análise automatizada de registros e gestão WLAN em modo centralizado de todos os equipamentos a partir de uma única console de administração;
Deverá estar devidamente licenciada para:
Suportar a coleta de, no mínimo, 100 GB de logs diários;
Possuir e permitir espaço de armazenamento de, no mínimo, 10 TB;
O apliance deve suportar:
Pelo menos duas interfaces 2x GE RJ-45
Suportar a configuração de RAID 0 e 1 para os discos internos;
Possuir 2 fontes de alimentação interna, redundante e hot-swap;
Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

Possui 24 meses de garantia, sendo 3 meses garantia legal mais 21 meses garantia estendida.
Realizar o backup das configurações para permitir o retorno de uma configuração salva;
Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;
Deve suportar a definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.
A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;
Através da análise de tráfego de rede, web e DNS, deve suportar a verificação de máquinas potencialmente comprometidas ou usuários com uso de rede suspeito;
Realizar agregação via pontuação, para geração de um veredito sobre máquinas comprometidas na rede e atividades suspeitas;
Utilizar técnicas de machine learning para a captura de índices de comprometimento, através de URLs, domínios e endereços IPs maliciosos;
Deve possuir um painel com as informações de máquinas comprometidas indicando informações de endereço IP dos usuários, veredito, número de incidentes etc.;
Deve oferecer um portal do cliente fácil de usar, permitindo acesso às capacidades seguras de SD-WAN, como monitoramento e modelos SD-WAN, políticas e objetos, painéis analíticos, visualizações e relatórios, auditoria e recursos adicionais, como documentação e links;
Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;
Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;
Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;
Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;
Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;
Deve possuir mecanismos de remoção automática para logs antigos;
Permitir importação e exportação de relatórios
Deve ter a capacidade de criar relatórios no formato HTML, PDF, XML e CSV;
Deve permitir exportar os logs no formato CSV;
Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;
Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;
A solução deve ter relatórios predefinidos;
Deve permitir o envio automático dos logs para um servidor FTP externo a solução;
Deve ter a capacidade de personalizar a capa dos relatórios obtidos;

Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;
Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;
Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;
Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;
Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;
Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;
Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;
Permitir o envio por e-mail relatórios automaticamente;
Deve permitir que o relatório seja enviado por e-mail para o destinatário específico;
Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;
Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;
Deve permitir o uso de filtros nos relatórios;
Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;
Permitir especificar o idioma dos relatórios criados;
Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;
Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;
Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;
Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;
Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;
Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;
Deve permitir visualizar em tempo real os logs recebidos;
Deve permitir o encaminhamento de log no formato syslog;
Deve permitir o encaminhamento de log no formato CEF (Common Event Format);
Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;
Deve ser capaz de visualizar alertas de surtos e baixar automaticamente manipuladores de eventos e relatórios relacionados;

Deve permitir o time de resposta a incidentes identificar se um artefato malicioso de "Zero Day" encontrado na rede faz parte de alguma campanha específica de malware, se foi visto até o momento somente na rede da instituição;
Caso o malware faça parte de alguma campanha, deve ser detalhado qual o objetivo dela, tipos de indústria que já foram alvo do malware, comportamento malicioso conhecido sobre o malware e quais são os autores;
Deve permitir gerar alertas de eventos a partir de logs recebidos;
Deve suportar o serviço de Indicadores de Compromisso (IoC) do mesmo fabricante, que mostra as suspeitas de envolvimento do usuário final na Web e deve relatar pelo menos: endereço IP do usuário, nome do host, sistema operacional, veredito (classificação geral da ameaça), o número de ameaças detectadas;
A solução deve possuir garantia, suporte e atualizações ao software durante a vigência do contrato;

Solução de Identificação e Autenticação Centralizada
Características mínimas da Solução de Identificação e Autenticação Centralizada.
A solução deverá ser do mesmo fabricante da solução de NGFW de fornecimento deste projeto;
Poderá ser entregue em equipamento único ou com composição de equipamentos. para atender as funcionalidades exigidas.
Deverá possuir licenciamento para pelo menos 9000 usuários locais;
Deverá possuir licenciamento para até 1.000 grupos de usuários,
Deverá possuir licenciamento para até 500 certificados de usuários.
Deverá possuir licenciamento para até 50 tokens para dispositivos móveis, compatíveis com sistemas Android e iOS.

Suportar administração em interface gráfica (GUI) por HTTP e/ou HTTPS;
Suporta administração em interface baseada em linhas de comando (CLI) por TELNET e/ou SSH;
Permitir definir perfis de administradores para a solução, de modo que possa segmentar a responsabilidade dos administradores por tarefas operativas;
Possuir indicador visual, centralizado, de informações críticas (estado da licença, versão de firmware, consumo de CPU/Memória/Disco, quantidade de usuários criados e licenciados);
Suportar a atualização do firmware via interface gráfica, por processo simplificado e intuitivo;
Suportar customização de mensagens padrão da solução como páginas de erro, portais de autenticação, auto registro, reset de senha e outros. Suportar também a inclusão, alteração e remoção de imagens nas mensagens/páginas sem a necessidade de recursos ou conectividade externa;
Suportar configuração de Alta Disponibilidade (HA), reduzindo ao máximo os períodos de interrupção;
Suportar implementações de HA como "Ativo-Passivo" ou sincronizando configurações entre duas caixas ativas;

Permitir sincronismo automático de configurações entre todos os equipamentos que componham a solução em HA;
Suportar implementação de HA sincronizando configurações com appliances em localidades geograficamente separadas;
Suportar a opção de backup criptografado;
Suportar backup automatizado (agendados por critérios pré-definidos), não somente sob demanda;
Suportar o backup completo da configuração, incluindo base de usuários, grupos, tokens, certificados, configurações de single-sign-on e etc. A solução deve também permitir a restauração de toda configuração diretamente da interface gráfica;
Suportar NTP (Network Time Protocol), visando o sincronismo de hora/data;
Suportar SNMP v1, v2 e v3 permitindo consultar MIB própria e envio de Traps;
Suportar nativamente Trap SNMP indicando mudança de status de HA;
Suportar captura de pacotes através da interface gráfica para Troubleshoot avançado em ferramentas de análise de pacotes (ex.: Wireshark);
O equipamento deve permitir o envio de e-mails relacionados a reset de senha, aprovação de novos usuários, auto-registro de usuários e autenticação de segundo fator (token);
Deve suportar o envio de mensagens SMS para os usuários através de gateways SMS de terceiros ou seu próprio serviço de envio de SMS, sendo este segundo licenciado ou não;
Deve suportar o registro de todos os eventos que os usuários de sua base de dados local realizem com suas contas, tais como criação de um usuário, troca de senha de um usuário e alteração de informação gerais;

AUTENTICAÇÃO:
A solução deve efetuar autenticação para a gerência de identidade dos usuários da rede, ajudando a simplificar a administração dos mesmos sendo um ponto central de controle de autenticação, onde múltiplos métodos de autenticação possam ser consolidados;
Deve suportar autenticação em dois fatores (two-factor authentication);
Deve possuir suporte a autenticação de dois fatores em pelo menos tokens lógicos como software para dispositivos móveis, e-mail e SMS, permitindo que seja dada a escolha de qual dos tipos utilizar para cada usuário e situação;
A solução deve permitir que se defina um perfil de complexidade mínimo para as senhas de todos os usuários cadastrados na base de dados local, possibilitando a definição de número mínimo de letras minúsculas, letras maiúsculas, caracteres numéricos, caracteres especiais e etc;
A solução deve permitir a criação de política de bloqueio automático de usuários após uma quantidade de falhas de autenticação, assim evitando ataques de força bruta;
A solução deve suportar a criação de usuários em base local, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade;

A solução deve permitir a criação em massa de usuários na base de dados local através da importação de lista de usuários a serem criados contida em arquivos externos;
A solução deve permitir a criação de novos usuários na base de dados local e que o criador/administrador possa definir uma senha no momento de criação;
A solução deve permitir a criação de novos usuários na base de dados local sem a definição de senha, exigindo que o mesmo utilize o token como único fator de autenticação;
Deve permitir associar os tokens aos usuários criados localmente na base de dados;
Deve permitir que os próprios usuários façam o registro dos seus tokens e relatem a perda de um token automaticamente, sem necessidade de envolver um administrador;
Remoção automática em massa de usuários desabilitados, baseado em critérios definidos;
A solução deve possuir formas que permitam que os usuários locais possam fazer o reset de suas senhas de forma segura sem a intervenção de administradores, através de correio eletrônico ou pergunta de segurança;
Deve suportar a criação de grupos de usuários, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade;
Os tokens deverão gerar códigos com no mínimo 6 dígitos e intervalos não superiores à 60 segundos
Suportar autenticação em dois fatores por aplicativo mobile (iOS e Android);
Suportar autenticação em dois fatores por envio de mensagem SMS;
Suportar autenticação em dois fatores por envio de e-mail;
Deve permitir desabilitar um token quando este seja roubado ou extraviado, permitindo sua reativação posterior quando/se for recuperado (Celulares / Tablets e contas de e-mail);
Deve prover um portal web para o auto-registro dos usuários, de forma que o mesmo acesse, preencha os seus dados e submeta o registro. Após o usuário efetuar o registro, o administrador deverá ser notificado automaticamente para aprovar ou negar o cadastro do mesmo antes de que ele seja ativado;
A solução deve funcionar como servidor RADIUS (Remote Authentication Dial-In User Server), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;
A solução deve suportar a integração com servidor RADIUS remoto;
A solução pode funcionar como servidor LDAP (Lightweight Directory Access Protocol), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;
A solução deve suportar a integração com servidor LDAP remoto (como Microsoft Active Directory);
A solução deve suportar autenticação de usuários com credenciais de mídias sociais de terceiros como Facebook, Twitter, LinkedIn e Google+;
A solução deve permitir que usuários que não possuam uma conta local ou em mídias sociais se autentiquem através de um rápido cadastro, que garanta o mínimo de rastreabilidade, através da validação de endereços de e-mail ou número de telefone;
A solução deve permitir o login automático de usuários visitantes depois de se registrarem com sucesso;
A solução deve permitir configurar os parâmetros de rede (como as configurações de WiFi) em um endpoint baixando um script ou um executável através do portal de visitantes;

Deve suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Indentity Provider - IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider -SP);
Deve permitir integração com bases do Azure Directory e GSuite;
Por meio do SAML, deve permitir integrações com SPs variados, tais como Office 365;
Deve suportar FIDO;
A solução deve apontar a última vez (data) em que um token foi utilizado;
A solução deve suportar OpenID Connect (OIDC);
Deve suportar autenticação adaptativa;
Deve suportar regras granulares no processo de autenticação. Ex: usuários se autenticando na VPN precisam utilizar MFA, mas, o mesmo usuário, em portal web, não precise informar o token;
Deve suportar push notification;

CONTROLE BASEADO EM PORTA:
A solução deve suportar nativamente (sem redirecionamentos) a integração e autenticação de switches e outros dispositivos compatíveis com o padrão 802.1X;
Suportar os seguintes métodos 802.1X EAP: PEAP (MSCHAPv2), EAP-TTLS, EAP-TLS e EAP-GTC;
Suportar interoperabilidade com equipamentos de acesso (switches) de outros fabricantes, para autenticação de portas junto a solução, através dos padrões 802.1X;
Deve suportar bypass de autenticação 802.1X para dispositivos conhecidos que não suportem 802.1X, a liberação deverá ser feita baseada no endereço MAC dos equipamentos previamente cadastrados, estes terão acesso a rede sem necessidade de autenticação ou ação do usuário ou dispositivo.

CERTIFICADOS:
A solução deve atuar como Autoridade Certificadora (CA);
Deve permitir a administração de certificados digitais, com emissão e revogação;
Deve permitir o uso de CA's confiáveis para validação de certificados emitidos por CA's externas;
Deve suportar OCSP para que se possa fornecer uma lista de certificados revogados (CRL);
Deve prover repositório para autenticação de VPN Site-to-Site através de Certificados;
Deve suportar SCEP Server (Simple Certificate Enrollment Protocol), permitindo a assinatura de requisições de certificados digitais (CSR) automaticamente ou com interação do administrador;
Deve ser capaz de importar outros certificados de CA's assim como a lista de certificados revogados;
Deve ser capaz de permitir ao administrador do sistema gerar, assinar e revogar certificados digitais para os usuários;
Suportar ao protocolo ACME para geração de certificados.

SERVIÇO DE AUTENTICAÇÃO ÚNICA (SINGLE SIGN-ON)

A solução deve prover capacidade de serviço SSO (Single Sign-On), com autenticação transparente (passiva) de usuários em sistemas compatíveis
Deve ser capaz de integrar-se a um diretório ativo (Windows AD) e poder oferecer a funcionalidade se SSO, onde a autenticação automática/transparente via SSO para os serviços necessários é baseada na autenticação prévia feita pelo usuário no domínio
Deve permitir definir uma lista de usuários de SSO que serão ignorados, evitando assim interferência de contas de serviços tais como antivírus ou scripts via GPO
Deve suportar análise de arquivos syslog enviados de fonte remota, para uso pelo serviço de SSO
Deve suportar Security Assertion Markup Language (SAML), agindo como autenticador de um Provedor de Serviços (Service Provider - SP) solicitando informações de identidade de usuários a Provedores de Identidade (Indentity Providers - IDP's) de terceiros
Deve suportar SSO baseado em Radius (RSSO - RADIUS Single Sign-On)
Deve suportar RSSO Accounting Proxy permitindo a recepção de pacotes radius de accouting, a modificação destes pacotes e o encaminhamento dos mesmos para vários outros pontos

SEGUNDO FATOR DE AUTENTICAÇÃO PARA REDES PRIVADAS VIRTUAIS

Permitir o download gratuito do seu provisionamento.
Instalado no dispositivo móvel sem que haja a necessidade de alteração de sua configuração, ou mesmo a capacidade de formatar o dispositivo móvel de forma remota.
Garantir a privacidade do dispositivo móvel.
Deve requerer a permissão do proprietário para envio de notificações ou qualquer tipo de alteração nas configurações.
Deve suportar, no mínimo, as principais plataformas de mobile do mercado: iOS, Android e Windows
Suportar ativação através da utilização de QR Codes e manual.
Criptografar o armazenamento de sementes utilizadas na geração do token.
Ter a capacidade de proteger abertura do aplicativo através de PIN, Impressão Digital ou Face Security.
Suportar que a senha gerada possa ser copiada para a área de transferência.
Suportar detalhes de login enviados ao telefone para aprovação com um toque.
Suportar à sua utilização como segundo fator de autenticação para acesso VPN via SSL ou IPSEC, sem a necessidade de utilização de um servidor RADIUS.

1.11. PLATAFORMA DE ANÁLISE DE LOG CENTRALIZADO DA SOLUÇÃO

Plataforma composta por hardware e software, específico para analisar os logos coletados dos equipamentos firewall e plataforma de autenticação.
Deve ser totalmente compatível com os itens de fornecimento deste projeto.
Armazenamento interno mínimo de 24TB;
Deve possuir 8 baias para discos rígidos;
Formato para montagem em rack com altura máxima de 2Us;

Raid por Hardware;
Possui duas fontes redundantes do tipo hot swap;
Possui 2 portas de 2.5gbps RJ45 e 2 portas 25GbE SFP28
Alimentação 100-240Vac, 50~60Hz
Consumo Máximo aproximado de 302W
Possui 24 meses de garantia, sendo 3 meses garantia legal mais 21 meses garantia estendida.

1.12. **RACK 19”**

O Rack 19” deverá ser instalado nos Próprios e atender no mínimo as especificações abaixo:
Possuir 8U de altura, por 570mm de profundidade;
Deverá ser do tipo “Rack de parede”;
Possuir laterais e porta em aço;
Porta frontal com fechadura e acrílico cristal;
Acompanha uma calha de tomadas com 4 tomadas devidamente fixada ao rack;
Acompanha um organizador de cabos U cor preta com fechamento frontal devidamente fixada ao rack;
Acompanha um patch pannel de 24 portas categoria 6 devidamente fixada ao rack;
Pintura em cor preta.

Deverá ser previsto a fixação do Rack com no mínimo 4 parafusos e buchas metálicas especiais para suportar o peso do rack mais o peso dos equipamentos de fornecimento deste projeto, considerando 1 nobreak / 2 Switches / 2 organizadores de cabos / 2 patch pannels / Cabeamento Cat 6 / Cabos elétricos / conversores de fibra optica).

1.13. **NOBREAK**

O Nobreak deverá possuir as características técnicas mínimas:
Tensão nominal de entrada Bivolt Automático (115/127/220v);
Sistema senoidal por aproximação retangular PWM;
Frequência de entrada 60 Hz ±4;
Variação máxima: 89 a 140V (em rede 115V) e 175 a 260 (em rede 220V);
Plugue do cabo de força no padrão NBR14136;
Capacidade de Potência de Saída 1500VA;
Fator de potência 0,7;
Tensão nominal de saída bivolt com seleção manual 115/220v;
Frequência de saída 60hz ±4% (Para operação em bateria);
Permite carregar as baterias mesmo com pouca carga;
Conexões de Saída 8 tomadas padrão NBR14136;
Rendimento: até 96% (para operação rede);
Bateria interna: 2 baterias 12Vdc/7Ah;

Bateria externa opcional: até 80ah / 24vDC;
Dimensões aproximadas: (AxLxP) 233x140x386 / Peso Aproximado bruto: 12,5kg;
Possui 24 meses de garantia, sendo 3 meses garantia legal mais 21 meses garantia estendida.

1.14. INFRAESTRUTURA DE COMUNICAÇÃO LÓGICA COMPLETA

Toda infraestrutura a ser criada entre o rack de distribuição aos propagadores de sinal, deverão ser do tipo metálica, de 1 polegada, possuir proteção contra corrosão, devidamente fixada e dimensionado conforme norma ABNT vigente.

A disposição e fixação da infraestrutura seca, deverá ser efetuada da melhor forma possível, de forma organizada, para que fique visualmente harmoniosa e sem fios aparente durante toda sua extensão.

A infraestrutura necessária (tubulação metálica e acessórios) para passagem de cabos lógicos e/ou elétricos a ser criada, será de responsabilidade da CONTRATADA, dimensionada conforme normas técnicas e de segurança vigentes.

CARACTERÍSTICAS GERAIS

Os equipamentos deverão ser instalados conforme diretrizes do Departamento de Tecnologia da Informação.
Os equipamentos deverão ser instalados de forma cobrir a extensão principal do departamento contemplado com sinal de rede sem fio.

Na proposta apresentada, deverá ser previsto todos os serviços e materiais necessários para possibilitar a instalação e utilização dos equipamentos de fornecimento deste projeto.

O sistema de comunicação prevê a implantação de equipamentos e sistemas de acesso Wi-Fi que possibilite:
-Uma conexão mais confiável;
-Performance otimizada;
-Implementação simplificada e transparente;
-Minimizar as zonas de sombra dentro das unidades;
-Gerenciamento centralizado;

Para tingir o objetivo esperado, o sistema a ser ofertado, deverá permitir a conexão simultânea de grandes quantidades de equipamentos gerenciados de forma centralizada, permitindo uma comunicação estável nas localidades contempladas neste projeto.

Os equipamentos principais servidores, controladores e sistemas, deverão ser instalados no CPD Municipal sito no Departamento de Tecnologia da Informação – DTI, Rua Serafim Carloçs 571, Bairro São José, São Caetano do Sul – São Paulo.

Os controladores secundários e/ou switches de distribuição, devem ser instalados nos racks existentes ou em novos Racks que devem ser instalados em local estratégico que facilite a distribuição do cabeamento necessário.

Devem ser fornecidos e utilizados guias organizadores de cabos para os racks, etiquetas térmicas e outros materiais para a correta organização e identificação dos cabos, portas de rede e pontos de dados envolvidos neste projeto. A identificação deve seguir norma ABNT de identificação de cabeamento estruturado.

Para a interligação lógica entre os propagadores de sinal e os racks de ativos de rede, deverá ser previsto a correta conectorização e identificação.

Os propagadores de sinal, deverão ser instalados dentro das salas indicadas pela administração, preferencialmente nas paredes laterais, fixados por parafuso e bucha adequados.

A alimentação elétrica dos equipamentos se dará através de porta POE do switch a ser fornecido.

Os equipamentos conectados à rede wireless objeto de implantação deste edital, acessarão à internet através de link de acesso fornecido pela CONTRATANTE interligado à controladora a ser instalada no CPD Municipal, sendo de responsabilidade da contratada configurar VLANS, endereçamentos de IPS, roteamentos, ACLs e demais configurações necessárias, que devem ser definidas em conjunto coma equipe técnica do DTI.

A interligação logica (backbone e interconects) deverão ser criados com velocidade gigabit, devendo ser utilizado cabeamento e conectores categoria 6, devidamente homologada pela ANATEL, com suporte à POE, em lances máximos de 100(cem) metros.

O cabeamento categoria 6 a ser utilizado deverá possuía as características mínimas abaixo:
-Categoria 6;
- Cabeamento Estruturado para transmissão de voz, dados e imagens, segundo requisitos da norma - ANSI/TIA-568-C.2 Categoria 6;
-O cabo utilizado deverá possuir certificação Anatel;
-O cabo deve ser composto por condutores de cobre sólido 23 AWG;

-Capa externa em composto retardante à chama, com baixo nível de emissão de fumaça e livre de halogênios;
-Possuir impresso na capa externa nome do fabricante, marca do produto, e sistema de rastreabilidade que permita identificar a data de fabricação dos cabos.
-Deve suportar velocidade de 1Gbps em lances de 100 metros;

Deverão ser fornecidos todos equipamentos e licenças necessárias para implantação e funcionamento deste projeto.

Os equipamentos ofertados deverão pertencer a linha corporativa do fabricante, não sendo aceito equipamentos destinados ao uso doméstico.

Deverão ser novos, sem uso anterior, não remanufaturados e estar em linha de produção pelo fabricante no momento da entrega da proposta.

Na eventualidade do equipamento não estar mais em linha de produção no ato da entrega, a licitante deverá comunicar formalmente a equipe técnica que analisará as especificações do equipamento substituto em aderência ao solicitado em edital.

A licitante deverá trocar produtos defeituosos em garantia, em até 5 dias uteis após solicitação de reparo.

1.15. **SERVIÇO DE SUPORTE E MANUTENÇÃO PREVENTIVA**

A CONTRATADA, durante a vigência do contrato, deverá fornecer suporte técnico aos equipamentos e sistemas da solução sem fio ofertada de instalação neste projeto, com o objetivo de manter em perfeito funcionamento o sistema e atuar na resolução de problemas, reconfigurações, alterações de topologia, acompanhamento e melhoria de utilização da solução e ainda solucionar eventuais dúvidas operacionais e problemas que venham a ocorrer e/ou impeçam o uso de todos os equipamentos e softwares fornecidos e instalados. O legado é de responsabilidade da CONTRATANTE.

Fornecer toda assistência necessária à equipe de colaboradores da CONTRATANTE, sempre que acionada, para esclarecimentos de dúvidas e execução de ajustes nos equipamentos fornecidos pela mesma.

Realizar correções na solução ou execução de quaisquer medidas necessárias para solucionarem falhas de funcionamento e o restabelecimento da solução, dentro da sua responsabilidade.

O acionamento do suporte técnico da CONTRATADA poderá ser feito através das seguintes opções: telefônica (central de atendimento técnico) ou correio eletrônico (e-mail de suporte).

A CONTRATADA deverá possuir serviço de manutenção corretiva com atendimento 8x5, ou seja (oito) horas por dia, 5 (cinco) dias por semana.

A CONTRATADA deverá possuir Central de Atendimento para abertura dos chamados, comprometendo-se a manter registros dos mesmos constando a descrição do problema e solução aplicada.

Durante o prazo de garantia dos equipamentos, a parte ou peça defeituosa, deverá ser substituída sem ônus para o CONTRATANTE, salvo quando o defeito for provocado por uso inadequado, como quebra proposital, vandalismo ou alamentos provenientes de infiltrações no local de instalação do equipamento.

A CONTRATADA será responsável pelo atendimento de Nível 1, 2 e 3. Os Níveis de atendimento são qualificados da seguinte forma:

1° Nível:

Suporte realizado através de conexão remota, objetivando a verificação, o diagnóstico e correção de problema funcional do SISTEMAS, focando nos seguintes aspectos:

- Classes de alarme
- “Hardware” e “software”
- “Backup” do sistema
- Aplicativos do Sistema
- Falhas relatadas pelo cliente
- Corrigir configurações diversas

2° Nível:

Suporte On-Site

Este serviço deve ser prestado localmente, através de profissionais técnicos qualificados. Este serviço será responsável por prestar suporte ao cliente em atividades de manutenção corretiva,

atendimentos em situações emergenciais, interrupções ou funcionamento inadequado dos sistemas, tendo como objetivo principal obter um serviço de suporte técnico presencial que garanta ou reestabeleça a operacionalidade e o bom desempenho dos equipamentos e ambientes envolvidos no contrato, bem como uma resposta rápida e emergencial às solicitações do cliente para os problemas identificados.

Atividades relacionadas ao Suporte On-Site:

- Corrigir configurações diversas;
- Atualizar software devido a falhas reconhecidas como bugs;
- Efetuar a troca de hardware devido a falhas e solicitar à troca ao fabricante dentro do período de garantia;

3° Nível:

Caso o problema não seja solucionado de acordo com os Níveis 1 e 2.

O atendimento será realizado pela equipe de profissionais especializados do Centro de Competência da CONTRATADA e se necessário com o acionamento do fabricante das soluções instaladas.

Quadro de SLA da CONTRATADA:

Classificação	**Tempo Máximo para Atendimento**
Alta	12 horas
Moderada	18 horas
Baixa	1 dia útil.

Alta: Problemas que prejudicam a operação da infraestrutura de rede/sistemas que a tornem inoperante.

Moderada: Problemas ou dúvidas que criam algumas restrições à operação da solução.

Baixa: Solicitações que não afetem o uso do sistema de forma imediata.

SLA – SERVICE LEVEL AGREEMENT

O ANS – Acordo de Níveis Serviço define as principais metas e responsabilidades da CONTRATADA no atendimento de chamados técnicos na execução e manutenção das redes de fibra óptica e de cabeamento estruturado;

Os chamados técnicos abertos serão classificados por grau de severidade, sendo que as Garantias Acessórias da Solução devem ser executadas dentro dos padrões mínimos de atendimento:

Severidade 1 (S1): o equipamento, acessório ou periférico apresenta pane, falha ou não conformidade técnica que o torna acima de 50% inoperante. O primeiro retorno telefônico da CONTRATADA deve ser realizado em no máximo 01 hora e a solução técnica, definitiva ou de contorno, não poderá exceder a 12 horas, contadas do chamado técnico;

Severidade 2 (S2): o equipamento, acessório, ou periférico apresenta pane, falha ou não-conformidade técnica que degrade a qualidade, prejudica a operação e o uso ou acesso de funções básicas. O primeiro retorno telefônico da CONTRATADA deve ser realizado em no máximo 02 horas e a solução técnica, definitiva ou de contorno, não poderá exceder a 18 horas, contadas do chamado técnico;

Severidade 3 (S3): o equipamento, acessório, ou periférico apresenta pane, falha ou não conformidade técnica que não afetem o rendimento do serviço. O primeiro retorno telefônico da CONTRATADA deve ser realizado em no máximo 02 horas e a solução técnica, definitiva ou de contorno, não poderá exceder a 24 horas, contadas do chamado técnico.

O serviço de manutenção descritos neste documento, serão faturados mensalmente conforme peso de importância do suporte em relação ao equipamento e cada peso com relação à quantidade de equipamentos efetivamente instalados neste projeto, conforme tabela a seguir:

DESCRIÇÃO	QTD	PESO PERCENTUAL DO SERVIÇO DE MANUTENÇÃO E SUPORTE
Firewall de alta capacidade Tipo I	2	30%
Propagador de sinal sem fio Tipo I (indoor)	400	20%
Propagador de sinal sem fio Tipo II (outdoor)	30	5%
Switch Gerenciável Tipo I	200	5%
Plataforma de autenticação e gerenciamento da Solução de Segurança	1	15%
Plataforma de Análise de Log Centralizado da Solução de Segurança	1	15%
Rack 19" 8Us	123	0%

Nobreak Tipo I - 1500VA	123	5%
Infraestrutura de comunicação lógica completa	8600	5%
		100%

CLÁUSULA SEGUNDA – DAS CONDIÇÕES DE ENTREGA DO OBJETO

2.1. A Autorização de Fornecimento será encaminhada por quaisquer meios de comunicação que possibilitem a comprovação do respectivo recebimento por parte da Detentora, inclusive correio eletrônico.

2.2. O fornecimento deverá ser realizado de acordo com as especificações técnicas constantes do edital, na forma prevista na proposta, naquilo que não o contrariar, dentro dos prazos estabelecidos sob pena de a(s) futura(s) Detentora (s) incorrer(em) nas sanções previstas neste Edital.

2.3. Os equipamentos deverão ser entregues e instalados, no endereço constante da Autorização de Fornecimento, conforme **ANEXO IA - Endereços da Prestação dos Serviços,** de segundas às sextas-feiras, no prazo de até 30 (trinta) dias corridos, contados a partir do recebimento da mesma.

2.3.1. Qualquer alteração de local de entrega será previamente informada à Detentora.

2.4. Os equipamentos serão solicitados sob demanda, conforme necessidades e disponibilidade orçamentária.

2.5. Todas as despesas decorrentes de carga, descarga, transporte ocorrerão por conta da empresa Detentora.

2.6. O material deve ser entregue em sua embalagem original, sem estar violada ou fracionada e em condições de transporte e acondicionamento indicados pelo fabricante.

2.7. No momento do recebimento, haverá avaliação para aferir conformidade com o solicitado.

2.8. Ao apresentar qualquer irregularidade na qualidade do produto, a Unidade requisitante entrará em contato com o fornecedor para que faça a troca do produto.

2.9. Todos os equipamentos fornecidos pela Detentora, deverão ter garantia de 24 (vinte e quatro) meses.

2.10. As garantias solicitadas terão início a partir da data de emissão da Nota Fiscal de entrega dos equipamentos.

CLÁUSULA TERCEIRA - DA VIGÊNCIA

3.1. O prazo de vigência da presente Ata de Registro de Preços será de 12 (doze) meses, contados a partir da assinatura do instrumento contratual, podendo ser prorrogado, a critério das partes, nos termos do artigo 84 da Lei Federal nº 14.133/21.

3.1.1. Na hipótese de prorrogação da vigência da Ata de Registro de Preços, as quantidades inicialmente registradas serão renovadas, na sua totalidade, independentemente do quantitativo utilizado no período de vigência, não sendo possível cumular com as quantidades não utilizadas.

CLÁUSULA QUARTA – RECURSOS, PAGAMENTO, REAJUSTE CONTRATUAL E ALTERAÇÕES.

4.1. As despesas com a execução do presente onerarão as dotações orçamentárias de n.º: **02.24.03.04.126.0170.2.063.3.3.90.30.00; 02.24.03.04.126.0170.2.063.3.3.90.39.00; 02.24.03.04.126.0170.2.063.4.4.90.52.00 - VERBAS DO TESOURO MUNICIPAL.**

4.2. Os pagamentos serão efetivados em 30 dias contados da data em que for atestado o fornecimento dos materiais ou a prestação de serviços. A atestação será efetuada no prazo máximo de 5 dias úteis após apresentação da Nota Fiscal/Fatura, a qual deverá ser aprovada, conferida e assinada pelo Setor Requisitante e encaminhada posteriormente, à Seção de Contabilidade para lançamento e demais providências, na conta bancária da **Detentora**, **Banco _____, agência n.º _____, conta n.º_____.**

4.2.1. Somente haverá a liberação, pela Secretaria Municipal da Fazenda, do pagamento devido à Detentora, quando da apresentação, pela Unidade Requisitante, de certidão devidamente assinada pelo secretário, conforme disposições contidas na Portaria nº 18.279, de 06 de janeiro de 2005.

4.3. Havendo divergência ou erro na emissão do documento fiscal, fica interrompido o prazo para o pagamento, sendo iniciada a nova contagem somente após a regularização dessa documentação.

4.3.1. A pessoa jurídica pode possuir vários estabelecimentos comerciais que são partes integrantes de uma mesma empresa. Contudo, para fins de execução do contrato, a emissão das notas fiscais deve sempre considerar o estabelecimento que efetivamente executou o contrato, não sendo lícito adotar conduta distinta a esta.

4.4. Ocorrendo atraso injustificado na liberação do pagamento, a Contratante poderá ser penalizada com multa de mora correspondente a 0,01% (um centésimo de percentual), do valor a ser pago, por dia de atraso até seu efetivo pagamento.

4.5. Ocorrendo atraso na liberação do pagamento por motivo injustificado, a Contratante poderá ser feita a atualização monetária, calculada pelo IPCA, aplicada sobre os valores da parcela devida, por dia de atraso até seu efetivo pagamento.

4.6. Não será efetuado qualquer pagamento à Contratada enquanto houver pendência de liquidação da obrigação financeira em virtude de penalidade ou inadimplência contratual.

4.7. Ocorrendo atraso na liberação por motivo injustificado, poderá ser feita a atualização monetária, calculada pelo IPCA, aplicada sobre os valores da parcela devida, por dia de atraso até seu efetivo pagamento.

4.8. Não será efetuado qualquer pagamento à Detentora enquanto houver pendência de liquidação da obrigação financeira em virtude de penalidade ou inadimplência contratual.

4.9. Os pagamentos serão efetuados através de ordem de pagamento bancário para qual deverão constar os dados bancários no corpo da nota fiscal.

4.10. Os pagamentos ficarão condicionados à apresentação pela Detentora dos seguintes documentos, devidamente atualizados:

4.10.1. Certidão negativa de débitos referente a todos os tributos federais e à Dívida Ativa da União por elas administrados, abrangendo inclusive as contribuições sociais previstas nas alíneas ‘a’ a ‘d’ do parágrafo único do art. 11 da Lei nº 8.212, de 24 de julho de 1991;

4.10.2. Certificado de regularidade de situação perante o Fundo de Garantia do Tempo de Serviço – FGTS;

4.10.3. Prova da regularidade para com o Cadastro de Informativo Municipal – CADIN Municipal.

4.10.4. Certidão negativa de débitos trabalhista – CNDT

4.10.5. Certidão negativa de débitos tributários mobiliários expedida pela Secretaria Municipal da Fazenda do Município de São Caetano do sul OU caso a empresa não seja inscrita no Cadastro de Contribuintes Mobiliários do Município de São Caetano do Sul, deverá apresentar declaração, firmada por seu representante legal, sob as penas da lei, de que não é cadastrada e de que nada deve a esta Municipalidade relativamente aos tributos relacionados com a prestação licitada.

4.11. Os preços serão fixos e irreajustáveis nos termos da Lei Federal 10.192/2001, sendo que na hipótese de prorrogação contratual, após o período de 12 (doze) meses, os preços poderão ser reajustados com base no índice do IPCA, ou outro índice que vier a substituí-lo, mediante requerimento da Detentora, quando da eventual prorrogação da Ata de Registro de Preços.

4.11.1. A data-base a ser considerada para o reajustamento dos preços será a data de apresentação da proposta comercial.

4.12. Eventuais alterações contratuais serão regidas pela Lei Federal nº 14.133/202, bem como por normas regulamentadoras.

4.13. O procedimento de recomposição do equilíbrio econômico-financeiro disposto na alínea “d” do inciso II, do artigo 124 da Lei Federal nº 14.133/2021 poderá ser iniciado por requerimento da CONTRATADA/DETENTORA ou por determinação da CONTRATANTE.

4.14. O procedimento de recomposição do equilíbrio econômico-financeiro disposto na alínea “d” do inciso II do artigo 24 da Lei 14.133/21 poderá ser iniciado por requerimento da Detentora ou por determinação do CONTRATANTE.

4.14.1. Quando o pedido for iniciado por requerimento da Detentora, o pedido deverá ser devidamente fundamentado, e estar acompanhado de todos os documentos necessários à demonstração do cabimento do pleito.

4.14.2. O pedido de recomposição do equilíbrio econômico-financeiro deverá ser formulado durante a vigência do contrato.

4.14.3. Recebida a notificação sobre o evento de desequilíbrio, a CONTRATANTE terá 30 (trinta) dias, prorrogáveis mediante justificativa apresentada por escrito neste prazo, para apresentar resposta ao pedido de recomposição do equilíbrio econômico-financeiro do CONTRATO.

4.15. A Detentora fica obrigada a aceitar, nas mesmas condições contratadas, os acréscimos ou supressões que se fizerem necessários no objeto, a critério exclusivo do CONTRATANTE, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

4.16. Eventual alteração será obrigatoriamente formalizada pela celebração de prévio termo aditivo ao presente instrumento, respeitadas as disposições da Lei Federal nº 14.133/21.

CLÁUSULA QUINTA – OBRIGAÇÕES DA DETENTORA:

5.1. Fornecer os produtos na quantidade e prazos estabelecidos no Edital, de acordo com as especificações técnicas constantes neste instrumento.

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

5.3. Compromete-se a fornecer os produtos na forma de sua apresentação na proposta, comprovando a marca, validade, procedência e demais características dos produtos, os quais serão conferidos pela Contratante;

5.4. Substituir, no local de entrega e no prazo ajustado, após notificação, o serviço recusado.

5.5. Todas as despesas decorrentes de seguros, transporte, tributos, embalagem, correrão por conta exclusiva da empresa Detentora.

5.6. A Detentora está obrigada a aceitar nas mesmas condições contratuais os acréscimos e supressões até 25% do valor inicial atualizado do contrato ou da nota de empenho.

5.7. Comunicar à Contratante toda e qualquer irregularidade ocorrida ou observada durante o fornecimento dos materiais.

5.8. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à Administração.

5.9. Obedecer às normas e rotinas da CONTRATANTE em especial as que disserem respeito à proteção de dados pessoais, à segurança, à guarda, à manutenção e a integridade das informações coletadas, custodiadas, produzidas, recebidas, classificadas, utilizadas, acessadas, reproduzidas, transmitidas, processadas arquivadas eliminadas ou avaliadas durante a execução do objeto a que se refere a Cláusula Primeira deste Contrato, observando as normas legais e regulamentares aplicáveis.

5.10. Atender às determinações da fiscalização do Gestor do Contrato e providenciar a imediata correção das deficiências apontadas pela fiscalização quanto a entrega dos produtos.

5.11. A Detentora deverá cumprir a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, nos termos do art. 116 da lei 14.133/2021.

5.12. Nomear preposto para representá-la na execução deste contrato durante o período de vigência.

5.13. Manter, durante a vigência do contrato, as condições de habilitação exigidas na licitação, devendo comunicar a contratante a superveniência de fato impeditivo da manutenção dessas condições.

5.14. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto deste contrato em que se verificarem vícios, defeitos ou incorreções, e terão o prazo de 48 horas para substituir o material rejeitado.

5.15. Comunicar à Contratante, no prazo máximo de 48 (quarenta e oito) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.

5.16. Comunicar à Contratante toda e qualquer irregularidade ocorrida ou observada durante a entrega do material.

5.17. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão, dentre outras, as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade.

5.18. Orientar tecnicamente os responsáveis pela operação dos bens, fornecendo os esclarecimentos necessários ao seu perfeito funcionamento.

5.19. Proceder a entrega dos bens, devidamente embalados, de forma a não serem danificados durante a operação de transporte e de carga e descarga, assinalando na embalagem a marca, destino e, quando for o caso, número da Licença de Importação ou documento equivalente, com as especificações detalhadas ou documento equivalente, para conferência.

5.20. Realizar testes e corrigir defeitos nos bens, inclusive com a sua substituição quando necessário, sem ônus para a CONTRATANTE, durante o período de garantia. A troca de produtos defeituosos deverá ser em até 5 dias uteis.

5.21. Responder por todos os ônus referentes a entrega dos bens ora contratados, desde os salários dos seus empregados, como também os encargos trabalhistas, previdenciários, fiscais e comerciais, que venham a incidir sobre o Contrato.

5.22. A Detentora deverá designar profissional qualificado que atuará como gerente de projeto, coordenando os demais profissionais envolvidos na execução do objeto, garantindo a sintonia das diversas atividades e o bom andamento do cronograma de trabalho.

5.23. O gerente de projeto também será o ponto de contato com os representantes do Município, para os quais reportará as atividades, fatos e eventuais dificuldades que deverão ser comunicadas ao gestor do contrato.

5.24. Entregar os bens no local indicado pela CONTRATANTE.

5.25. Responsabilizar-se:

5.26. a) Por quaisquer acidentes na entrega dos bens.

5.27. b) Pelo pagamento de seguros, impostos, taxas e serviços, encargos sociais e trabalhistas, e quaisquer despesas referentes aos bens.

5.28. Executar o objeto em conformidade com as condições deste instrumento.

5.29. Responsabilizar-se pelos danos causados diretamente a CONTRATANTE ou a terceiros, decorrentes da sua culpa ou dolo, quando da execução do objeto, não podendo ser arguido para efeito de exclusão ou redução de sua responsabilidade o fato de a CONTRATANTE proceder a fiscalização ou acompanhar a execução contratual.

5.30. Responder por todas as despesas diretas e indiretas que incidam ou venham a incidir sobre a execução do contrato, inclusive as obrigações relativas a salários, previdência social, impostos, encargos sociais e outras providencias, respondendo obrigatoriamente pelo fiel cumprimento das leis trabalhistas e especificas de acidentes do trabalho e legislação correlata, aplicáveis ao pessoal empregado na execução contratual.

5.31. Prestar imediatamente as informações e os esclarecimentos que venham a ser solicitados pela CONTRATANTE, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidas no prazo de 24 (vinte e quatro) horas.

5.32. Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta comercial, observando o prazo mínimo exigido pela Administração.

5.33. Providenciar a substituição de qualquer profissional envolvido na execução do objeto contratual, cuja conduta seja considerada indesejável pela fiscalização da CONTRATANTE.

5.34. A equipe de trabalho da contratada, deverá orientar a equipe de funcionários municipais sempre que necessário, no que tange operação, funcionalidades e configurações do sistema contratado, sem custos à CONTRATANTE.

CLÁUSULA SEXTA – OBRIGAÇÕES DA CONTRATANTE:

6.1. Cumprir o prazo fixado para realização do pagamento;

6.2. Indicar o funcionário responsável pelo acompanhamento do instrumento contratual;

6.3. Comunicar à Detentora sobre quaisquer irregularidades dos produtos entregues;

6.4. Fiscalizar o fornecimento dos materiais, zelando pelo fiel cumprimento do presente contrato, promovendo seu recebimento, conferindo a qualidade, especificação exigida dos mesmos, assim como os preços apresentados;

6.5. Prestar as informações e os esclarecimentos que venham a ser solicitados pelo Fornecedor Contratado, durante o prazo vigente do Contrato;

6.6. Receber o objeto no dia previamente agendado, no horário de funcionamento da unidade responsável pelo recebimento.

6.7. Solicitar o reparo ou a substituição do objeto em que se verificarem vícios, defeitos ou incorreções.

6.8. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes deste Termo de Referência e da proposta, para fins de aceitação e recebimento definitivos.

6.9. Proporcionar a Detentora todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do objeto contratual.

6.10. Designar um funcionário como gestor do contrato e que servirá de contato junto à CONTRATADA para gestão, acompanhamento e esclarecimentos que porventura se fizerem necessários durante a vigência contratual.

6.11. Comunicar à Detentora, toda e qualquer orientação acerca dos serviços, excetuados os entendimentos orais determinados pela urgência, que deverão ser confirmados, por escrito, no prazo de 1 (um) dia útil.

6.12. Fornecer e colocar à disposição da Detentora todos os elementos e informações que se fizerem necessários à execução dos serviços.

6.13. Acompanhar, fiscalizar e auditar a execução dos serviços prestados, nos aspectos técnicos, de segurança, de confiabilidade e quaisquer outros de seu interesse, através de pessoal próprio ou de terceiros designados para este fim.

6.14. A CONTRATANTE deverá assegurar acesso aos técnicos credenciados pela CONTRATADA, a todos equipamentos para a execução dos serviços de manutenção, prestando os esclarecimentos que eventualmente venham a ser solicitados.

6.15. A CONTRATANTE deverá designar um funcionário responsável, que acompanhará o pessoal técnico da CONTRATADA em todas as visitas, para a comprovação de eventuais irregularidades.

6.16. Caso a CONTRATANTE substitua o funcionário responsável pelo atendimento, deverá informar por escrito à Detentora.

6.17. É expressamente vedado à CONTRATANTE em qualquer hipótese, utilizar-se de serviços de terceiros ou próprio, para intervir no conserto, alteração do equipamento ou acessórios sem prévia e expressa autorização da Detentora.

6.18. Notificar, formal e tempestivamente, a Detentora sobre as irregularidades observadas no cumprimento do contrato.

6.19. Efetuar os pagamentos devidos a Detentora nas condições estabelecidas neste Termo.

6.20. Aplicar as penalidades previstas em lei e neste instrumento.

CLÁUSULA SÉTIMA – SANÇÕES E RESCISÃO:

7.1. A recusa injustificada da adjudicatária em assinar o contrato, aceitar ou retirar o instrumento equivalente, dentro do prazo estabelecido caracteriza o descumprimento total da obrigação assumida, sujeitando-o a juízo da Administração, nos termos da legislação municipal à multa de 20% (vinte por cento) sobre o valor da obrigação não cumprida.

7.2. Poderão ainda ser aplicadas as seguintes sanções, em razão da execução:

7.2.1. Multa por atraso: 1% (um por cento) por dia sobre o valor da parcela em atraso, até o limite de 10% (dez por cento), podendo a Prefeitura a partir do 10º dia considerar rescindido o Contrato, sem

prejuízo das demais sanções cabíveis.

7.2.1.1. O prazo para pagamento das multas moratórias será de 3 (três) dias úteis a contar da intimação da Detentora. A critério da Administração, e sendo possível, o valor das referidas multas será descontado dos pagamentos eventualmente devidos à PMSCS, garantida a ampla defesa nos termos da Lei.

7.3. Pela inexecução total do contrato, será aplicada à Detentora a multa de 20% (vinte por cento) sobre o valor total do ajuste.

7.4. Pela inexecução parcial do contrato será aplicada à Detentora a multa de até 10% (dez por cento) sobre o valor da obrigação não cumprida.

7.5. Multa de 10% (dez por cento), por descumprimento de quaisquer das obrigações decorrentes do ajuste que não estejam previstas nos subitens acima, a qual incidirá sobre o valor total do Contrato.

7.6. Além das multas acima, a Administração poderá, ainda, impor as seguintes penalidades:

7.6.1. Advertência;

7.6.2. Suspensão temporária do direito de licitar e impedimento de contratar com o Município de São Caetano do Sul, pelo prazo de até dois anos;

7.6.3. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação.

7.7. Se a licitante deixar de entregar a documentação ou apresentá-la falsamente, enseja o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará pelo prazo de até 05 (cinco) anos, impedida de contratar com a Administração Pública, sem prejuízo das multas previstas no Edital e demais cominações legais.

7.8. As penalidades são independentes e a aplicação de uma não exclui a das outras, quando cabíveis.

7.9. Constatada a inexecução contratual ou a hipótese do item 7.1, será a Detentora intimada da intenção da PMSCS quanto à aplicação da penalidade, concedendo-se prazo para interposição de defesa prévia, nos termos do art. 155 a 163 da Lei Federal nº 14.133/21.

7.10. Não sendo apresentada a defesa prévia pela Detentora ou havendo o indeferimento da mesma quando interposta, a Prefeitura providenciará a notificação da Detentora quanto à aplicação da penalidade, abrindo-se prazo para interposição de recurso administrativo, nos termos do artigo 166 da Lei Federal nº 14.133/21.

7.10.1. Decorridas as fases anteriores, o prazo para pagamento das multas será de 3 (três) dias úteis a contar da intimação da Detentora. A critério da Administração, e sendo possível, o valor devido será descontado da garantia prestada ou, sendo esta insuficiente, será descontado dos pagamentos eventualmente devidos à Administração. Não havendo prestação de garantia, o valor das multas será diretamente descontado do crédito que porventura haja.

7.11. Se a Contratante decidir pela não aplicação da multa, o valor retido será devolvido à Detentora.

7.12. É assegurado nos termos legais os prazos para o exercício do direito da ampla defesa e do contraditório, na aplicação das sanções.

7.13. A falsidade das declarações prestadas, objetivando os benefícios da LC 123/06, devidamente atualizada, caracterizará o crime de que trata o art. 299 do Código Penal, sem prejuízo do enquadramento em outras figuras penais e da sanção prevista de impedimento de licitar e contratar com a Administração do Município de São Caetano do Sul.

7.14. O prazo para pagamento das multas será de 05 (cinco) dias úteis a contar da intimação da empresa apenada. A critério da Administração e sendo possível, o valor devido será descontado da importância que a empresa tenha a receber da PMSCS. Não havendo pagamento, o valor será inscrito como dívida ativa, sujeitando a devedora a processo executivo.

7.15. Constituirão motivos para extinção do contrato, assegurados o contraditório e a ampla defesa, as situações previstas no artigo 137 da Lei 14.133/21.

7.16. A extinção do contrato, observando o disposto nos artigos 138 e 139 da Lei 14.133/21, poderá ser:

I - Determinada por ato unilateral e escrito da Administração, exceto no caso de descumprimento decorrente de sua própria conduta;

II - Consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração;

III - Determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso

arbitral, ou por decisão judicial.

7.17. A CONTRATANTE terá a opção de extinguir o contrato, sem ônus, quando não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

7.18. A Detentora se sujeita às sanções previstas nos artigos 156 da Lei Federal 14.133/21, nos termos previstos no instrumento editalício.

7.19. A aplicação de uma das sanções não implica na exclusão de outras previstas na legislação vigente.

7.20. O pagamento de multas não exime a Detentora da reparação de eventuais danos, perdas ou prejuízos que seu ato punível venha a acarretar à CONTRATANTE.

7.21. As multas deverão ser recolhidas no prazo de 10 (dez) dias corridos, a contar da data do recebimento da comunicação enviada por esta Administração.

7.22. Os valores relacionados a multas poderão ser deduzidos, até seu valor total, de quaisquer pagamentos devidos à Detentora, mesmo que referentes a outras avenças, ou deduzidas de eventual garantia de contrato. Poderão, alternativamente, ser inscritas em Dívida Ativa para cobrança executiva ou cobradas judicialmente.

7.23. As decisões relacionadas a multas, penalidades e advertências, bem como as notificações dessas decisões, serão publicadas em Diário Oficial do Município e encaminhadas via correios para as empresas sancionadas, garantindo o direito de ampla defesa, a contar da confirmação de recebimento da decisão.

CLÁUSULA OITAVA – DISPOSIÇÕES GERAIS:

8.1. Considera-se parte integrante deste ajuste, como se nele estivessem transcritos, o Edital do Pregão nº __/2026 com seus Anexos e a Proposta Comercial, constantes no Processo Administrativo nº 3548807.425.00007034/2025-90.

8.1.1 A existência de preços registrados **não obriga** a PMSCS a firmar as contratações que deles poderão advir.

8.2. O não comparecimento da DETENTORA, no prazo assinalado, para assinar o contrato ou instrumento equivalente, quando cabível, sem motivo justo e aceito pela Unidade, caracterizará negativa do fornecimento, sujeitando a DETENTORA à penalidade prevista na cláusula 7.1. deste instrumento.

CLÁUSULA NONA – GESTOR CONTRATO

9.1. O gestor da presente contratação será o servidor indicado e, na sua ausência, a Secretária Municipal de Gestão e Governo Digital, nos termos do Decreto Municipal nº 12.176/2025 e Portaria nº 44.004/2026, o qual será responsável pelo acompanhamento e fiscalização da execução do termo contratual objeto do presente certame, procedendo ao registro das ocorrências e adotando as providências necessárias ao fiel cumprimento do ajuste, bem como, responsabilizar-se á pela vigência, com o consequente controle dos prazos de início e término contratual, aditamentos e instauração de novo processo de licitação, caso seja deliberado pela continuidade dos serviços ou fornecimento.

9.2. Compreenderá na fiscalização aludida no item anterior, a atestação e aprovação dos serviços prestados, de que os mesmos atendem as especificações e finalidades contratuais, de forma a ser concretizado o acompanhamento.

9.3. O Gestor responderá administrativamente, civil e penalmente pelo cumprimento do contrato ou instrumento equivalente, quando verificado a não observância dos requisitos acima causando prejuízo à Administração ou comprometimento das atividades procedimentais.

CLÁUSULA DÉCIMA – FORO:

10.1. O foro competente para dirimir qualquer dúvida ou ação decorrente do presente Contrato é o foro da Comarca de São Caetano do Sul, com renúncia expressa de qualquer outro, por mais privilegiado que seja.

Nada mais havendo a ser declarado, vai assinada pelas partes e testemunhas a tudo presente e de tudo cientes, para que produza os regulares efeitos de Lei e de Direito.

São Caetano do Sul, __ de _____ de 2026.

PMSCS

DETENTORA

ANEXO VIIA

ENDEREÇOS DA PRESTAÇÃO DOS SERVIÇOS

LOCAIS DE INSTALAÇÃO DOS EQUIPAMENTOS.

Os equipamentos poderão ser instalados nos seguintes endereços relacionados abaixo, visto que as quantidades serão definidas conforme necessidade de cobertura de rede sem fio em cada localidade bem como disponibilidade orçamentária de cada departamento.

Os equipamentos Enterprise (firewall, plataforma de autenticação e plataforma de análise de log) serão instalados do Rack de equipamento existente no Departamento de Tecnologia da Informação, situado na Rua Serafim Carlos, 571, Bairro São José, São Caetano do Sul.

Possíveis endereços de instalação dos equipamentos:

ENDEREÇO	BAIRRO
AL CASSAQUERA 00227	BARCELONA
AL JOAO GALEGO 00001	SANTA MARIA
AL PORTO ALEGRE,CDE 00800	STA MARIA
AL PORTO ALEGRE,CDE 00820	STA MARIA
AL PORTO ALEGRE,CDE 01540	STA MARIA
AV ANTONIO PRADO,CONS 00000	CENTRO
AV ANTONIO PRADO,CONS 00250	CENTRO
AV ANTONIO PRADO,CONS 00307	CENTRO
AV AUGUSTO DE TOLEDO,DR 00000	OSWALDO CRUZ
AV AUGUSTO DE TOLEDO,DR 00195	SANTA PAULA
AV AUGUSTO DE TOLEDO,DR 00255	SANTA PAULA
AV AUGUSTO DE TOLEDO,DR 00350	SANTA PAULA
AV FERNANDO SIMONSEN 00130	SANTA PAULA
AV FERNANDO SIMONSEN 00160	CERAMICA
AV FERNANDO SIMONSEN 00566	CERAMICA
AV GOIAS 00340	CERAMICA
AV GOIAS 00600AN 3	BARCELONA
AV GOIAS 00950	BARCELONA
AV GOIAS 02000	BARCELONA
AV GOIAS 02101	BARCELONA
AV GOIAS 03400	BARCELONA
AV GUIDO ALIBERTI 00020	BARCELONA
AV GUIDO ALIBERTI 01610	BARCELONA

AV GUIDO ALIBERTI 01651	CENTRO
AV JOAO XXIII,PAPA 00601	CENTRO
AV KENNEDY,PRES 02100	CENTRO
AV KENNEDY,PRES 02300	JD S CAETANO
AV KENNEDY,PRES 02400	BOA VISTA
AV LIBERO BADARO 00000	BOA VISTA
AV PARAISO 00600	BOA VISTA
AV PARAISO 00831	JD S CAETANO
AV PARANAPANEMA 00670	OLIMPICO
AV PROSPERIDADE 00441	OLIMPICO
AV PROSPERIDADE 00671	NOVA GERTY
AV ROBERTO SIMONSEN,SEN 00282+AN 1	PROSPERIDADE
AV RODRIGUES ALVES,DR 00093+	PROSPERIDADE
AV TIETE 00301	CENTRO
AV TIJUCUSSU 00800	FUNDACAO
AV VITAL BRASIL FILHO 00300	NOVA GERTY
AV VITAL BRASIL FILHO 00361	OLIMPICO
AV VITAL BRASIL FILHO 00600+ESCOLA SYLVIOROMERO	OSVALDO CRUZ
AV WALTER THOME 00064	OSVALDO CRUZ
ETRLAGRIMAS 00320	OSVALDO CRUZ
ETRLAGRIMAS 00515	OSVALDO CRUZ
ETRLAGRIMAS 00579	OSVALDO CRUZ
ETRLAGRIMAS 01165	OLIMPICO
ETRLAGRIMAS 01630	MAUA
ETRLAGRIMAS 01656	MAUA
PCABADEN POWELL 00001	MAUA
R ALEGRE 00497	MAUA
R ANGELO APARECIDO RADIM 00090+GUARITA GCMS	MAUA
R ANTONIO BENTO 00140	MAUA
R ANTONIO BENTO 00180	CENTRO
R ANTONIO JOAO,TTE 00413	SANTA PAULA
R ANTONIO,STO 00050+FARMACIA POP GOV	SAO JOSE
R ANTONIO,STO 00117	SANTA PAULA
R ARARAQUARA 00063	SANTA PAULA
R ARLINDO MARCHETTI 00508	SANTA PAULA
R ARMANDO DE A PEREIRA,ENG 00000	CERAMICA
R ARMANDO DE A PEREIRA,ENG 00120	CENTRO

R ARMANDO DE A PEREIRA,ENG 01470	CENTRO
R ARNALDO SANTE LOCOSELLI 00158	FUNDACAO
R AURELIA 00257	SANTA MARIA
R AURELIA 00257+HOSP EMERG ALBERT S	CERAMICA
R BELL ALLIANCE 00000+ESQ R WINSTON CHUR	CERAMICA
R BELL ALLIANCE 00225	CERAMICA
R BERILOS 00113	CERAMICA
R BERTOLINO CUNHA 00100	STA PAULA
R BOA VISTA 00150	STA PAULA
R BOA VISTA 00200	STA PAULA
R BUSCH 00042FR	JD S CAETANO
R CAMISAO,CEL 00320	JD SAO CAETANO
R CAPIVARI 00500	PROSPERIDADE
R CAPIVARI 00624	OSWALDO CRUZ
R CARLO DEL PRETE,MAJ 00651	BOA VISTA
R CASEMIRO DE ABREU 00560	BOA VISTA
R CASTORES 00060	NOVA GERTI
R CEARA 00509+CRE FUDA??O	OSWALDO CRUZ
R CLOVIS BEVILACQUA 00075	NOVA GERTY
R CORAL 00155	NOVA GERTY
R DEODORO,MAL 00000+FRENTE TRAV PEDESTR	CENTRO
R DEODORO,MAL 00300	CENTRO
R DEODORO,MAL 00445	CENTRO
R DEODORO,MAL 00830	CERAMICA
R DEODORO,MAL 01111	MAUA
R DESIREE MALATEAUX 00129	FUNDACAO
R DIONIZIO MERCADO 00199	CERAMICA
R DOMENICO BOTAN 00091	PROSPERIDADE
R DURVAL VILALVA,DR 00135	STA PAULA
R EDUARDO PRADO 00000	SANTA PAULA
R EDUARDO PRADO 00001	SANTA PAULA
R EDUARDO PRADO 00201	SANTA PAULA
R ERNESTO GIULIANO,CAV 00849+ESCOLA ANACLETO C	SANTA PAULA
R ERNESTO GIULIANO,CAV 01050	MAUA
R ERNESTO GIULIANO,CAV 01301	VL GERTI
R ESPIRITO SANTO 00277	OSWALDO CRUZ
R ESPIRITO SANTO 01330	FUNDACAO

R ESTILAC LEAL,GAL 00058	SAO JOSE
R ETERNIDADE 00013	SAO JOSE A
R ETERNIDADE 00261	SAO JOSE
R ETERNIDADE 00263	SAO JOSE
R FATIMA,N S 00497	SAO JOSE
R FLAQUER,SEN 00134	SAO JOSE
R FLORIDA 00295+POSTO SAUDE	OSVALDO CRUZ
R FLORIDA 00525	OSVALDO CRUZ
R FLORIDA 00960	OSVALDO CRUZ
R FLORIDA 00975	BAIRRO CERAMICA
R GARCA 00121	BAIRRO CERAMICA
R GARCA 00323	BAIRRO CERAMICA
R GIOVANI PERUCCHI 00190+ESCOLA OSWALDO S M	BAIRRO CERAMICA
R GOITACAZES 00301	BAIRRO CERAMICA
R GONZAGA 00241	BAIRRO CERAMICA
R HELOISA PAMPLONA 00180+ESCOLA S FLAQUER	MAUA
R HELOISA PAMPLONA 00269+NGA-43 SAMUEL KLEIN	MAUA
R HELOISA PAMPLONA 00304	MAUA
R HELOISA PAMPLONA 00316	MAUA
R HELOISA PAMPLONA 00402	SANTA PAULA
R HERCULANO DE FREITAS 00200	SAO JOSE
R HERCULANO DE FREITAS 00265	BARCELONA
R HUMBERTO DE CAMPOS 00000	BARCELONA
R HUMBERTO DE CAMPOS 00550	BARCELONA
R HUMBERTO DE CAMPOS 00600	BARCELONA
R INHAUMA DE,VISC 00905	PROSPERIDADE
R IVAI 00063+ESCOLA EDA MONTOANE	PROSPERIDADE
R JOAO RAMALHO 00100	OSWALDO CRUZ
R JOAQUIM NABUCO 00172	CENTRO
R JOSE BENEDETTI 00550+ EMEF	OSWALDO CRUZ
R JURUA 00050+CER AGUIAS	FUNDACAO
R JUSTINO PAIXAO 00141	FUNDACAO
R LAFAYETTE,CONS 00619	FUNDACAO
R LISBOA 00399	FUNDACAO
R LOURDES 00460	FUNDACAO
R LOURDES 00525	FUNDACAO
R LUIZ LOUZA 00048	FUNDACAO

R LUIZ LOUZA 00170+CRE GONZAGA	SAO JOSE
R MARANHAO 00022+ESCOLA BARTOLOMEU B	SAO JOSE
R MARANHAO 00611	SAO JOSE
R MARIA MACEDO,PROF 00240	OSWALDO CRUZ
R MARTIM FRANCISCO 00177+ESCOLA BENEDITO P A	SANTA MARIA
R MAUA,BR 00133	BOA VISTA
R MAXIMILIANO LORENZINI 00122	SANTO ANTONIO
R MIGUEL GLEBOCCHI 00090+ESCOLA DECIO GAIA	SANTO ANTONIO
R MOGI GUASSU 00080	NOVA GERTY
R NELLY PELLEGRINO 00930	JD S CAETANO
R NELLY PELLEGRINO 00954	BARCELONA
R NELSON 00231	OSVALDO CRUZ
R NESTOR MOREIRA 00300	NOVA GERTY
R NESTOR MOREIRA 00360	NOVA GERTY
R ORIENTE 00333	OLIMPICO
R ORIENTE 00501	OLIMPICO
R OSWALDO CRUZ 01153+UBS NAIR SPINA	OLIMPICO
R OTAVIO MANGABEIRA 00017	OLIMPICO
R PARA 00080	SANTO ANTONIO
R PARA 00088	SANTO ANTONIO
R PARAIBA 00646	CENTRO
R PASTEUR 00430	SANTA PAULA
R PAULO,S 00230+CRE TAMAYO	SAO JOSE
R PAZ 00010	FUNDACAO
R PELEGRINO BERNARDO 00515	BOA VISTA
R PERI 00316	OLIMPICO
R PERI 00361	NOVA GERTY
R PERNAMBUCO 00100	NOVA GERTY R
R PERRELLA 00000	NOVA GERTY
R PIAUI 00420	NOVA GERTI
R PORTO CALVO 00205	CERAMICA
R PRATES 00430	CERAMICA
R PRESTES MAIA 00100	BARCELONA
R PRUDENTE DE MORAIS 00081	BARCELONA
R RAFAEL CORREA SAMPAIO 00584+ B	SANTA PAULA
R RAFAEL CORREA SAMPAIO 00600	OSWALDO CRUZ
R RIO DE JANEIRO 00018+18/28	CENTRO

R RIO GRANDE DO SUL 00083	CENTRO
R RIO GRANDE DO SUL 00790	CENTRO
R ROSA,STA 00079	JD SAO CAETANO
R SEBASTIAO DIOGO 00099	SANTO ANTONIO
R SÃO PAULO, 200 (TAMOYO)	OSWALDO CRUZ
R SERAFIM CARLOS 00571	MAUA
R SERAFIM CONSTANTINO 00000+COMJUV	OLIMPICO
R SILVIA 00160	OSWALDO CRUZ
R SILVIA 00670+ESCOLA ROSALVITO C	OSWALDO CRUZ
R SILVIA 01743	CENTRO
R TAPAJOS 01085	FUNDACAO R
R TEFFE 00460	STO ANTONIO
R TEODORO SAMPAIO 00201	OSWALDO CRUZ
R TIRADENTES 00000	OSWALDO CRUZ
R TOMASO TOME 00270	NOVA GERTY
R TUPI 00300	SANTA PAULA
R ULYSSES TORNINCASA 00160	SANTO ANTONIO
R VANDA 00011+NASF PSF	SANTO ANTONIO
R VANDA 00073	OSVALDO CRUZ
R VICTOR MEIRELLES 00066	SANTO ANTONIO
R VIEIRA DE CARVALHO 00525	SANTO ANTONIO
TR SEBASTIAO GOMES LIMA 00060	SANTA PAULA

E demais localidades que vierem a ser criadas durante vigência contratual.