PREGÃO ELETRÔNICO Nº 27/2025
PROCESSO DE COMPRAS Nº 873/2025
TIPO DE JULGAMENTO DA LICITAÇÃO: Menor preço por lote

A Universidade Municipal de São Caetano do Sul - USCS torna público que fará realizar a licitação na modalidade de pregão eletrônico, do tipo menor preço global por lote, conforme descrito neste Edital e seus Anexos, e em conformidade com a Lei Federal nº 14.133/2021, Lei Complementar Federal nº 123/2006 com as devidas alterações introduzidas pelas Leis Complementares Federais nº 147/2014 e 155/2016, Lei Municipal nº 4.660/2008 e portaria da Universidade USCS de número 115/2024.

UNIDADE CONTRATANTE:
Reitoria da Universidade Municipal de São Caetano do Sul – USCS

ENDEREÇO:
Avenida Goiás, 3.400, Bairro Barcelona, São Caetano do Sul - São Paulo, CEP 09550-051. telefone 55 (11) 4239-3302 e 4239-3215.

LOCAL, DATA E HORÁRIO DA SESSÃO PÚBLICA DE PROCESSAMENTO DO PREGÃO:

A sessão pública de processamento do Pregão Eletrônico será realizada no endereço eletrônico https://pregaoeletronico.saocaetanodosul.sp.gov.br/uscs/ mediante condições de segurança, criptografia e autenticação, em todas as suas fases.

DATA: 19/12/2025 às 11h.

PARTIICIPAÇÃO:
Ampla participação.

MODO DE DISPUTA DE LANCES:
Modo de disputa aberto.

RITO: Procedimental comum, conforme disposto no artigo 29 da Lei 14.133/2021.

O pregão em referência será conduzido por pregoeiro, devidamente designado pela autoridade superior e contará com auxílio de equipe de apoio, de acordo com regramento definido na Lei 14.133/2021 e pelas normas contidas neste edital.

1. DO OBJETO DA LICITAÇÃO

1.1. O presente pregão tem por objeto a contratação de empresa especializada para fornecer Solução de Serviço gerenciado para gestão ativos de rede WiFi, monitoramento e segurança, incluindo fornecimento de softwares, equipamentos e licenciamentos na modalidade *As a Service*, suporte técnico especializado, acessórios e garantia para atendimento da Universidade Municipal de São Caetano do Sul, conforme condições e especificações constantes neste edital e seus anexos.

1.2. A solução gerenciada de ativos de rede deverá abranger o fornecimento da infraestrutura necessária, configuração, implantação, gerenciamento e monitoramento contínuo de switches, pontos de acesso WiFi e controladora com vistas a garantir alta disponibilidade, segurança e desempenho da infraestrutura de Tecnologia da Informação da Universidade USCS, levando-se em conta que o ambiente de WiFi deverá comportar o acesso simultâneo de 10.000 usuários.

2. DAS CONDIÇÕES PARA PARTICIPAÇÃO

2.1. Poderão participar deste pregão eletrônico todos os interessados do ramo de atividade pertinente ao objeto da contratação e que atenderem a todas as exigências constantes deste edital e seus anexos.

2.1.1. O registro no Portal Eletrônico da Universidade Municipal 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, concedem autorização para participação em qualquer pregão eletrônico.

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

2.2. Os proponentes interessados em participar deste processo licitatório deverão retirar o edital completo e seus anexos nos endereços eletrônicos a partir dos links https://licitacao.uscs.edu.br/ ou https://pregaoeletronico.saocaetanodosul.sp.gov.br/uscs/;

Nota: É importante o acesso frequente à página eletrônica da Universidade, 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.

2.2.1. Os interessados em adquirir o edital pessoalmente deverão, na ocasião da aquisição, disponibilizar mídia removível (pen drive), no endereço da Rua Maceió, 177, Bairro Barcelona, São Caetano do Sul/SP, CEP 09551-030, setor de Licitações/Compras da Universidade USCS.

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

2.3.1. Organizações da Sociedade Civil de Interesse Público – OSCIP, atuando nessa condição;

2.3.2. ***Não*** poderão participar empresas estrangeiras que não funcionem no País; empresas estrangeiras que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente; os interessados que se encontrem sob processo de falência, concurso de credores, dissolução, liquidação, salvo o disposto na Súmula nº 50 do Tribunal de Contas do Estado de São Paulo, bem como aqueles que tenham incorrido nas sanções dispostas no artigo 155, incisos III e IV da Lei Federal nº 14.133/2021, em substituição aos artigos da legislação revogada, dispostos na Súmula nº 51 do TCESP;

2.3.3. Não poderão participar empresas estrangeiras que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

2.3.4. 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 nº 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;

2.3.5. O impedimento de que trata o subitem 2.3.4. será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante;

2.3.6. A idoneidade dos participantes será consultada nos 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)

2.3.7. 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;

2.3.8. Não poderá participar empresas controladoras, controladas, nos termos da Lei nº 6.404/1976, concorrendo entre si;

2.3.9. Não poderão participar pessoas físicas ou jurídicas 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;

2.3.10. Demais condições estabelecidas no artigo 14 da Lei Federal 14.133/2021;

2.3.11. Pessoa física ou jurídica que estejam enquadradas nas disposições do artigo 10 da Lei Federal número 9.605/1998;

2.4. Empresas reunidas em consórcio poderão participar da licitação desde que respeitados os requisitos dispostos no artigo 15 da Lei Federal nº 14.133/2021;

2.5. A proponente interessada em participar deste processo licitatório referenciado no lote 01, deverá declarar que detém a documentação de conformidade que é um parceiro credenciado, revendedor autorizado do fabricante, comprovando sua capacidade para oferecer e fornecer suporte aos equipamentos ofertados no formato *as a service*, bem como deverá estar apta a realizar suas implantações, assim, evitando processos de falsificação de licenciamento e até mesmo importação irregular de hardware.

2.6. Deverá ser prestada comprovação do recolhimento a título de garantia de proposta para licitar, concernente ao **lote único**, no valor de R$ 66.922,34 (sessenta e seis mil, novecentos e vinte e dois reais e trinta e quatro centavos), correspondente a 1% do valor estimado, conforme disposto no § 1º do caput do artigo 58 da Lei Federal 14.133/2021. A garantia de proposta (lotes 01 e/ou 02) poderá ser prestada optando-se por uma das modalidades de que trata o parágrafo primeiro do artigo 96 da mesma Lei.

2.6.1. Se o proponente optar pela garantia na modalidade **caução** em moeda corrente, mediante guia de recolhimento expedida pelo setor de Contabilidade e Finanças da Universidade Municipal de são Caetano do Sul, situado à Rua Maceió, 177, Bairro Barcelona São Caetano do Sul, obrigatoriamente, deverá fazê-la até 02 (dois) dias úteis anterior à abertura da sessão pública do certame.

2.6.2. O comprovante de recolhimento a título de garantia de proposta, em quaisquer das modalidades previstas no § 1º do artigo 96, deverá, obrigatoriamente, sob pena de desclassificação, integrar os documentos da proposta comercial relacionados.

2.7. *Não* poderá participar empresa que tenha sido proibida pelo Plenário do CADE de participar de licitações promovidas pela Administração Pública federal, estadual, municipal, direta e indireta, em virtude de prática de infração à ordem econômica, nos termos do artigo 38, inciso II, da Lei Federal n° 12.529/2011.

2.8. *Não* poderá participar empresa que tenha sido proibida de contratar com o Poder Público em razão de condenação por ato de improbidade administrativa, nos termos do artigo 12 da Lei Federal nº 8.429/1992.

2.9. *Não* poderá participar empresa declaradas inidônea pelo Poder Público e não reabilitadas.

2.10. *Não* poderá participar cooperativa, considerando-se que as particularidades do objeto não são atinentes ao disposto nos termos do artigo 16 da Lei Federal 14.133/2021.

2.11. Será vedada a subcontratação de pessoa física ou jurídica, se aquela ou os dirigentes desta mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente da entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou se deles forem cônjuge, companheiro ou parente em linha reta, colateral, ou por afinidade, até o terceiro grau.

2.12. Não se admitirá oferta que não contemple a integralidade dos itens que compõe os equipamentos e/ou serviços em disputa, bem como a sua perfeita relação funcional no âmbito da solução.

2.12.1. A licitação será composta por lote único, formado pelos equipamentos *as a service*, softwares, materiais, licenciamento, garantias e serviços disposto no termo de referência deste edital.

2.13. As empresas interessadas em participar do presente certame, **poderão** realizar **Visita Técnica**, através de seu representante legal ou técnico, devidamente credenciados pela empresa, a fim de tomar ciência das instalações e locais da Universidade Municipal São Caetano do Sul, onde será executada a solução de serviço de gerenciamento e gestão de ativos e de segurança de rede nas dependências das diversas unidades USCS. Na oportunidade, os proponentes poderão receber informações que por ventura sejam necessárias acerca das obrigações da presente licitação, notadamente em relação a distribuição e dispoção dos equipamentos as a service nas respectivas unidades, bem como informações que eventualmente possam permitir adequada precificação e formulação de proposta comercial.

2.13.1. A Vistoria Técnica ocorrerá durante o período da publicação do edital, salvo no período de suspensão do certame, se houver, devendo ser agendada previamente com o senhor Alessandro

Parada pelo e-mail dti@online.uscs.edu.br unidades Barcelona, Centro e Conceição) e Paulo Sérgio Ruiz pelo e-mail pruiz@online.uscs.edu.br (unidade Itapetininga), ocasião em que serão emitidos os comprovante que serão apresentados na sessão pública do pregão, conforme disposto no **Anexo XIII** deste edital.

2.14. O comprovante de **Vistoria Técnica**, quando realizada, deverá ser apresentado juntamente com os Documentos de Habilitação, conforme disposto no artigo 63 da Lei Federal 14.133/2021.

2.15. A vistoria técnica, embora não obrigatória, é importante para permitir ao proponente extrair as particularidades da infraestrutura predial e suas possíveis implicações que possam impactar na formulação da proposta comercial, contudo, faculta-se ao licitante optar por declarar que se abstém de realizá-la conforme modelo apresentado no **Anexo XIV** – "Declaração de Abstenção de Vistoria", assumindo completa e irrestrita responsabilidade pelos imprevistos e problemas decorrentes do desconhecimento das realidades das Unidades de execução dos serviços, em razão de sua não realização, nos termos do § 3º, artigo 63 da Lei Federal 14.133/2021.

2.16. O atestado de visita técnica deverá ser emitido considerando as unidades efetivamente visitadas pelo pretenso proponente. Na hipótese de que pelo menos uma das cinco unidades não seja vistoriada, o licitante deverá apresentar para a unidade não vistoriada a declaração de abstenção de vistoria nos termos do **Anexo XIV**.

3. DA REPRESENTAÇÃO E DO CREDENCIAMENTO NO SISTEMA DE PREGÃO ELETRÔNICO

3.1. Poderão participar desta licitação, as pessoas que atenderem as exigências deste Edital.

3.2. A participação do interessado no pregão eletrônico, dar-se-á a partir da plataforma https://pregaoeletronico.saocaetanodosul.sp.gov.br/uscs/ 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;

3.3. O acesso ao pregão, para efeito de encaminhamento proposta de preço, lances sucessivos, documentos de habilitação e demais documentos, somente se dará mediante prévia definição de senha privativa, conforme disposto no subitem 2.1.1.;

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

3.5. 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 à USCS a responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros;

3.6. 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;

3.7. A participação no pregão estará condicionada obrigatoriamente a inscrição na plataforma, conforme descrito no subitem 3.2., antes da data e horário previsto no edital para início da sessão, e o credenciamento do licitante deverá ser requerido e acompanhado dos documentos elencados abaixo:

3.7.1. Proposta de preços conforme disposto no modelo **Anexo II** e demais documentos obrigatórios que a integram;

3.8. O custo de operacionalização e uso do sistema ficará a cargo do licitante;

3.9. O registro no Portal de Pregão Eletrônico da Universidade Municipal de São Caetano do Sul é gratuito.

4. DA PROPOSTA COMERCIAL

4.1. O encaminhamento da proposta comercial para o sistema eletrônico pressupõe o pleno conhecimento e atendimento às exigências de classificação e habilitação previstas no edital. A 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;

4.1.1. Nos preços apresentados deverão estar inclusos todos os custos/despesas e encargos inerentes ao fornecimento dos serviços e/ou bens, correspondentes a todo o período de execução até a vigência final fixada neste edital;

4.1.2. A omissão de qualquer custo ou 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 indiretas, as quais serão assim consideradas. No caso de erros aritméticos, serão considerados pelo pregoeiro, para fins de seleção e contratação, os valores retificados;

4.1.3. 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 valor unitário;

4.1.4. O objeto ofertado deverá atender plenamente às especificações contidas no Termo de Referência deste edital - **Anexo I**. O licitante deverá fixar preço unitário, **mensal e global** para os serviços e/ou bens licitados referentes ao lote único sob disputa, considerando o período de 24 meses, discriminado todos os valores unitários e totais de cada item, líquidos, fixos e irreajustáveis, em moeda nacional, expressos com duas casas decimais, desprezando-se as frações remanescentes, para a data fixada para apresentação da proposta;

4.1.5. Documento comprobatório referente ao recolhimento a título de garantia de proposta concernente ao **lote único em disputa**, em quaisquer das modalidades previstas no § 1º do artigo 96 da Lei Federal 14.133/2021;

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

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

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

4.1.9. Quando do preenchimento da Proposta Comercial no sistema **plataforma do pregão eletrônico** da USCS, será desclassificada a proposta que identificar o licitante através da razão social, endereço, telefone ou qualquer outra informação que possibilite a identificação prévia da empresa, portanto, no curso desse edital, o proponente não deverá preencher a marca, modelo e fabricante para os serviços de instalação, configuração e parametrização (que corresponde aos tens 4, 10 e 13 do Anexo II).

5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS, ETAPA COMPETITIVA E JULGAMENTO DAS PROPOSTAS

5.1. A partir do horário previsto no edital e no sistema para cadastramento e encaminhamento da proposta comercial terá início a sessão pública do pregão eletrônico, quando serão divulgadas as propostas recebidas, para avaliação e aceitabilidade do pregoeiro.

5.1.1. 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 para usufruirdos benefícios estabelecidos na Lei Complementar 123/2006 e suas alterações;

5.1.1.1. O licitante que não informar essa condição mencionada no subitem imediatamente acima, antes do envio da proposta perderá o direito ao tratamento diferenciado, inclusive no que concerne ao § 2º do artigo 44 da Lei Complementar 123/2006.

5.1.2. A análise das propostas pelo pregoeiro, limitar-se-á ao atendimento das condições estabelecidas neste Edital e seus anexos e à legislação vigente;

5.1.3. O proponente detentor da melhor oferta **deverá** apresentar imediatamente após a convocação a ser efetuada pelo agente público pregoeiro, a documentação oficial (quickspec ou datasheet) contendo as especificações técnicas dos **equipamentos *as a service*, licenciamento e serviços** que compõem a solução ofertada, inclusive no que tange as certificações e homologações necessárias à consecução do projeto, para verificação do responsável pela análise técnica, onde possam ser constatadas de forma clara e objetiva as características, que concretamente integrarão o contrato, sendo que tais equipamentos e serviços dispostos na proposta comercial deverão estar em conformidade com toda a especificação técnica apresentada no anexo, nomeado Termo de Referência deste edital, como condição de julgamento da proposta comercial;

5.1.4. O sistema ordenará automaticamente as propostas classificadas pelo pregoeiro;

5.1.5. A desclassificação da proposta será fundamentada e registrada no sistema, acompanhada em tempo real por todos os participantes;

5.1.6. O licitante que tiver sua proposta desclassificada e desejar recorrer da decisão deverá observar o disposto no item 09 deste edital.

5.2. Classificadas as propostas, o agente público 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;

5.2.1. O valor de redução mínima entre os lances será de 0,5% (cinco décimos por cento) e incidirá sobre o valor unitário de cada item que integra o lote único em disputa (Anexo III), portanto, será utilizado o conceito de redução linear, cujo valor final do lote ajustado em decorrência da etapa competitiva e de negociação, será apreciado em proposta readequada;

5.2.2. O licitante poderá oferecer, conforme definido no edital, valores iguais ou superiores ao menor já ofertado e registrado pelo sistema, observado o intervalo mínimo de diferença de percentuais/valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta.

5.3. Nos termos do Inciso I do artigo 56, da Lei Federal nº 14.133/21, será adotado o **Modo Aberto** de disputa, o qual terá etapa de lances com duração de 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema, quando houver lance ofertado nos últimos 02 (dois) minutos do período de duração da sessão pública. A prorrogação automática da etapa de lances (02 minutos) 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 pregoeiro poderá, assessorado pela equipe de apoio, se assim considerar necessário, admitir o reinício da etapa de envio de lances, na situação prevista pelo § 4º do artigo 56 da Lei Federal nº 14.133/21;

5.3.1. A situação prevista no item anterior e no § 4º do artigo 56, da Lei Federal nº 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, vez que já encerrada a etapa de lances. Os demais licitantes poderão formular outros lances, inclusive intermediários entre si;

5.3.2. O pregoeiro tem a ação de iniciar a fase de lances, depois, todo processo é automático, conforme explanado acima, desse modo, 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.

5.4. Não poderá haver desistência dos lances ofertados, sujeitando-se o proponente que descumprir sua proposta às penalidades constantes no item 17 deste edital.

5.4.1. Excepcionalmente, o licitante poderá excluir seu último lance ofertado, **uma única vez**, no prazo de quinze segundos após o registro no sistema, caso o lance seja inconsistente, contenha erro de digitação ou seja inexequível.

5.5. 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.

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

5.7. 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.

5.8. Devido a impossibilidade de previsão de tempo extra, as empresas participantes deverão estimar o seu valor mínimo de lance a ser ofertado, evitando assim, cálculos de última hora, que poderão resultar em uma disputa frustrada por falta de tempo hábil.

5.9. O critério de aceitabilidade dos preços propostos pelas licitantes será o de compatibilidade com os preços praticados prelo mercado, coerentes com o objetivo ora licitado.

5.10. 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;

5.10.1. Em caso de empate entre duas ou mais propostas, serão utilizados os critérios de desempate estabelecidos pelo artigo 60 da Lei nº 14.133/21, ressalvando-se o disposto no § 2º do artigo 44 da Lei Complementar 123/2006 que estará automaticamente assegurado no decurso desse processo licitatório.

5.11. Definido o desempate entre duas ou mais propostas, o pregoeiro poderá negociar condições mais vantajosas com o primeiro colocado;

5.11.1. Caso o primeiro colocado, mesmo após a negociação, permaneça com sua proposta acima do preço máximo definido pela Universidade USCS, a negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida.

5.12. O pregoeiro anunciará a licitante detentora da proposta ou lance de menor valor, imediatamente após o encerramento da referida etapa de lances da sessão pública ou, quando for o caso, após negociação e decisão sobre a aceitação do lance de menor valor.

5.13. A escolha da melhor proposta terá como critério de julgamento o menor preço global para o lote único.

5.14. Após a fase competitiva, o agente publico pregoeiro em decorrência da necessidade de avaliação técnica documental acerca dos equipamentos, licenciamentos e serviços ofertados no âmbito da solução (quickspec ou datasheet), poderá suspender a sessão pública para execução de tal análise para o proponente detentor de melhor oferta;

5.14.1. O tempo de suspensão da sessão pública, dar-se-á em decorrência da necessidade temporal para análise desse conteúdo, pela equipe técnica da Universidade USCS.

5.15. O presente edital se submete ao disposto na Lei Complementar 123/2006 e sua posteriores alterações e aos termos da Lei Municipal nº 4660/2008 no que couber;

5.16. Serão desclassificadas as propostas:

a) apresentadas por licitante impedida de participar, nos termos do subitem 5.1.4. deste edital;

b) formuladas por licitantes participantes de cartel, conluio ou qualquer acordo conclusivo voltado a fraudar ou frustrar o caráter competitivo do certame licitatório;

c) contiverem vícios insanáveis;

d) não atendam as especificações, prazos e condições fixados neste edital;

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

f) não tiverem sua exequibilidade demonstrada, quando exigida pelo pregoeiro.

5.17. O pregoeiro, ao final do julgamento das propostas, solicitará ao licitante mais bem classificado que envie a proposta adequada concernente ao último lance ofertado, após a negociação, se houver, **no prazo de 2 (duas) horas,** acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste edital e já apresentados, sob pena de desclassificação.

5.18. Sendo considerada aceitável a proposta de menor preço para o lote único, bem como obedecidas às exigências fixadas neste edital, o pregoeiro passará para a etapa habilitação do licitante detentor de melhor oferta que a tiver formulado, com base na documentação enviada na própria sessão pública.

6. DA HABILITAÇÃO

6.1. Para fins de habilitação no presente Pregão o licitante vencedor deverá apresentar os documentos a seguir especificados, válidos na data de sua apresentação. 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.

6.1.1. Para efeito de exigência concernente aos documentos de habilitação, essa administração se pautará nos termos definidos no âmbito da Lei 14.133/2021, respeitando-se em particular, as determinações contidas nos incisos II e III do caput do artigo 63.

6.2. **Relativos à Habilitação Jurídica**:

6.2.1. Registro Comercial, para empresa individual;

6.2.2. Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, para as sociedades empresariais, e, no caso de sociedades por ações, acompanhado dos documentos comprobatórios de eleição de seus administradores;

6.2.3. Inscrição do ato constitutivo, no caso de sociedades simples (civis), acompanhada, quando couber, de prova do registro da ata da eleição da diretoria em exercício (Registro Civil de Pessoas Jurídicas);

6.2.4. 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.

6.3. **Relativos à Regularidade Social, Fiscal e Trabalhista**:

6.3.1. Prova de inscrição no Cadastro Nacional de Pessoa Jurídica do Ministério da Fazenda (CNPJ);

6.3.2. 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 (certidão conjunta nos termos da Portaria MF 358/2014), referente a todos os tributos federais e à Dívida Ativa da União por elas administrados, abrangendo inclusive as contribuições sociais previstas nas alíneas “a” e “d” do parágrafo único do artigo 11, da Lei nº 8.212/1991;

6.3.3. Prova de regularidade para com a Fazenda estadual (relativos a dívida inscrita), consistente na apresentação de certidão que comprove regularidade fiscal ao Estado ou Distrito Federal;

6.3.4. Prova de regularidade para com a Fazenda municipal da sede da empresa licitante, consistente na apresentação de certidão de regularidade de débitos municipais mobiliários;

6.3.5. Prova da regularidade para com o Cadastro de Informativo Municipal CADIN do Município de São Caetano do Sul, emitida pelo site: https://cadin.saocaetanodosul.sp.gov.br/;

6.3.5.1. Todos os licitantes deverão apresentar o documento exigido no subitem 6.3.5. inclusive aquelas que não se encontram sediadas neste município, em cumprimento ao inciso I, do artigo 3º, da Lei 5.581/2017;

6.3.5.2. No caso de isenção ou de não incidência dos impostos devidos ao Estado e/ou Município, deverá, a licitante apresentar declaração assinada pelo representante legal, sob pena da lei;

6.3.6 Prova de Regularidade relativa ao Fundo de Garantia por Tempo de Serviço, através do Certificado de Regularidade do FGTS (CRF) ou do documento denominado "Situação de Regularidade do Empregador", com prazo de validade em vigor na data marcada para o processamento do Pregão Eletrônico;

6.3.7. Certidão de Inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação da Certidão Negativa de Débitos Trabalhistas ou de Certidão Positiva de Débitos Trabalhistas com efeito de negativa, nos termos do artigo 642-A da Consolidação das Leis do Trabalho, com prazo de validade em vigor na data marcada para o processamento do Pregão eletrônico;

6.3.8. Declaração de Regularidade perante o Ministério do Trabalho no que se refere à observância do disposto no Inciso XXXIII do artigo 7º da Constituição Federal, nos termos do modelo constante, conforme modelo do **Anexo IV** deste edital;

6.3.9. A licitante deverá apresentar declaração indicando que sua proposta econômica compreende a integralidade dos custos para atendimento dos direitos trabalhistas, sob pena de desclassificação conforme modelo disposto no do **Anexo IX**;

6.3.10. Declaração de que cumpre as exigências de reserva de cargos para pessoas com deficiência e para reabilitados da Previdência Social previstas na Lei Federal 8.213/1991, nos termos do modelo constante do **Anexo X**;

6.3.11. As licitantes que se encontram na condição de Microempresa ou Empresa de Pequeno Porte deverão nos termos da legislação fiscal, apresentar declaração de enquadramento, conforme modelo do **Anexo VI** deste edital;

6.3.11.1. Para efeito da Lei Complementar Federal nº 123/2006 com as devidas alterações introduzidas pelas Leis Complementares Federais 147/2014 e 155/2016 e, do art. 22 da Lei Municipal nº 4.660/2008, as microempresas e empresas de pequeno porte deverão apresentar toda a documentação relativa a regularidade fiscal e trabalhista, mesmo que esta apresente alguma restrição;

6.3.11.2. Havendo alguma restrição quanto à regularidade fiscal e trabalhista, será assegurado o prazo de 5 (cinco) dias úteis, contados a partir do momento em que a licitante for declarada vencedora do certame, prorrogável por igual período, a critério da Administração, para fins de apresentação das certidões negativas ou positivas com efeito de negativas;

6.3.11.3. A licitante habilitada com pendências, deverá por ocasião da assinatura do contrato ou da retirada do instrumento equivalente, comprovar sua regularidade fiscal e trabalhista, sob pena de decadência do direito à contratação, sem prejuízo da aplicação das sanções cabíveis.

6.3.12. Serão aceitas certidões positivas com efeito de negativas. Não constando do documento seu prazo de validade, será aceito documento emitido até 180 (cento e oitenta) dias imediatamente anteriores à data marcada para o processamento do pregão eletrônico.

6.4. **Relativos à Qualificação Econômico-Financeira**:

6.4.1. Apresentação de publicação dos dois últimos balanços patrimoniais incluindo a documentação do resultado dos exercícios 2023 e 2024. Não sendo a licitante obrigada a publicar seu balanço, deverá apresentar fotocópia legível de página do Diário Geral, onde tenha sido transcrito o balanço patrimonial, Ativo/Passivo, e a demonstração do resultado do exercício. Estes documentos deverão conter os respectivos termos de abertura e encerramento, registrados na Junta Comercial ou Cartório de Registro Civil de Pessoas Jurídicas. Esta exigência também se aplica às licitantes que optam pela Tributação Simplificada do Imposto de Renda Pessoa Jurídica (“Lucro Presumido” ou “microempresa”).

6.4.2. As licitantes obrigadas ao Sistema Público de Escrituração Digital – SPED devem apresentar suas demonstrações financeiras impressas pelo sistema, devidamente validado, do ano base exigível pela lei, acompanhado dos seus respectivos Termos de Abertura e Encerramento, Demonstração do Resultado do Exercício e Recibo de Entrega.

6.4.3. A licitante que apresentar balanço patrimonial e/ou Demonstração do Resultado do Exercício em meio eletrônico deverá observar as normas de escrituração contábil em forma eletrônica pertinentes.

6.4.4. Comprovação da situação financeira da licitante desde que fique evidenciado, via demonstrativos, relativos ao balanço apresentado, o atendimento dos seguintes índices:

a) A empresa deverá apresentar os cálculos de situação financeira, baseando-se na obtenção dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), **≥ 1**(um), resultantes da aplicação das fórmulas, devidamente assinada por profissional competente (contador):

LG = (AC + RLP) / (PC + ELP)

SG = AT / (PC+ELP)

LC = AC / PC

ONDE: AC = Ativo Circulante; PC = Passivo Circulante; RLP = Realizável a Longo Prazo; ELP = Exigível a Longo Prazo e AT = Ativo Total.

b) As fórmulas deverão estar devidamente aplicadas em memorial de cálculos juntado ao balanço, devidamente assinado pelo responsável técnico (**contador**).

6.4.5. Certidão Negativa de Falência expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial expedida no domicílio da pessoa física. Não constando do documento seu prazo de validade, será aceito documento emitido até 180 (cento e oitenta) dias imediatamente anteriores à data marcada para o processamento do pregão.

6.5. **Relativos à Qualificação Técnica**:

6.5.1. Comprovação de aptidão para o fornecimento do objeto do presente edital, estando de acordo com as características, quantidades e prazos compatíveis. 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 fornecimento similares obedecerão ao percentual de 50% (cinquenta por cento), nos termos do artigo do artigo 67, § 2º, da Lei Federal 14.133/2021. Somente serão considerados válidos atestados com timbre da entidade expedidora e com identificação do nome completo. O atestado deverá ser datado e assinado por pessoa física identificada pelo seu nome e cargo exercido na entidade, bem como dados para eventual contato, estando as informações sujeitas à conferência pelo pregoeiro.

6.5.1.1. Somente serão considerados válidos atestados com timbre da entidade expedidora e com identificação do nome completo. O atestado deverá ser datado e assinado por pessoa física identificada pelo seu nome e cargo exercido na entidade, bem como dados para eventual contato, estando as informações sujeitas à conferência pelo pregoeiro

6.5.1.2. O(s) quantitativo(s), quando não mencionado(s) no(s) atestado(s), e/ou não mencionados em ambientes de tecnologia que atendem ao percentual estipulado de acordo com o parágrafo segundo do artigo 67 da Lei 14.133/2021, poderá(ão) ser comprovado(s) por quaisquer documentos, tais como, contratos, notas fiscais ou outros documentos equivalentes, desde que reste demonstrada a execução concomitante dos serviços atestados e fornecimento dos equipamentos, levando-se em conta a capacidade de acessos simultâneos no que diz respeito a infraestrutura dos serviços de rede WiFi e conectividade para atendimento nesta contratação.

6.5.2. O licitante deverá **declarar** formalmente, de acordo com o contido no **Anexo XII**, que detém *status de parceiro credenciado do fabricante dos equipamentos,* ou, que é revendedor autorizado do fabricante, indicando sua capacidade para oferecer e fornecer suporte aos equipamentos ofertados *as a service*, bem como deverá estar apto a realizar suas implantações.

6.6. **Relativo à capacitação Profissional**

6.6.1. A licitante deverá indicar em declaração nos termos do **Anexo XI**, que dispõe de pelo menos um profissional gerente projetos, um profissional analista de monitoramento de redes e serviços sênior e um profissional de monitoramento de rede de serviços junior, com qualificação técnica mínima compatível com as exigências de cunho técnico/tecnológicos para suportar a implantação, configuração, suporte técnico e manutenção, bem como as atividades laborais vinculadas à segurança de rede WiFi e monitoramento, considerando-se que esses profissionais estarão à frente da equipe de pessoal necessário à prestação dos serviços concernentes ao objeto do certame, respeitando-se as particularidades inerentes ao escopo de contratação.

6.6.2. A licitante deverá apresentar, no ato de celebração do contrato, a comprovação de certificação técnica necessária dos profissionais que integrarão a equipe de trabalho designada para consecução do projeto, consoante ao disposto no subitem 6.6.1., sob pena de, em não apresentando, sujeitar-se às penalidades dispostas no item 17 deste edital.

6.7. **Outras exigências de Qualificação**:

6.7.1. Declaração de atendimento às normas relativas à saúde e segurança no trabalho, em virtude das disposições do parágrafo único, artigo 117 da Constituição do Estado de São Paulo, nos termos do modelo constante do constante do **Anexo VII** deste edital;

6.7.2. Declaração de que cumpre o pleno atendimento aos requisitos de habilitação nos termos do modelo constante no **Anexo V** deste edital;

6.7.3. Declaração de atendimento às condições gerais de privacidade, nos termos da Lei Federal 13.709/2018 – LGPD, descritos no modelo registrado sob a forma do **Anexo VIII** - "Declaração de Condições Gerais de Privacidade e Proteção de Dados de Pessoas.

6.7.4. A licitante, se realizar vistoria, deverá apresentar declaração constante do **Anexo XIII**, assinada por funcionário designado pela USCS, indicando que efetivamente realizou visita técnica para tomar ciência acerca das condições e das particularidades referente aos locais (unidades 1, 2, 3, 4, e 5) dispostos no item "a" nomeado *"Unidades da Universidade USCS que integram o projeto"* no Termo de Referência.

6.7.5. Na hipótese de o proponente optar por não realizar a visita técnica em pelo menos uma das unidades apontadas no subitem imediatamente anterior, deverá, sob pena de inabilitação entregar a declaração referente àquela(s) unidade(s) não vistoriada(s) nos termos aportados no **Anexo XIV** deste edital.

7. DISPOSIÇÕES GERAIS DA HABILITAÇÃO

7.1. O 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;

7.2. A verificação será certificada pelo pregoeiro e deverá ser anexada aos autos os documentos passíveis de obtenção por meio eletrônico, salvo impossibilidade devidamente justificada;

7.3. 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;

7.4. Não serão aceitos documentos autenticados digitalmente pelo **Cartório Azevedo Bastos**, considerando-se a impossibilidade de consultar a autenticidade das autenticações, conforme comunicado disponibilizado no site do referido Cartório;

7.4.1. *"Em razão de intervenção determinada pela Conselheira Jane Granzoto Torres da Silva, do Conselho Nacional de Justiça, o 1º Registro Civil de Pessoas Naturais de João Pessoa está sob a responsabilidade de Sidnei da Silva Perfeito. Também em razão da intervenção, estão suspensos quaisquer serviços de autenticação digital".*

7.5. Os documentos eletrônicos produzidos com a utilização de processo de certificação disponibilizada pela ICP-Brasil, nos termos nos termos da Medida Provisória nº 2.200-2, ou ainda do artigo 5º da Lei Federal 14.063/2020, serão recebidos e presumidos verdadeiros em relação aos signatários, dispensando-se o envio de documentos originais e cópias autenticadas em papel;

7.6. Caso a licitante provisoriamente vencedora com o menor preço venha a desatender as exigências para a habilitação, o pregoeiro 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 autoria atenda aos requisitos de habilitação, caso em que será declarada vencedor.

8. DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO E PEDIDO DE ESCLARECIMENTO AO EDITAL

8.1. Qualquer pessoa é parte legítima para impugnar o edital de licitação por irregularidade na aplicação da Lei, ou pedir esclarecimentos devendo protocolar o pedido até 3 (três) dias úteis antes da data de abertura do certame, ou seja, **até às 23:59 horas do dia 15/12/2025**, no endereço da a Rua Maceió, 177, Bairro Barcelona, São Caetano do Sul - São Paulo, CEP 09551-030 ou, preferencialmente por meio da inserção na plataforma do pregão eletrônico https://pregaoeletronico.saocaetanodosul.sp.gov.br/uscs/ , ou ainda a partir do envio por e-mail

no endereço licitacao@online.uscs.edu.br quando se tratar de pedido de esclarecimentos/questionamentos.

8.1.1. Concernente à impugnação, o seu devido conhecimento/recebimento se dará somente com o ingresso dos documentos que configure competência e poderes para exercer tal ação, juntamente com o documento sob a forma de peça impugnatória. Neste sentido, ainda não serão conhecidas as impugnações apresentadas fora do prazo legal

8.2. A resposta à impugnação ou 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.

8.3. Todas as solicitações de esclarecimento, bem como suas respostas serão numeradas sequencialmente e serão consideradas como aditamentos a este instrumento convocatório, sendo juntadas ao respectivo processo licitatório.

8.4. Caberá a autoridade competente receber, examinar e decidir as impugnações (signatário do edital) e, ao pregoeiro caberá decidir sobre as solicitações de esclarecimento ao edital e aos anexos, além de poder requisitar subsídios formais aos responsáveis pela elaboração desses documentos, bem como contar com o auxílio técnico e/ou jurídico.

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

8.5. Acolhida a impugnação ou os esclarecimentos apresentados em face do Edital e a modificação consubstanciada na decisão, NÂO comprometer os aspectos de formulação da proposta por parte dos proponentes, ou ainda não se traduzam em prejuízo no prazo de apresentação dos documentos relativos à sua participação no certame, a data original da sessão do pregão eletrônico será resguardada, caso contrário, será designada nova data para a realização do certame (§ 1º, art. 55, Lei nº 14.133/21).

8.6. 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.

8.7. Não serão aceitas consultas, reclamações, impugnações ou questionamentos efetivados por meio de ligação telefônica ou consulta verbal.

9. DOS RECURSOS ADMINISTRATIVOS

9.1 Declarada vencedora, o pregoeiro informará às licitantes por meio de mensagem lançada no sistema, da qual poderão manifestar sua intenção de interpor recurso, que deverá ser realizada por meio eletrônico, utilizando exclusivamente o campo próprio disponibilizado no sistema de pregão no prazo de 10 (dez) minutos.

9.2. 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 aos autos do processo.

9.3. A formalização dos recursos, observados os prazos legais, será dirigida ao pregoeiro nos termos do art. 165, § 1º, da Lei 14.133/2021, e será efetivada por meio de documento com identificação do Processo e número do Pregão eletrônico **devendo ser redigido ou anexado em campo específico do sistema**, sob pena de decadência do direito de recorrer.

9.4. A falta de manifestação imediata da licitante, bem como a não apresentação das razões recursais no prazo estabelecido no item 9.2., importará na decadência do direito de recorrer da decisão.

9.5. O recurso contra decisão do pregoeiro terá efeito suspensivo.

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

9.7. Não serão conhecidos os recursos interpostos após os respectivos prazos legais, bem como os encaminhados por endereçamento postal, correio eletrônico (e-mail) ou em desacordo com o estabelecido nos itens 9.2. e 9.3. deste edital.

9.8. Decididos os recursos e constatada a regularidade dos atos praticados, a autoridade superior adjudicará e homologará o processo licitatório e determinará a convocação das adjudicadas para a assinatura do contrato e retirada da ordem de início de serviços.

10. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

10.1. O objeto da licitação será adjudicado e homologado ao licitante declarado vencedor, por ato da Autoridade Superior da Universidade Municipal de São Caetano do Sul.

11. DA CONTRATAÇÃO

11.1. O instrumento contratual resultante desse processo licitatório 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

11.2. Após a homologação do certame, o proponente vencedor será convocado para assinar o instrumento contratual no prazo de 05 (cinco) dias úteis, em conformidade com a minuta apresentada na forma do Anexo XVI, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas na Lei 14.133/2021, no edital e outras legislações aplicáveis;

11.2.1. O prazo de convocação poderá ser prorrogado uma vez, por igual período, mediante solicitação da parte durante seu transcurso, devidamente justificado e, desde que aceito pela contratante;

11.3. Na hipótese de o vencedor da licitação não assinar o contrato ou manifestar a recusa no recebimento da nota de empenho, no prazo e nas condições estabelecidas, sem prejuízo da aplicação das sanções previstas na Lei 14.133/2021, no edital e em outras legislações aplicáveis, será facultado à Administração convocar os licitantes remanescentes, na ordem de classificação, para apresentar os documentos de habilitação nos termos definidos neste edital para celebrar a contratação, nas condições definidas em proposta pelo licitante vencedor;

11.4. Antes de formalizar a contratação ou prorrogar o prazo de vigência do contrato, a Administração deverá além de verificar a regularidade fiscal e trabalhista do contratado, consultar o Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), Cadastro Nacional de Empresas Punidas (CNEP) e o Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa e Inelegibilidade (CNIA CNJ), emitir as certidões negativas de inidoneidade, de impedimento e de débitos trabalhistas e juntá-las ao respectivo processo;

11.4.1. Se o adjudicatário incorrer nas penalidades do artigo 156, incisos III e IV da Lei 14.133/21, ficará impedido de contratar com a Administração;

11.5. Se, por ocasião da formalização do contrato, a prova de regularidade para com a Fazenda Federal (através da Certidão Conjunta Negativa de Débitos relativos a Tributos Federais e à Dívida Ativa da União nos termos da Portaria MF 358/2014 – unificada com a Certidão de Regularidade de Débitos relativos às Contribuições Previdenciárias e às de Terceiros) e a prova de regularidade para com o Fundo de Garantia por Tempo de Serviço, através do Certificado de Regularidade do FGTS (CRF) ou do documento denominado "Situação de Regularidade do Empregador", estiverem com os prazos de validade vencidos, a USCS verificará a situação por meio eletrônico hábil de informações, certificando nos autos do processo a regularidade e anexando os documentos passíveis de obtenção por tais meios, salvo impossibilidade devidamente justificada;

11.5.1. Havendo a impossibilidade da obtenção dos documentos por meio eletrônico, será a adjudicatária notificada para que providencie o envio da documentação sob pena de decair o direito ao fornecimento, sem prejuízo das sanções previstas no artigo 156 da Lei Federal 14.133/21;

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

11.7. Quando do recebimento do instrumento contratual, o adjudicatário deverá também assinar o termo de Ciência e Notificação;

11.8. A Universidade Municipal de São Caetano do Sul providenciará a publicação do instrumento contratual, resultante deste processo licitatório no Portal Nacional de Contratações Públicas (PNCP) e de seus eventuais termos aditivos na forma prevista no artigo 94 da Lei 14.133/2021.

12. DOS PRAZOS PARA ENTREGA E EXECUÇÃO DOS SERVIÇOS

12.1. A Contratada deverá cumprir os seguintes prazos para a perfeita execução do instrumento contratual a ser celebrado com a Universidade Municipal de São Caetano do Sul:

12.1.1. A Contratada deverá cumprir o prazo estipulado de até 45 dias para fornecimento dos equipamentos switch de acesso tipos 1, 2 e 3, bem como os equipamentos descritos como pontos de acesso tipos 1, 2, 3, 4 e 5, ambos *as a service*, contendo em todos os bens entregues na sede da Universidade USCS (Campus Barcelona ao gestor designado) a indicação de registro patrimonial da proponente Contratada, cujo prazo de entrega será contado nos termos do subitem 12.2 do edital.

12.1.2. Em relação a etapa de implementação que se ancora nas atividades de instalação, configuração e ativação física dos equipamentos, quantificados e especificados sob o crivo técnico no Termo de referência do edital, a Contratada terá prazo de até 45 dias para sua finalização, portanto, o proponente deverá considerar 90 dias como prazo máximo para a disponibilização completa da solução objeto do certame, incluindo-se nesse intervalo temporal os aspectos ligados à infraestrutura do projeto, contados nos termos do subitem 12.2. do instrumento convocatório.

12.1.3. A empresa quando da entrega física dos equipamentos, deverá elaborar plano de implementação junto a Universidade USCS (cronograma), cujo documento deverá conter a distribuição dos equipamentos nas unidades da USCS que integrarão o projeto, obedecendo ao mapa que contém a localização de cada ponto de acesso e switch nas respectivas unidades (Anexo XV), topologia física e lógica, bem como o quadro de pessoal alocado na tarefa e os respectivos papeis assumidos por cda membro da equipe, aderente às exigências técnica/tecnológicas aportadas no Termo de Referência do Edital.

12.1.4. O cronograma de execução, deverá indicar de modo percentual a distribuição e execução dos serviços, considerando-se o dimensionamento e as respectivas unidades da Universidade USCS que integram o projeto, estabelecido no termo de referência do edital (item "**a**")

12.2. Caso a ordem de serviço seja enviada por correspondência eletrônica, o prazo para entrega dos equipamentos *as a service*, instalação e configuração da solução contratada, independente do recebimento, inicia-se 24 (vinte e quatro) horas após sua expedição, ressaltando-se que o prazo deve iniciar em dia útil.

12.3. Concluído a fase de estruturação, que contempla a disponibilização física de equipamentos *as a service* e implementação da solução, com escopo definido a partir das especificações contidas no termo de referência do edital, o gestor do contrato designado pela USCS terá o prazo máximo de até 10(dez) dias para conferência, validação e emissão do **TERMO DE ACEITAÇÃO**.

12.3.1. Em particular, no que concerne a entrega e implantação dos equipamentos *as a service*, bem como os serviços de instalação e configuração, dar-se-ão de modo parcial, de acordo com o cronograma a ser definido entre a Contratada e a Gestão do instrumento de contrato da Universidade USCS. Portanto, o **termo de aceitação** e consequentemente pagamento por essa etapa de infraestrutura será gradual, do mesmo modo, a ativação dos serviços decorrentes de tal implantação (suporte técnico, parametrização e monitoramento).

12.4. Quanto ao início dos serviços de suporte técnico, serviços de monitoramento e segurança, serão computados para efeito de pagamento na data constante do termo de aceitação emitida pela gestão do instrumento de contrato da Universidade USCS, respeitando-se a condição (*pró-rata - no sentido de proporcionalidade*) disposta no subitem 12.1.4. e seguintes para o primeiro pagamento, caso não se inicie no primeiro dia do mês.

***Importante*:** Reunião inicial para definição de cronograma do projeto - após o envio da ordem de serviços, será agendada uma reunião no prazo de até 05 dias pelo gestor designado para o acompanhamento do contrato, onde será discutido os parâmetros e variáveis a serem consideradas na elaboração do **Cronograma** de execução de serviços para que sejam

cumpridos os prazos supracitados. Dessa reunião será lavrada em Ata circunstanciada que deverá ser acostada ao processo de compras 873/2025.

13. DA VIGÊNCIA DO CONTRATO

13.1. A Universidade Municipal de São Caetano do Sul firmará contrato resultante deste processo licitatório para fornecer Solução de Serviço Gerenciado para Gestão ativos de rede WiFi, monitoramento e segurança, incluindo fornecimento de softwares, equipamentos, licenciamentos *as a Service*, bem como suporte técnico especializado e garantias, por prazo de 24 (vinte e quatro) meses consecutivos e ininterruptos, contados a partir do recebimento da ordem de serviços, conforme disposto no subitem 12.2., podendo ser prorrogado por igual período, de comum acordo, desde que devidamente justificado e manifestado com antecedência mínima de 60 (sessenta) dias antes do seu término, estendendo-se até o limite máximo de 120 meses, nos termos do artigo 107, da Lei Federal 14.133/2021.

13.2. No caso de prorrogação será lavrado o respectivo termo.

14. DO FATURAMENTO E DO PAGAMENTO

14.1. A empresa contratada, quando da disponibilização dos equipamentos e execução dos serviços instalação, configuração e ativação conforme descritos no termo de referência, deverá comunicar por escrito o evento e emitir as respectivas notas fiscais, encaminhando-as ao fiscalizador técnico designado para o contrato para averiguação e emissão dos respectivos termos e posterior liberação dos pagamentos correspondentes.

14.1.1. Para efeito de pagamento, particularmente no que concerne a etapa de infraestruturação, que compreende, contudo, não se limita a execução dos serviços de instalação, configuração e ativação dos equipamentos, obrigatoriamente, deverá ser respeitado a condição definida no subitem 12.3.1. deste edital.

14.1.2. O pagamento destinado à etapa de implementação será efetuado à Contratada em uma única parcela, no prazo até 10 (dez) dias uteis, contados do primeiro dia seguinte ao recebimento do Termo de Aceitação juntamente com a documentação fiscal completa (nota fiscal e demais documentos exigíveis), pelo setor de contas a pagar da Universidade USCS.

14.2. **Faturamento mensal**

14.2.1. A empresa Contratada emitirá uma nota fiscal mensal discriminando os serviços de gerenciamento de solução para gestão de ativos de rede WiFi, monitoramento e segurança, incluindo fornecimento as a service de software, equipamentos e licenciamentos, além do suporte técnico especializado, acessórioas e garantias para switchs e pontos de acesso, no último dia útil do mês de prestação desses serviços, encaminhando-a ao gestor/fiscalizador do contrato, que deverá, no máximo no próximo dia útil efetuar a conferência, liberação e encaminhamento ao setor de contas a pagar da Universidade USCS.

14.2.2. O pagamento do serviço mensal será efetuado regularmente na 2ª (segunda) terça-feira do mês subsequente ao início dos serviços, desde que a nota fiscal e **Termo de liberação de pagamento** emitido pelo gestor/fiscalizador do contrato seja encaminhado ao setor de contas a pagar da USCS no prazo mencionado no subitem 14.2.1.

14.2.3. Para efeito de pagamento no primeiro período (mês), dar-se-á embasado no termo de aceite do Gestor do instrumento contratual e, será proporcional ao número de dias efetivos da prestação dos serviços contratados.

14.3. Caso o término da contagem aconteça em dias sem expediente bancário, o pagamento ocorrerá no primeiro dia útil imediatamente subsequente.

14.4. A Universidade USCS poderá exigir a comprovação de quitação das obrigações trabalhistas vencidas relativas ao contrato, de acordo com disposto no § 3º do artigo 121 da Lei 14.133/2021 como condição para liberação de pagamento.

14.5. Havendo divergência ou erro na emissão da documentação fiscal, será interrompida a contagem do prazo para fins de pagamento, sendo iniciada contagem somente após a regularização da documentação fiscal.

14.5.1. Constatado a situação de irregularidade, o contratado será notificado formalmente, para que, no prazo de até 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da USCS.

14.6. A permanência da condição de irregularidade, sem a devida justificativa ou com justificativa não aceita pela USCS, poderá culminar em rescisão contratual, sem prejuízo da apuração de

responsabilidade e da aplicação de penalidades fixadas no item 17 deste edital, observado o contraditório e a ampla defesa.

14.6.1. Eventualmente, em caso de atraso pela USCS no pagamento pelos serviços executados, desde que a empresa contratada não tenha concorrido de alguma forma para tanto, o valor devido deverá ser acrescido de encargos moratórios proporcionais aos dias de atraso, apurados desde a data limite prevista para opagamento até a data do efetivo pagamento, à taxa de 6% (seis por cento) ao ano, aplicando-se a seguinte fórmula:

EM = I x N x VP

EM = Encargos Moratórios a serem acrescidos ao valor originalmente devido

I = Índice de atualização financeira, calculado segundo a fórmula:

I = (6 / 100) / 365

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

VP = Valor atualizado da parcela em atraso.

14.6.1.1. Em caso de atraso superior a 30 dias do vencimento, o valor principal será atualizado monetariamente pelo índice IPCA do último mês, anterior à data limite, divulgado pelo IBGE.

14.6.1.2. Para efeito de aplicação dos itens imediatamente acima, a empresa contratada deverá apresentar solicitação expressa e formal, ocasião em que se realizará a análise e negociação com a USCS.

14.7. A Universidade USCS emitirá ordem de pagamento a crédito em conta bancária em nome do credor, que poderá ser indicada na "Proposta Comercial", ficando terminantemente vedada a negociação da duplicata mercantil na rede bancária ou com terceiros.

14.8. Independente do percentual de tributo inserido na planilha que define a proposta comercial, quando houver, serão retidos na fonte, na realização do pagamento, os percentuais estabelecidos na legislação vigente.

15. DAS RESPONSABILIDADES E OBRIGAÇÕES DA CONTRATADA

15.1. No cumprimento deste edital, a licitante obrigar-se-á:

15.1.1. Executar o objeto do certame sob sua inteira responsabilidade, rigorosamente de acordo com as especificações contidas nos anexos I, II e XV. É salutar reafirmar que a Contratante não aceitará fornecimento de serviço ou equipamentos físicos ou ainda softwares e garantias, diferentes daqueles dispostos no Termo de Referência deste edital.

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

15.1.3. Responsabilizar pelo fornecimento dos bens e execução dos serviços objeto da licitação, cabendo ao seu representante na condição de preposto acompanhar o cumprimento rigoroso dos prazos, organização de reuniões, entrega de documentos, elaboração de relatórios de acompanhamento e quaisquer atividades pertinentes à execução dos serviços.

15.1.4. Registrar as ocorrências havidas durante a execução do objeto dando ciência a Universidade Municipal de São Caetano do Sul, respondendo integralmente por sua omissão.

15.1.5. Manter durante a execução do objeto, todas as condições de habilitação e qualificação exigidas no processo licitatório.

15.1.6. Prestar os serviços sempre por pessoal qualificado, respondendo perante a USCS e a terceiros por todos os ônus, encargos, perdas e/ou danos porventura resultantes da execução do objeto da prestação de serviços.

15.1.7. Providenciar e custear pessoal habilitado em quantidade necessária para a execução dos serviços até o cumprimento integral do contrato.

15.1.8. Providenciar e custear os recursos computacionais (hardware, software e demais elementos de ordem computacional), quando couber, utilizados por sua equipe de suporte técnico, monitoramente e de segurança relacionado ao gerenciamento da solução de gestão de ativos de rede, no desempenho de suas funções exigidas via celebração de contrato.

15.1.9. Manter equipe de profissionais treinados nas melhores práticas e tecnologias existentes no mercado de cibersegurança.

15.1.10. Não reproduzir, divulgar ou utilizar em benefício próprio, ou de terceiros, quaisquer dados ou informação de que tenha tomado ciência em razão da execução dos serviços discriminados neste instrumento, sem o consentimento, prévio e formal da Universidade USCS.

15.1.11. A Universidade USCS não assumirá nenhuma responsabilidade pelo pagamento de impostos e outros encargos que competirem à Contratada, nem se obrigará a fazer a essa qualquer restituição ou reembolso de quantias ou acessórios que a mesma despender com esses pagamentos.

15.1.12. A licitante contratada poderá realizar subcontratação parcial do objeto (atividades relacionadas somente a etapa de infraestrutura), desde que tal subcontratação não diga respeito à atividade fim do objeto do certame, conforme disposto no artigo 122 da Lei 14.133/2021, contudo, sua efetiva realização deverá ser devidamente justificada e precedida expressamente de autorização da Universidade Municipal de São Caetano do Sul.

15.1.13. A subcontratação dos serviços, será de inteira responsabilidade da licitante que será contratada e deverá seguir as condições e especificações delimitadas para o objeto no termo de referência deste edital.

15.1.14. Para efeito da respectiva subcontratação, a licitante apresentará à administração documentação que comprove capacitação técnica do subcontratado, que deverá ser avaliada e acostada aos autos do processo.

16. DA FISCALIZAÇÃO E SUPERVISÃO

16.1. Não obstante ser a Contratada a única e exclusiva responsável, inclusive perante terceiros, pela execução do objeto do contrato, reserva-se à Universidade Municipal de São Caetano do Sul o direito de, sem que de qualquer forma restrinja a plenitude da responsabilidade da Contratada, exercer a mais ampla fiscalização para a consecução do objeto.

17. DAS SANÇÕES ADMINISTRATIVAS E PENALIDADES

17.1. Comete infração administrativa, nos termos da Lei Federal 14.133/2021, a proponente vencedora do certame e/ou contratada que der causa à inexecução parcial ou total do contrato; ensejar o retardamento da execução do instrumento; apresentar documentação falsa ou praticar ato fraudulento durante a execução do contrato; comportar-se de modo inidôneo ou cometer fraude de qualquer natureza; praticar ato lesivo previsto no artigo 5º da Lei Federal 12.846/2013.

17.1.1. As empresas que cometerem as infrações dispostas no item 17.1, estarão sujeitas a aplicação de advertência formal, impedimento de licitar e contratar com a administração pública, ser declarada inidônea para licitar e contratar, além da aplicação de multas reparatórias e/ou moratórias, conforme o caso.

17.1.2. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Universidade USCS, bem como não impede essa administração de se utilizar cumulativamente da aplicação das sanções com as multas previstas.

17.2. A recusa injustificada da adjudicatária em aceitar ou retirar o termo de contrato, no prazo e nas condições estabelecidas caracterizará descumprimento total da obrigação assumida, sujeitando-o a juízo da Administração, nos termos, inclusive, da legislação municipal:

a) À multa de 30% (trinta por cento) sobre o valor do contrato;

b) Ao pagamento correspondente à diferença de preço decorrente de nova licitação ou contratação, para o mesmo fim;

17.2.1. O disposto no subitem 17.2. não se aplicará aos licitantes remanescentes quando convocados nos termos do subitem 11.3. deste edital.

17.3. Pela inexecução total do contrato, será aplicada à Contratada a multa de 30% (trinta por cento) sobre o valor total do ajuste;

17.4. Pela inexecução parcial do contrato, será aplicada à Contratada a multa de 20% (vinte por cento) sobre o valor da obrigação não cumprida.

17.5. Pelo atraso injustificado a Contratada incorrerá em multa diária de 0,5% (cinco décimos por cento) sobre o valor do contrato, excluída, quando for o caso, parcela correspondente aos impostos incidentes, quando destacados no documento fiscal, sendo que a aplicação da multa terá início no primeiro dia seguinte ao término do prazo contratual do serviço.

17.5.1. Os atrasos injustificados superiores a 30 (trinta) dias corridos serão obrigatoriamente considerados inexecução total ou parcial, estando a Contratada sujeita as sanções previstas nos subitens 17.3 ou 17.4.

17.6. Além das multas e das penalidades aqui contidas, poderão ser aplicadas à Contratada, sanções decorrentes do não cumprimento das condições estabelecidas pelo ***Service Level Agreement*** que integra o Termo de Referência do edital, item 11 e seguintes, conforme verificação e enquadramento do Gestor do instrumento de contrato designado pela USCS.

17.7. As multas a que aludem os subitens anteriores não impedem que a Administração rescinda unilateralmente o contrato e aplique outras sanções previstas nas Leis Federais e Municipais, a saber:

17.7.1. Advertência, por escrito, no caso de pequenas irregularidades.

17.7.1.1. A sanção de advertência poderá ser aplicada nos seguintes casos:

I. Descumprimento das determinações necessárias à regularização das faltas ou defeitos observados na prestação dos serviços;

II. Outras ocorrências que possam acarretar transtornos no desenvolvimento dos serviços da USCS, desde que não caiba a aplicação de sanção mais grave.

17.7.2. Suspensão temporária do direito de licitar e impedimento de contratar com a Administração, pelo prazo de até três anos, quando da inexecução contratual sobrevier prejuízo para a Administração;

17.7.2.1. A penalidade de suspensão será cabível quando o licitante participar do certame e for verificada a existência de fatos que o impeçam de contratar com a Administração Pública. Caberá ainda a suspensão quando a licitante, por descumprimento de cláusula contratual tenha causado transtornos no desenvolvimento dos serviços da USCS.

17.7.3. 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.

17.7.3.1. Se o licitante deixar de entregar a documentação ou apresenta-la falsamente, ensejar 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 cinco anos, impedido de contratar com a Administração Pública, sem prejuízo das multas previstas no edital e das demais cominações legais.

17.7.4. Verificado que a obrigação foi cumprida com atraso injustificado caracterizando a inexecução parcial, a USCS poderá reter preventivamente, o valor da multa dos eventuais créditos que a Contratada tenha direito, até a decisão definitiva, assegurada a ampla defesa.

17.7.4.1. Se a USCS decidir pela não aplicação da multa, o valor retido será devolvido à Contratada.

17.8. Os atos previstos como infrações administrativas na Lei Federal nº 14.133/2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei Federal 12.846/2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei.

17.9. Independentemente das sanções retro, a Contratada ficará sujeita ainda, à composição das perdas e danos causados à Administração, decorrentes de sua inadimplência, bem como arcará com a correspondente diferença de preços verificada em nova contratação, na hipótese de os demais classificados não aceitarem a contratação pelos mesmos preços e prazos fixados pelo inadimplente.

17.10. A personalidade jurídica da empresa vencedora poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Edital para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com a empresa vencedora.

17.11. É assegurada nos termos legais os prazos para exercício do direito da ampla defesa e do contraditório, na aplicação das sanções previstas no escopo dos artigos 155 a 162 da Lei 14.133/2021, conforme o caso.

18. DO REAJUSTE DE PREÇOS

18.1. Os valores constantes da proposta e expressos em reais concernentes à solução de serviço gerenciado para gestão ativos de rede WiFi, monitoramento e segurança, incluindo fornecimento de softwares, equipamentos, licenciamentos *as a service*, bem como suporte técnico especializado, acessórios e garantias, poderão sofrer reajustes somente após o interregno de 12 meses, contados nos termos previstos no subitem 12.3. e seguintes deste edital.

18.2. Na hipótese de manutenção do contrato, transcorridos os primeiros 12 meses, poderão ser reajustados partir do 13º (décimo terceiro) mês, de acordo com a variação do Índice Nacional de Preços ao Consumidor Amplo – IPCA/IBGE, conforme legislação em vigor ou por outro índice que venha substituí-lo.

18.3. O reajuste poderá ser concedido mediante expressa solicitação da Contratada, para análise e negociação com a USCS, e terá incidência de pagamento respeitando-se as condições e períodos estabelecidos no item 18.1.

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

19. DA GESTÃO DO CONTRATO

19.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei 14.133/2021, e cada parte responderá pelas consequências de sua inexecução.

19.2. O agente público designado para assumir a função de Gestor do instrumento contratual resultante deste processo licitatório será o responsável pela Diretoria de Tecnologia da Informação e Inovação, cujas atribuições lhes permitirá ainda estabelecer o(s) fiscalizadores técnicos. Os designados serão responsáveis pelo acompanhamento e execução do termo contratual objeto do presente certame, procedendo, de acordo com suas competências, ao registro das ocorrências e adotando as providências necessárias ao fiel cumprimento do ajuste, bem como, responsabilizar-se-ão pela vigência, com o consequente controle dos prazos de início e término contratual, eventual prorrogação, aditamentos e instauração de novo processo de licitação quando couber.

19.3. O fiscal técnico do contrato anotarão para efeito de histórico de gerenciamento, todas as ocorrências relacionadas à sua execução, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. Identificada quaisquer irregularidades, este emitirá notificação, indicando o prazo para correção em sua execução.

19.4. O fiscal técnico comunicarão ao gestor desse instrumento, em prazo não inferior a 60 (sessenta) dias do término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

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

19.6. O gestor do contrato deverá coordenar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

19.7. O gestor tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido por comissão, ou, pelo departamento competente para tal, em conformidade ao disposto no artigo 158 da Lei 14.133/2021.

19.8. O gestor deverá elaborar relatório final contendo informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades relativas à administração e execução contratual.

20. DA DOTAÇÃO ORÇAMENTÁRIA

20.1. As despesas decorrentes da contratação, objeto deste processo licitatório, correrão à conta dos recursos consignados no orçamento da Contratante, em conformidade com o disposto no parágrafo 2º do artigo 12 da Lei nº. 10.320, de 16 de dezembro de 1968, de acordo com a dotação orçamentária.

20.2. No tocante à classificação das despesas Orçamentárias pertinentes a este certame é conjecturada a de número 12.364.1500.2.100.3.3.90.40.00.

21. DA GARANTIA CONTRATUAL

21.1. A licitante declarada vencedora, em até 10(dez) dias úteis contados da assinatura do contrato, deverá fazer prova de recolhimento, a título de garantia de execução do contrato, equivalente a

5% (cinco por cento) do valor total pactuado, com vencimento para 60 (sessenta) dias após a data da entrega final dos serviços, correspondente a data da última parcela a ser paga pela Universidade Municipal de São Caetano do Sul, cabendo à Contratada optar por quaisquer modalidades assecuratórias previstas no parágrafo 1º do artigo 96 da Lei Federal 14.133/2021.

21.1.1. A garantia quando prestada nas modalidades fiança bancária e seguro garantia, deverá prever a cobertura de indenizações decorrentes de responsabilização da **Tomadora** dos serviços por obrigações assumidas pela Contratada, inclusive às concernentes aos encargos trabalhistas, previdenciários, fiscais e comerciais, nos termo deste contrato.

21.1.2. Na hipótese de o contratado optar pela modalidade de garantia inscrita no inciso II do parágrafo 1º do artigo 96 (Lei 14.133/2021), o prazo para prestação de garantia será assegurado nos termos do § 3º do mesmo artigo da mesma Lei, contudo, sua aplicação dar-se-á subsidiariamente ao contido no item 21.1 deste edital .

21.2. Na hipótese de evidenciar qualquer impropriedade ou incorporação, a Contratante exigirá sua regularização ou substituição no prazo de 5(cinco) dias úteis da data de intimação.

21.3. A falta de atendimento à convocação para regularização ou substituição da garantia na forma e prazo especificado no item 21.2. acima, sujeitará a Contratada às seguintes consequências:

a) Retenção dos pagamentos que lhe sejam devidos, para recomposição da garantia contratual, na modalidade caução em dinheiro; ou

b) Caracterização de inexecução contratual, ensejando a consequente aplicação de penalidade prevista na item 17 deste documento e, ainda, a rescisão do ajuste com fundamento nos incisos do artigo 155 da Lei Federal nº 14.133/2021.

21.3.1. Caberá a Contratante decidir motivadamente entre a retenção de pagamentos para recomposição da garantia contratual ou a caracterização da inexecução contratual.

21.4. A correção monetária da garantia prestada na forma de caução em dinheiro será calculada com base na variação do índice IPCA/IBGE e, no caso de utilização de cheque, a data inicial da correção será a do crédito bancário.

22. DA GARANTIA DOS EQUIPAMENTOS

22.1. Os equipamentos *as a service* terão garantia e licenciamento pelo fabricante, conforme mencionado na Proposta Comercial da Contratada, contados do recebimento dos produtos pelo gestor/fiscalizador do contrato.

22.2. Durante o período de vigência do instrumento contratual a Contratada deverá substituir os equipamentos que apresentarem problemas de fabricação ou que denotem não serem novos ou ter sinais de uso anterior.

22.3. A garantia não cobre os danos causados pelo não atendimento das especificações operacionais, negligência ou mau uso dos equipamentos.

22.4. A garantia é intransferível e só beneficia a própria Universidade USCS, como adquirente original dos equipamentos, não compreende a reposição de partes e peças perecíveis e sujeitas ao desgaste natural.

22.5. Estão previstos, nessa garantia, os equipamentos adquiridos, sendo que quando apresentarem problemas, deverão ser consertados ou substituídas no prazo de 5(cinco) dias úteis, com as mesmas características, sem nenhum ônus para a Universidade Municipal de São Caetano do Sul.

23. DAS DISPOSIÇÕES GERAIS

23.1. O presente Edital, seus anexos e a proposta da licitante vencedora integrarão o termo de contrato, independentemente de transcrição.

23.2. Da sessão pública para recebimento, julgamento de proposta de preços, e habilitação documental deste processo licitatório, lavrar-se-á ata circunstanciada, na qual serão registradas as ocorrências relevantes, inclusive os diálogos enunciados por meio da ferramenta do sistema de pregão eletrônico"chat".

23.3. É facultada ao pregoeiro ou autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar ou ter sido providenciado no ato da sessão pública.

23.4. O agente público pregoeiro e a equipe de apoio, se entenderem conveniente ou necessário, poderão se utilizar de assessoramento técnico e jurídico específicos para tomar decisões

relativas ao presente certame licitatório, por meio de documento devidamente formalizado o qual integrará o respectivo processo.

23.5. A proponente que no prazo de validade da proposta de preços não venha a mantê-la, ou convocada para assinar o contrato concernente ao objeto do certame, caso não o faça no prazo estipulado neste edital, perderá a garantia de proposta em favor da Universidade Municipal de São Caetano do Sul, sem prejuízo das demais sanções legais aplicáveis.

23.6. A devolução da garantia de proposta enunciada no item acima, quando prestada nas modalidades previstas nos incisos I e IV do parágrafo primeiro do artigo 96, dar-se-á após a homologação do certame e consequente contratação do objeto.

23.7. A autoridade superior poderá revogar a licitação por razões de interesse público, derivado de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo invalidá-la por ilegalidade, de ofício ou por provocação de qualquer pessoa, mediante ato escrito e fundamentado, sem que caiba direito a qualquer indenização.

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

23.9. Os proponentes assumem todos os custos de preparação e apresentação de sua proposta e a USCS não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

23.10. Os proponentes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.

23.11. O proponente que vier a ser contratado, ficará obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

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

23.13. Na contagem dos prazos estabelecidos neste edital e seus anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na USCS.

23.14. O desatendimento de exigências formais não essenciais não importará no afastamento da licitante, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta, durante a realização da sessão pública de pregão.

23.15. As normas que disciplinam este pregão serão sempre interpretadas em favor da ampliação da disputa entre os interessados, sem comprometimento da segurança do futuro contrato.

23.16. Qualquer pedido de **esclarecimento** em relação a eventuais dúvidas na interpretação deste instrumento convocatório e seus anexos, bem como de cópias da legislação mencionada, devem ser solicitados por meio de documento digitalizado e assinado, inseridos em campo próprio do Portal de Compras da Universidade Municipal de São Caetano do Sul através do link https://pregaoeletronico.saocaetanodosul.sp.gov.br/uscs/ , ou enviado para o e-mail: licitacao@online.uscs.edu.br , ou ainda, podem ser solicitadas por escrito, ao pregoeiro, na Rua Maceió, 177, Bairro Barcelona, São Caetano do Sul/SP – CEP 09551-030, até três dias úteis antes da data marcada para a abertura do certame.

23.16.1. A íntegra da resposta aos esclarecimentos elaborados a partir dos questionamentos será divulgada no sítio eletrônico oficial da Universidade no link https://licitacao.uscs.edu.br/ e no portal de compras, via link https://pregaoeletronico.saocaetanodosul.sp.gov.br/uscs/, no prazo de até três dias úteis, limitado ao último dia útil anterior à data de abertura do certame.

23.17. A participação na presente licitação implica em ciência quanto à obrigação de assinar, juntamente com Contrato o "Termo de Ciência e Notificação" (de acordo com o anexo LC-01, da instrução do TCESP 001/2020), e que o descumprimento poderá gerar penalizações

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

23.19. Para as demais condições de contratação, observar as disposições constantes do Anexo I - Termo de Referência deste Edital.

23.20. Prazo para retirada do contrato ou instrumento equivalente de 05 (cinco) dias úteis.

23.21. Aos casos omissos aplicar-se-ão as demais disposições constantes da Lei Federal número 14.133/2021.

23.22. Para dirimir as questões oriundas deste Edital, não resolvidas na esfera administrativa, é competente o Foro da Comarca de São Caetano do Sul, por mais privilegiado que outro seja.

23.23. Integram o instrumento convocatório, conforme o caso:

ANEXO I TERMO DE REFERÊNCIA.

ANEXO II PROPOSTA COMERCIAL.

ANEXO III REDUÇÃO DE LANCES.

ANEXO IV DECLARAÇÃO DE REGULARIDADE PERANTE O MINISTÉRIO DO TRABALHO.

ANEXO V DECLARAÇÃO DE CUMPRIMENTO DAS CONDIÇÕES DE HABILITAÇÃO.

ANEXO VI DECLARAÇÃO DE ENQUADRAMENTO COMO MICROEMPRESA OU EMPRESA DE PEQUENO PORTE PARA FRUIÇÃO DOS BENEFÍCIOS DA LEI COMPLEMENTAR Nº 123/2006 COM AS DEVIDAS ALTERAÇÕES INTRODUZIDAS PELAS LEIS COMPLEMENTARES FEDERAIS NÚMERS 147/2014 E 155/2016, E LEI MUNICIPAL Nº 4.660/2008.

ANEXO VII DECLARAÇÃO DE ATENDIMENTO ÀS NORMAS RELATIVAS À SAÚDE E SEGURANÇA NO TRABALHO.

ANEXO VIII DECLARAÇÃO DE CONDIÇÕES GERAIS DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS.

ANEXO IX DECLARAÇÃO DE QUE A PROPOSTA ECONÔMICA CONTEMPLA TODOS OS CUSTOS TRABALHISTAS.

ANEXO X DECLARAÇÃO DE CUMPRE OS REQUISITOS DE RESERVA DE CARGOS PARA PESSOAS PORTADORAS DE DEFICIÊNCIA E REABILITADOS DA PREVIDÊNCIA SOCIAL.

ANEXO XI DECLARAÇÃO DE QUALIFICAÇÃO TÉCNICA DOS PROFISSIONAIS QUE SERÃO ALOCADOS NA EXECUÇÃO DO PROJETO.

ANEXO XII DECLARAÇÃO DE CREDENCIADO/REVENDEDOR AUTORIZADO JUNTO AOS FABRICANTES DOS EQUIPAMENTOS.

ANEXO XIII DECLARAÇÃO DEVISITA TÉCNICA.

ANEXO XIV DECLARAÇÃO DE ABSTENÇÃO DE REALIZAÇÃO DE VISITA TÉCNICA.

ANEXO XV LAY OUT E TOPOLOGIA ACERCA SOLUÇÃO PROPOSTA PARA DISTRIBUIÇÃO DOS EQUIPAMENTOS WI-FI.

ANEXO XVI MINUTA DE CONTRATO E TERMO DE CONFIDENCIALIDADE E RESPONSABILIDADE DE PROTEÇÃO DE DADOS PESSOAIS.

ANEXO XVII TERMO DE CIÊNCIA E NOTIFICAÇÃO E DECLARAÇÃO DE DOCUMENTOS À DISPOSIÇÃO DO TRIBUNAL DE CONTAS DO ESTADO - LC-01; LC-02 e PC 02.

ANEXO XVIII ESTUDO TÉCNICO PRELIMINAR

ANEXO XIX PLANO DE GESTÃO DE RISCO.

São Caetano do Sul, 04 de dezembro de 2025.

_____

Prof. Ms. Orlando Antônio Bonfatti
Pró-Reitor Administrativo e Financeiro

ANEXO I

TERMO DE REFERÊNCIA
Pregão Eletrônico nº 27/2025
Processo de Compras nº 873/2025

OBJETO

O presente Termo de Referência tem como objetivo a contratação de empresa especializada para fornecr solução de serviço gerenciado para gestão de ativos de rede WiFi, monitoramento e segurança, incluindo fornecimento de softwares, equipamentos e licenciamentos na modalidade *As a Service*, suporte técnico especializado, acessórios e garantias para atendimento da Universidade Municipal de São Caetano do Sul da Universidade Municipal de São Caetano do Sul, considerando o acesso simultâneo de 10.000 usuários conectados à rede WiFi.

A solução é destinada ao atendimento dos colaboradores, discentes e docentes, bem como toda comunidade que utiliza os serviços da USCS, e deverá ser implementada nas seguintes unidades:

a) Unidades da Universidade USCS que integram o projeto:

1. Unidade Campus Barcelona: Avenida Goiás, 3400, Barcelona, São Caetano do Sul/SP, CEP 09550-051
2. Unidade Campus Centro: Rua Santo Antônio, 50, Centro, São Caetano do Sul/SP, CEP 09521-160
3. Unidade Campus Centro II: Rua Samuel Klein, 83, Centro, São Caetano do Sul, CEP 09510-125
4. Unidade Campus Conceição: Rua Conceição, 321, Santo Antônio, São Caetano do Sul, CEP 09530-060
5. Unidade Campus Itapetininga: Avenida Doutor Ciro Albuquerque, 4750 - Taboãozinho, Itapetininga/SP, CEP 18200-021

PARÂMETROS GERAIS, DESCRIÇÃO DA SOLUÇÃO E REQUESITOS DA CONTRATAÇÃO

A contratação em tela tem objetivo de atualizar o parque tecnológico da USCS, tornando compatível com a atual necessidade da Instituição, notadamente em relação ao atendimento qualificado aos seus usuários. A Universidade USCS, encontra-se em plena expansão de acordo com seu Planejamento Estratégico, tendo em registrado expressivo crescimento em sua estrutura física e sua capacidade de atendimento a comunidade. Desta forma, essa contratação é primordial para que a Universidade possa gerir e sustentar seus serviços que demandem conectividade. Neste sentido, há a necessidade de manter e racionalizar a infraestrutura de rede adequada, com a devida capacidade e com serviços de garantia e suporte técnico vigentes, suportando a atual demanda e sua projeção de crescimento futuro.

A solução prevê a disponibilização de equipamentos e tecnologias de última geração, conforme requisitos e quantitativos a seguir apresentados, devendo todos serem licenciados de modo a garantir o seu funcionamento adequado, bem como a segurança das aplicações da USCS e o suporte contínuo.

A solução está composta em diferentes itens e subitens, agrupados em um lote único. A composição em lote único atende melhor aos interesses da Universidade, a medida em que assegura maior interoperabilidade entre os equipamentos e consequentemente uma melhor gestão dos ativos e do próprio contrato.

No escopo desse projeto, essa administração tem a pretensão de contratar no mercado empresa com expertise para fornecer solução de serviço gerenciado de ativos de rede WiFi, baseada em equipamentos licenciados de switch e ponto de acesso *as a service*, integrada a prestação de serviços de suporte técnico especializado no formato 24x7, segurança e monitoramento, por período de 24 meses.

Considerando-se as particularidades inerentes ao processo de contratação de serviços tecnológicos, será necessário estabelecer reunião inicial de projeto (*kick off*) tão logo seja celebrado o instrumento de contrato resultante desse processo de compras. Após envio da ordem de serviços, essa administração agendará a reunião, onde será discutido os aspectos relativos ao cronograma de execução dos serviços contratados, em particular, questões relacionadas a etapa de implementação da solução.

Deverão ser apresentados durante a fase de julgamento da proposta, a documentação oficial (quickspec ou datasheet) contendo as especificações técnicas dos equipamentos *as a service*, licenciamento e serviços que compõem a solução ofertada, inclusive no que se refere as certificações e homologações

necessárias à consecução do projeto e demais itens que compõe a solução, para permitir a consistente avaliação de todos os itens ofertados.

A solução deve contemplar o serviço técnico especializado e monitoramento da infraestrutura de tecnologia, para atender o seguinte escopo:

O serviço de suporte operacional especializado deverá ser disponibilizado para apoiar as necessidades oriundas dos objetos dos itens deste documento, podendo ser realizado de forma presencial e/ou remota e deverá ter as seguintes características:

- Trabalhar em estreita colaboração com Diretoria de Tecnologia da Informação e Inovação, como equipes de suporte técnico, analistas de rede e equipes de segurança cibernética, para resolver problemas complexos, implementar mudanças e melhorias na infraestrutura de rede da Universidade;
- Acompanhar o monitoramento de rede e da controladora, receber alertas e notificações de problemas de rede, como interrupções de serviço e quedas de conexão. Investigar e resolver esses alertas/notificações, garantindo o mínimo de tempo de inatividade e impacto nos serviços;
- Realizar verificações regulares de rotina, atualizações de firmware, instalação de patches de segurança e outras atividades para manter a rede em bom estado de funcionamento;
- Avaliar novas funcionalidades e sugerir ajustes que possam melhorar a eficiência e a segurança da rede;
- Realizar novas instalações, configurações, suporte técnico, manutenções preventivas e corretivas dos equipamentos e softwares (switches, ponto de acesso WiFi e controladoras);
- Reportar e elaborar notas técnicas sobre problemas graves para a Diretoria de Tecnologia da Informação e Inovação quando solicitado;
- Criação e acompanhamento no preenchimento de Requisição de Mudança (RDM) na infraestrutura de rede, segundo os procedimentos de gerenciamento de mudanças estabelecidos pela USCS. Isso envolve a análise de impacto, planejamento, execução e documentação das alterações realizadas;
- Monitorar e garantir que os NMS (Níveis Mínimos de Serviços) sejam cumpridos;
- Colaborar com equipes de projeto para implementar novas soluções de rede, como expansões, migrações ou atualizações tecnológicas de acordo com as demandas da USCS.

Necessidades de Negócio

- Continuidade dos serviços de TIC: Prover o aporte tecnológico necessário, para a implantação e a sustentação dos sistemas Institucionais, em consonância com a arquitetura tecnológica computacional.
- Conformidade: Alinhamento às boas práticas e condições de mercado para assegurar um ambiente tecnológico compatível.
- Manutenção e sustentabilidade: Prover e atualizar continuamente os recursos e ferramentas de Tecnologia da Informação.
- Garantia e suporte: Manter o parque atualizado com garantia e suporte às aplicações
- Segurança e privacidade: Prover mecanismos de segurança, compatível com a camada em que esses equipamentos se enquadram, visando a conferir confidencialidade, integridade e disponibilidade dos dados trafegados nos equipamentos de tecnologia.
- A Contratada deverá declarar que possui certificados do fabricante, comprovando que os produtos possuem a garantia solicitada neste termo de referência.

Necessidades Tecnológicas - Governança

- Alta disponibilidade: Fornecimento de infraestrutura tecnológica com certa redundância de ativos computacionais, constituindo serviços/sistemas mais resilientes e tolerantes a determinadas falhas em equipamentos e componentes de tecnologia da informação.
- Mitigação de riscos relativos à mudança e migração: Capacidade de migração das cargas de processamento da infraestrutura atual para a nova com riscos mitigados quanto à continuidade das operações e disponibilidade.
- Gerenciamento e monitoração: Capacidade de acompanhar, metrificar e realizar atividades em ativos e componentes computacionais por meio de interfaces de gerenciamento, que permitam o monitoramento o uso e a capacidade disponível de tais equipamentos.

- Escalabilidade e flexibilidade: Capacidade da solução ser adaptável, fornecendo infraestrutura para que os sistemas/serviços abrigados consigam ser expandidos, visando a atender, da melhor forma, às necessidades organizacionais.
- Auditoria e controle: Fornecer maneiras de controle e auditoria, compatível com a camada em que esses equipamento0s de tecnologia da informação se enquadram, visando a propiciar registros de acessos, definir papéis e suas respectivos privilégios e demais funcionalidades empregadas para se permitir o rastreio e controle de usuários.
- Atualização tecnológica: Capacidade de oferecer o aporte tecnológico necessário para a implantação de novos serviços, em consonância com as novas tecnologias disponíveis no mercado.

NecessidadesTtecnológicas - Requisitos técnicos esperados

- As especificações técnicas mínimas apuradas para o atendimento às necessidades do projeto, encontram-se descritas no tópico “Especificações Técnicas Mínimas da Solução”.
- O proponente deve declarar que é parceiro oficial ou que é revendedor autorizado pelo fabricante do equipamento ofertado.

TIPOLOGIA ACERCA DAS ESPECIFICAÇÕES E EXIGÊNCIAS APLICADAS AO PROJETO

A empresa a ser contratada será responsável pela aquisição, entrega, implementação (instalação e configuração) e licenciamento de todos os equipamentos *as a service* necessários e descritos no quadro a seguir desse documento. Ressalte-se que a Universidade Municipal de São Caetano do Sul, no âmbito desta contratação, não aceitará a entrega de hardwares e/ou softwares que não contemplem plenamente as especificações elencadas neste termo de referência.

Todos os equipamentos deverão ser entregues ao gestor designado para acompanhamento do contrato de prestação de serviço resultante desse processo licitatório, na sede da Universidade USCS, Campus Barcelona.

Item	Descrição	Qtde de Equipamento	Métrica	Quantidade
1	**Serviço gerenciado de solução para gestão ativos de rede, monitoramento e segurança, incluindo fornecimento de softwares, equipamentos, licenciamentos, suporte técnico especializado, acessórios e garantia.**			
1.1	**Serviço gerenciado de Switch, incluindo fornecimento de equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.**			
1.1.1	Switch de acesso tipo 1, *As a Service*, incluindo equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.	28	Meses	24
1.1.2	Switch de acesso tipo 2, *As a Service*, incluindo equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.	2	Meses	24
1.1.3	Switch de acesso tipo 3, *As a Service*, incluindo equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.	2	Meses	24
1.1.4	Implementação – instalação e configuração física da solução de Switch.	32	Serviço	1
1.2	**Serviço gerenciado de Ponto de Acesso (AP), incluindo fornecimento de equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.**			
1.2.1	Ponto de acesso tipo 1, *As a Service*, incluindo fornecimento de equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.	185	Meses	24
1.2.2	Ponto de acesso tipo 2, *As a Service*, incluindo fornecimento de equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.	12	Meses	24
1.2.3	Ponto de acesso tipo 3, *As a Service*, incluindo fornecimento de equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.	12	Meses	24
1.2.4	Ponto de acesso tipo 4, *As a Service*, incluindo fornecimento de equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.	6	Meses	24

1.2.5	Ponto de acesso tipo 5, *As a Service*, incluindo fornecimento de equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.	4	Meses	24
1.2.6	Implementação – instalação e configuração física da solução de Ponto de Acesso.	219	Serviço	1
1.3	**Serviço gerenciado de solução para gestão de ativos de rede, monitoramento e segurança, incluindo fornecimento de softwares, controladora (SaaS), licenciamento e suporte técnico especializado, acessórios e garantia.**			
1.3.1	Solução para gestão de switches, monitoramento e segurança, incluindo fornecimento de softwares, licenciamento e suporte técnico especializado.	1	Meses	24
1.3.2	Solução para gestão de pontos de acesso, monitoramento e segurança, incluindo fornecimento de softwares, controladora (SaaS), licenciamento e suporte técnico especializado.	1	Meses	24
1.3.3	Instalação, configuração e parametrização da solução para gerenciamento e gestão do parque de ativos de switches e pontos de acessos (251 equipamentos).	251	Serviço	1

Quadroa 01

1. CARACTERISTICAS GERAIS

1.1. As licenças a serem fornecidas para a implementação da solução, deverão estar em nome da USCS, e deverá estar vigente durante todo o período contratual.

1.2. O equipamento deve ser novo, sem uso anterior e o modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação na data de entrega da proposta.

1.3. Deve ser fornecida a versão mais recente (última versão comercial disponível) dos softwares, plataformas, sistemas operacionais e firmwares instalados.

1.4. Os requisitos técnicos devem ser sempre de fornecimento obrigatório, o proponente deverá comprovar através de documentos oficiais do fabricante.

1.5. O licenciamento deve ser unitário, por ativo gerenciado, suportando switches e pontos de acesso WiFi.

1.6. A contratada deverá fornecer todos os acessórios necessários para implantação e funcionamento do serviço contratado.

1.7. Todas as funcionalidades requisitadas nas especificações da solução, incluindo relatórios e informações analíticas, devem estar contempladas nas licenças.

2. SWITCHES COORPORATIVOS - REQUISITOS GERAIS PARA SWITCHES TIPOS 1, 2, e 3:

2.1. Todos os Switches do Lote especificados no presente documento devem ser do mesmo fabricante, compondo uma solução única de rede, para assegurar a compatibilidade funcional de todos os recursos e permitir o gerenciamento unificado.

2.2. Todos os acessórios que serão utilizados na prestação do serviço, tais como cabos de força (padrão ABNT NBR 14136) e cabos de interconexões (DAC/AOC/FIBRAS e etc), assim como transceivers e conversores de mídia deverão estar inclusos na solução.

2.2.1. A contratada a seu critério poderá prover protetores elétricos tais como mecanismos, acessórios e/ou equipamentos de proteção contra quedas, interrupções e distúrbios elétricos, para provimento e continuidade dos serviços do objeto do Anexo I – Termo de ReferênciaA.

2.3. O modelo do equipamento ofertado deve possuir, na data da entrega da proposta, homologação junto à ANATEL com certificado disponível publicamente no endereço eletrônico desta agência reguladora, conforme a Resolução número 242 de 30 de novembro de 2000.

2.4. Esses switches deverão possuir a mesma gerência dos pontos de acesso wifi de maneira centralizada, em ambiente de nuvem como serviço (**SaaS**).

2.5. O equipamento deve possuir dimensão adequada para instalação em rack padrão EIA 19 polegadas e ter altura máxima de 1U (uma unidade de altura de rack).

2.6. **SWITCH DE ACESSO - TIPO 1**

2.7. **FUNCIONALIDADES GERAIS DOS SWITCHES TIPOS 1:**

2.7.1. **ESPECIFICAÇÕES GERAIS**

2.7.1.1. Deve possuir altura máxima 1 (um) rack unit (RU);

2.7.1.2. Deve possuir fonte de alimentação interna, do tipo auto-sense, para operar de 100 a 240 VAC;

2.7.1.3. Deve possuir 8 (oito) portas 10/100/1000 Mbps, usando conectores RJ-45;

2.7.1.4. As portas 10/100/1000 BASE-T devem ser do tipo MDI/MDIX automático;

2.7.1.5. Deve possuir, no mínimo, 2 (duas) portas 1 Gbps SFP, as quais não devem operar em modo "combo" com as portas 10/100/1000 BASE-T em par trançado;

2.7.1.6. Deve possuir capacidade de processamento igual ou superior a 42 (quarenta e dois) Mpps;

2.7.1.7. Deve possuir capacidade de switching igual ou superior a 56 (cinquenta e seis) Gbps;

2.7.1.8. Deve possuir, pelo menos, 4 MB de buffers de pacotes;

2.7.1.9. Deve possuir, pelo menos, 2 GB de memória DRAM;

2.7.1.10. Deve possuir, pelo menos, 8 GB de memória NVRAM;

2.7.1.11. Deve ser do tipo compacto e fanless;

2.7.1.12. Deve implementar os protocolos IEEE 802.3af Power over Ethernet (PoE) e IEEE 802.3at Power over Ethernet Plus (PoE+);

2.7.1.13. Deve possuir PoE power budget de pelo menos 124 (cento e vinte e quatro) watts;

2.7.1.14. Deve possuir porta de console para gerenciamento utilizando conector RJ-45 ou USB Tipo C;

2.7.1.15. Deve possuir LEDs indicativos de energização, atividade do link e velocidade das portas;

2.7.1.16. Deve permitir identificar através de sinalização visual onde o switch está localizado no rack através de comandos para ligar e desligar os LEDs do equipamento;

2.7.1.17. Deve possuir botão de reset para voltar para configuração default de fábrica;

2.7.1.18. Deve implementar o padrão IEE 802.3az (Energy-Efficient Ethernet);

2.7.1.19. Deve possuir certificado de homologação junto à ANATEL de acordo a resolução 242 com documentos disponíveis publicamente no sítio público dessa agência na Internet;

2.7.2. **Funções de camada 2**

2.7.2.1. Deve possuir capacidade de no mínimo 32.000 (trinta e dois mil) endereços MAC;

2.7.2.2. Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad. Deve permitir a configuração de pelo menos 128 (cento e vinte oito) grupos de LACP com pelo menos 8 (oito) portas dentro de um mesmo grupo;

2.7.2.3. Deve implementar o protocolo IEEE 802.1Q para criação de pelo menos 4000 (quatro mil) vlans ativas;

2.7.2.4. Deve implementar o protocolo IEEE 802.1s (Multiple Spanning Tree), IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1D (MAC Bridging, Spanning Tree);

2.7.2.5. Deve ser compatível com o protocolo PVST / PVST+ e PRST;

2.7.2.6. Deve permitir a configuração de pelo menos 250 (duzentas e cinquenta) instâncias de Spanning Tree;

2.7.2.7. Deve implementar BPDU Guard e Root Guard;

2.7.2.8. Deve permitir a configuração de VLANs "trunking" de acordo com o protocolo 802.1Q e VLANs nativas (sem tag) simultaneamente na mesma porta;

2.7.2.9. Deve permitir a criação VLANs privadas;

2.7.2.10. Deve permitir a configuração de VLAN Q-in-Q Tagging de acordo com o padrão IEEE802.1ad ou IEEE802.1QinQ;

2.7.2.11. Deve implementar selective QinQ;

2.7.2.12. Deve implementar para o protocolo UDLD (Uni-Directional Link Detection) ou DLDP (Device Link Detection Protocol) ou similar;

2.7.2.13. Deve implementar jumbo frames até 9000 bytes nas portas Gigabit Ethernet;

2.7.2.14. Deve implementar mecanismos para controle do tráfego broadcasts, multicast e unknown unicast;

2.7.2.15. Deve implementar mecanismo de detecção ativa de loops através do envio frames de detecção. Na detecção de um evento de loop, deve ser capaz de realizar o bloqueio da porta (port shutdown);

2.7.2.16. Deve permitir a configuração de endereços MAC unicast e multicast estáticos em múltiplas portas ethernet simultaneamente, para permitir a configuração de “clusters” de firewalls;

2.7.2.17. Deve implementar IGMP Snooping para IGMPv1, IGMPv2 e IGMPv3;

2.7.2.18. Deve implmenetar MLD snooping v1 e v2;

2.7.2.19. Deve implementar protocolo de proteção de topologia em anel;

2.7.2.20. Deve possuir DHCP Server para IPv4 e IPv6;

2.7.3. **Qualidade de Serviço**

2.7.3.1. Deve permitir priorização de tráfego usando 8 (oito) filas de priorização por porta;

2.7.3.2. Deve permitir priorização de tráfego baseado no padrão IEEE 802.1p e no campo DSCP do protocolo Diffserv;

2.7.3.3. Deve implementar pelos menos os seguintes métodos para configuração das filas de priorização: ponderada, prioridade estrita e ambas combinadas;

2.7.3.4. Implementar priorização de tráfego baseado em porta física, protocolo IEEE 802.1p, endereços IP de origem e destino e portas TCP/UDP de origem e destino;

2.7.3.5. Deve permitir a configuração de Rate Limiting de entrada;

2.7.3.6. Deve permitir a configuração de Rate Shaping de saída;

2.7.3.7. Deve implementar os seguintes algoritmos de fila: Strict Priority e Round Robin com distribuição de pesos WRR (Weighted Round Robin) e uma combinação entre os dois métodos SP e WRR;

2.7.4. **Segurança**

2.7.4.1. Deve permitir autenticação de usuários usando o padrão IEEE 802.1x, permitindo associação dinâmica de VLANs e ACLs usando profiles definidas por um servidor RADIUS externo;

2.7.4.2. Deve permitir a associação de VLANs restritas para usuários que falhem durante a autenticação 802.1X;

2.7.4.3. Implementar método de autenticação baseado em endereço MAC para os dispositivos que não possuírem suplicantes 802.1X;

2.7.4.4. Deve possuir capacidade de autenticação 802.1x com atribuição de VLAN, regras de acesso de segurança e QoS individuais para, no mínimo, 02 (dois) dispositivos (Ex.: Telefone IP e PC) conectados em uma única porta e usando VLANs distintas;

2.7.4.5. Deve permitir, no mínimo e em cada porta, os seguintes tipos de autenticação usando VLANs distintas:

2.7.4.5.1. 2 (dois) dispositivos que suportam o padrão IEEE 802.1x;

2.7.4.5.2. 2 (dois) dispositivos MAC que não suportam o padrão IEEE 802.1x;

2.7.4.5.3. 1 (um) dispositivo que suporta o padrão IEEE 802.1x e 1 (um) dispositivo MAC que não suporta o padrão IEEE 802.1x;

2.7.4.6. O equipamento deve permitir a configuração de reautenticação 802.1x periódica;

2.7.4.7. O equipamento ofertado deve permitir a autenticação via Web Authentication para usuários que não possuem 802.1x;

2.7.4.8. Deve implementar “Change of Authorization” de acordo com a RFC 5176;

2.7.4.9. Deve permitir a autenticação de usuários para acesso às funções de gerenciamento usando-se os protocolos RADIUS, TACACS ou TACACS+;

2.7.4.10. Deve permitir a criação de ACLs para a filtragem de tráfego IPv4 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, bits do protocolo 802.1p e campo DSCP do protocolo Diffserv;

2.7.4.11. Deve permitir a criação de ACLs para a filtragem de tráfego IPv6 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, campo PCP do protocolo 802.1p e campo DSCP do protocolo Diffserv;

2.7.4.12. Deve implementar ACLs de entrada e ACLs de saída para IPv4;

2.7.4.13. Deve implementar ACLs de entrada e ACLs de saída para IPv6;

2.7.4.14. Permitir a filtragem do tráfego através de pelo menos 500 (quinhentas) regras de ACL (Access Control List);

2.7.4.15. Deve implementar segurança de acesso baseada em endereços MAC de origem, com a possibilidade de bloqueio permanente ou temporário das portas onde for detectada uma violação de segurança;

2.7.4.16. Deve permitir a criação de filtros de endereço MAC de origem e destino;

2.7.4.17. Deve possuir protocolos para proteção de ataques de Denial of Service;

2.7.4.18. Deve possuir funcionalidade de proteção contra servidores DHCP não autorizados DHCPv4 snooping e DHCPv6 snooping;

2.7.4.19. Deve possuir funcionalidade de proteção contra-ataques do tipo “ARP Poisoning”;

2.7.4.20. Deve implementar IP Source Guard em IPv4 e IPv6;

2.7.4.21. Deve implementar proteção contra-ataques do tipo TCP SYN e ataques do tipo Smurf;

2.7.4.22. Deve permitir o monitoramento da movimentação de um endereço MAC de uma porta para outra, facilitando a distinção entre um movimento legítimo com um movimento malicioso de um ataque de MAC spoofing;

2.7.4.23. Deve implementar RADsec conforme RFC6614;

2.7.5. **Gerenciamento**

2.7.5.1. Deve permitir monitoração e configuração usando SNMP v1, v2 e v3;

2.7.5.2. Deve permitir o gerenciamento via SNMPv3 com as seguintes opções: sem autenticação e sem privacidade, com autenticação e sem privacidade e com autenticação e com privacidade;

2.7.5.3. Deve ser possível enviar “traps” e realizar o gerenciamento via SNMP através das redes IPv4 e IPv6;

2.7.5.4. Deve permitir a configuração de porta para espelhamento de tráfego, para a coleta de pacotes em analisadores de protocolo ou detecção de intrusão;

2.7.5.5. Deve permitir espelhamento de tráfego baseado em Porta, VLAN, Filtro MAC e ACL;

2.7.5.6. Deve permitir a configuração de porta para espelhamento de tráfego para uma porta em um switch remoto;

2.7.5.7. Deve implementar gerenciamento usando SSH v2 utilizando os algoritmos de criptografia 3DES e AES. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

2.7.5.8. Deve implementar gerenciamento via Telnet. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

2.7.5.9. Deve implementar pelo menos 4 (quatro) grupos de RMON;

2.7.5.10. Deve permitir o monitoramento dos transceivers óticos, retornando informação de temperatura, potência de transmissão (dBm), potência de recepção (dBm) e status;

2.7.5.11. Deve implementar funcionalidade de diagnóstico do cabo de par trançado, retornando informação de comprimento do cabo, status do link;

2.7.5.12. Deve permitir a atualização de arquivos de configuração e imagens de firmware usando TFTP ou FTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

2.7.5.13. Deve permitir a atualização de imagens de firmware dos equipamentos de uma pilha sem a necessidade de reinicialização simultânea de todos os equipamentos da pilha, permitindo a continuidade do tráfego de dados durante o processo de atualização;

2.7.5.14. Deve permitir configuração automática do seu próprio endereço IP e a seguir carga automática de um arquivo de configuração pré-definido, usando um servidor DHCP e um servidor TFTP ou FTP;

2.7.5.15. Deve implementar o protocolo LLDP conforme o padrão IEEE 802.1AB, bem como LLDP-MED;

2.7.5.16. Deve permitir a configuração de seu relógio interno de forma automática através do protocolo NTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

2.7.5.17. Deve permitir armazenamento simultâneo de duas imagens de firmware em memória flash.

2.7.5.18. Deve permitir o envio de mensagens de syslog à pelo menos 2 servidores distintos. Deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

2.7.5.19. Deve permitir o envio de syslog com formato conforme RF5424 para prover mais informações no seu header;

2.7.5.20. Deve implementar funcionalidade de rollback automático de configuração, permitindo que o switch retorne automaticamente para uma configuração estável prévio caso o administrador não confirmar a alteração realizada dentro de um prazo de tempo configurável.

2.8. **SWITCH DE ACESSO – TIPO 2**

2.8.1. **ESPECIFICAÇÕES GERAIS**

2.8.1.1. Deve possuir altura máxima 1 (um) rack unit (RU);

2.8.1.2. Deve possuir fonte de alimentação interna, do tipo auto-sense, para operar de 100 a 240 VAC;

2.8.1.3. Deve possuir 24 (vinte e quatro) portas 10/100/1000 Mbps, usando conectores RJ-45;

2.8.1.4. As portas 10/100/1000 BASE-T devem ser do tipo MDI/MDIX automático;

2.8.1.5. Deve possuir, no mínimo, 4 (quatro) portas 1/10 Gbps SFP+, as quais não devem operar em modo “combo” com as portas 10/100/1000 BASE-T em par trançado;

2.8.1.6. Deve possuir capacidade de processamento igual ou superior a 96 (noventa e seis) Mpps;

2.8.1.7. Deve possuir capacidade de switching igual ou superior a 128 (cento e vinte e oito) Gbps;

2.8.1.8. Deve possuir, pelo menos, 4 MB de buffers de pacotes;

2.8.1.9. Deve possuir, pelo menos, 2 GB de memória DRAM;

2.8.1.10. Deve possuir, pelo menos, 8 GB de memória NVRAM;

2.8.1.11. Deve implementar os protocolos IEEE 802.3af Power over Ethernet (PoE) e IEEE 802.3at Power over Ethernet Plus (PoE+);

2.8.1.12. Deve implementar funcionalidade que garante o fornecimento contínuo de energia para dispositivos alimentados (PDs) conectados a um switch, mesmo durante o processo de reinicialização do switch, recurso conhecido como Perpetual PoE ou Persistent PoE;

2.8.1.13. Deve possuir PoE power budget de pelo menos 370 (trezentos e setenta) watts;

2.8.1.14. Deve possuir porta de console para gerenciamento utilizando conector RJ-45 ou USB Tipo C;

2.8.1.15. Deve possuir LEDs indicativos de energização, atividade do link e velocidade das portas;

2.8.1.16. Deve permitir identificar através de sinalização visual onde o switch está localizado no rack através de comandos para ligar e desligar os LEDs do equipamento;

2.8.1.17. Deve possuir botão de reset para voltar a para configuração default de fábrica;

2.8.1.18. Deve implementar o padrão IEE 802.3az (Energy-Efficient Ethernet);

2.8.1.19. Deve possuir certificado de homologação junto à ANATEL de acordo a resolução 242 com documentos disponíveis publicamente no sítio público dessa agência na Internet;

2.8.2. **Funções de camada 2**

2.8.2.1. Deve possuir capacidade de no mínimo 32.000 (trinta e dois mil) endereços MAC;

2.8.2.2. Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad. Deve permitir a configuração de pelo menos 128 (cento e vinte oito) grupos de LACP com pelo menos 8 (oito) portas dentro de um mesmo grupo;

2.8.2.3. Deve implementar o protocolo IEEE 802.1Q para criação de pelo menos 4000 (quatro mil) vlans ativas;

2.8.2.4. Deve implementar o protocolo IEEE 802.1s (Multiple Spanning Tree), IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1D (MAC Bridging, Spanning Tree);

2.8.2.5. Deve ser compatível com o protocolo PVST / PVST+ e PRST;

2.8.2.6. Deve permitir a configuração de pelo menos 250 (duzentas e cinquenta) instâncias de Spanning Tree;

2.8.2.7. Deve implementar BPDU Guard e Root Guard;

2.8.2.8. Deve permitir a configuração de VLANs “trunking” de acordo com o protocolo 802.1Q e VLANs nativas (sem tag) simultaneamente na mesma porta;

2.8.2.9. Deve permitir a criação VLANs privadas;

2.8.2.10. Deve permitir a configuração de VLAN Q-in-Q Tagging de acordo com o padrão IEEE802.1ad ou IEEE802.1QinQ;

2.8.2.11. Deve implementar selective QinQ;

2.8.2.12. Deve implementar para o protocolo UDLD (Uni-Directional Link Detection) ou DLDP (Device Link Detection Protocol) ou similar;

2.8.2.13. Deve implementar jumbo frames até 9000 bytes nas portas Gigabit Ethernet;

2.8.2.14. Deve implementar mecanismos para controle do tráfego broadcasts, multicast e unknown unicast;

2.8.2.15. Deve implementar mecanismo de detecção ativa de loops através do envio frames de detecção. Na detecção de um evento de loop, deve ser capaz de realizar o bloqueio da porta (port shutdown);

2.8.2.16. Deve permitir a configuração de endereços MAC unicast e multicast estáticos em múltiplas portas ethernet simultaneamente, para permitir a configuração de “clusters” de firewalls;

2.8.2.17. Deve implementar IGMP Snooping para IGMPv1, IGMPv2 e IGMPv3;

2.8.2.18. Deve implmenetar MLD snooping v1 e v2;

2.8.2.19. Deve implementar protocolo de proteção de topologia em anel;

2.8.2.20. Deve possuir DHCP Server para IPv4 e IPv6;

2.8.3. **Qualidade de Serviço**

2.8.3.1. Deve permitir priorização de tráfego usando 8 (oito) filas de priorização por porta;

2.8.3.2. Deve permitir priorização de tráfego baseado no padrão IEEE 802.1p e no campo DSCP do protocolo Diffserv;

2.8.3.3. Deve implementar pelos menos os seguintes métodos para configuração das filas de priorização: ponderada, prioridade estrita e ambas combinadas;

2.8.3.4. Implementar priorização de tráfego baseado em porta física, protocolo IEEE 802.1p, endereços IP de origem e destino e portas TCP/UDP de origem e destino;

2.8.3.5. Deve permitir a configuração de Rate Limiting de entrada;

2.8.3.6. Deve permitir a configuração de Rate Shaping de saída;

2.8.3.7. Deve implementar os seguintes algoritmos de fila: Strict Priority e Round Robin com distribuição de pesos WRR (Weighted Round Robin) e uma combinação entre os dois métodos SP e WRR;

2.8.4. **Segurança**

2.8.4.1. Deve permitir autenticação de usuários usando o padrão IEEE 802.1x, permitindo associação dinâmica de VLANs e ACLs usando profiles definidas por um servidor RADIUS externo;

2.8.4.2. Deve permitir a associação de VLANs restritas para usuários que falhem durante a autenticação 802.1X;

2.8.4.3. Implementar método de autenticação baseado em endereço MAC para os dispositivos que não possuírem suplicantes 802.1X;

2.8.4.4. Deve possuir capacidade de autenticação 802.1x com atribuição de VLAN, regras de acesso de segurança e QoS individuais para, no mínimo, 02 (dois) dispositivos (Ex.: Telefone IP e PC) conectados em uma única porta e usando VLANs distintas;

2.8.4.5. Deve permitir, no mínimo e em cada porta, os seguintes tipos de autenticação usando VLANs distintas:

2.8.4.5.1. 2 (dois) dispositivos que suportam o padrão IEEE 802.1x;

2.8.4.5.2. 2 (dois) dispositivos MAC que não suportam o padrão IEEE 802.1x;

2.8.4.5.3. 1 (um) dispositivo que suporta o padrão IEEE 802.1x e 1 (um) dispositivo MAC que não suporta o padrão IEEE 802.1x;

2.8.4.6. O equipamento deve permitir a configuração de reautenticação 802.1x periódica;

2.8.4.7. O equipamento ofertado deve permitir a autenticação via Web Authentication para usuários que não possuem 802.1x;

2.8.4.8. Deve implementar “Change of Authorization” de acordo com a RFC 5176;

2.8.4.9. Deve permitir a autenticação de usuários para acesso às funções de gerenciamento usando-se os protocolos RADIUS, TACACS ou TACACS+;

2.8.4.10. Deve permitir a criação de ACLs para a filtragem de tráfego IPv4 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, bits do protocolo 802.1p e campo DSCP do protocolo Diffserv;

2.8.4.11. Deve permitir a criação de ACLs para a filtragem de tráfego IPv6 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, campo PCP do protocolo 802.1p e campo DSCP do protocolo Diffserv;

2.8.4.12. Deve implementar ACLs de entrada e ACLs de saída para IPv4;

2.8.4.13. Deve implementar ACLs de entrada e ACLs de saída para IPv6;

2.8.4.14. Permitir a filtragem do tráfego através de pelo menos 500 (quinhentas) regras de ACL (Access Control List);

2.8.4.15. Deve implementar segurança de acesso baseada em endereços MAC de origem, com a possibilidade de bloqueio permanente ou temporário das portas onde for detectada uma violação de segurança;

2.8.4.16. Deve permitir a criação de filtros de endereço MAC de origem e destino;

2.8.4.17. Deve possuir protocolos para proteção de ataques de Denial of Service;

2.8.4.18. Deve possuir funcionalidade de proteção contra servidores DHCP não autorizados DHCPv4 snooping e DHCPv6 snooping;

2.8.4.19. Deve possuir funcionalidade de proteção contra-ataques do tipo “ARP Poisoning”;

2.8.4.20. Deve implementar IP Source Guard em IPv4 e IPv6;

2.8.4.21. Deve implementar proteção contra-ataques do tipo TCP SYN e ataques do tipo Smurf;

2.8.4.22. Deve permitir o monitoramento da movimentação de um endereço MAC de uma porta para outra, facilitando a distinção entre um movimento legítmo com um movimento malicioso de um ataque de MAC spoofing;

2.8.4.23. Deve implementar RADsec conforme RFC6614;

2.8.5. **Gerenciamento**

2.8.5.1. Deve permitir monitoração e configuração usando SNMP v1, v2 e v3;

2.8.5.2. Deve permitir o gerenciamento via SNMPv3 com as seguintes opções: sem autenticação e sem privacidade, com autenticação e sem privacidade e com autenticação e com privacidade;

2.8.5.3. Deve ser possível enviar “traps” e realizar o gerenciamento via SNMP através das redes IPv4 e IPv6;

2.8.5.4. Deve permitir a configuração de porta para espelhamento de tráfego, para a coleta de pacotes em analisadores de protocolo ou detecção de intrusão;

2.8.5.5. Deve permitir espelhamento de tráfego baseado em Porta, VLAN, Filtro MAC e ACL;

2.8.5.6. Deve permitir a configuração de porta para espelhamento de tráfego para uma porta em um switch remoto;

2.8.5.7. Deve implementar gerenciamento usando SSH v2 utilizando os algoritmos de criptografia 3DES e AES. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

2.8.5.8. Deve implementar gerenciamento via Telnet. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

2.8.5.9. Deve implementar pelo menos 4 (quatro) grupos de RMON;

2.8.5.10. Deve permitir o monitoramento dos transceivers óticos, retornando informação de temperatura, potência de transmissão (dBm), potência de recepção (dBm) e status;

2.8.5.11. Deve implementar funcionalidade de diagnóstico do cabo de par trançado, retornando informação de comprimento do cabo, status do link;

2.8.5.12. Deve permitir a atualização de arquivos de configuração e imagens de firmware usando TFTP ou FTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

2.8.5.13. Deve permitir a atualização de imagens de firmware dos equipamentos de uma pilha sem a necessidade de reinicialização simultânea de todos os equipamentos da pilha, permitindo a continuidade do tráfego de dados durante o processo de atualização;

2.8.5.14. Deve permitir configuração automática do seu próprio endereço IP e a seguir carga automática de um arquivo de configuração pré-definido, usando um servidor DHCP e um servidor TFTP ou FTP;

2.8.5.15. Deve implementar o protocolo LLDP conforme o padrão IEEE 802.1AB, bem como LLDP-MED;

2.8.5.16. Deve permitir a configuração de seu relógio interno de forma automática através do protocolo NTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

2.8.5.17. Deve permitir armazenamento simultâneo de duas imagens de firmware em memória flash.

2.8.5.18. Deve permitir o envio de mensagens de syslog à pelo menos 2 servidores distintos. Deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

2.8.5.19. Deve permitir o envio de syslog com formato conforme RF5424 para prover mais informações no seu header;

2.8.5.20. Deve implementar funcionalidade de rollback automático de configuração, permitindo que o switch retorne automaticamente para uma configuração estável prévio caso o administrador não confirmar a alteração realizada dentro de um prazo de tempo configurável.

2.9. **SWITCH DE ACESSO - TIPO 3**

2.9.1. **ESPECIFICAÇÕES GERAIS**

2.9.1.1. Deve possuir altura máxima 1 (um) rack unit (RU);

2.9.1.2. Deve possuir fonte de alimentação interna, do tipo auto-sense, para operar de 100 a 240 VAC;

2.9.1.3. Deve possuir 48 (quarenta e oito) portas 10/100/1000 Mbps, usando conectores RJ-45;

2.9.1.4. As portas 10/100/1000 BASE-T devem ser do tipo MDI/MDIX automático;

2.9.1.5. Deve possuir, no mínimo, 4 (quatro) portas 1/10 Gbps SFP+, as quais não devem operar em modo “combo” com as portas 10/100/1000 BASE-T em par trançado;

2.9.1.6. Deve possuir capacidade de processamento igual ou superior a 132 (cento e trinta e dois) Mpps;

2.9.1.7. Deve possuir capacidade de switching igual ou superior a 176 (cento e setenta e seis) Gbps;

2.9.1.8. Deve possuir, pelo menos, 4 MB de buffers de pacotes;

2.9.1.9. Deve possuir, pelo menos, 2 GB de memória DRAM;

2.9.1.10. Deve possuir, pelo menos, 8 GB de memória NVRAM;

2.9.1.11. Deve implementar os protocolos IEEE 802.3af Power over Ethernet (PoE) e IEEE 802.3at Power over Ethernet Plus (PoE+);

2.9.1.12. Deve possuir PoE power budget de pelo menos 370 (trezentos e setenta) watts;

2.9.1.13. Deve possuir porta de console para gerenciamento utilizando conector RJ-45 ou USB Tipo C;

2.9.1.14. Deve possuir LEDs indicativos de energização, atividade do link e velocidade das portas;

2.9.1.15. Deve permitir identificar através de sinalização visual onde o switch está localizado no rack através de comandos para ligar e desligar os LEDs do equipamento;

2.9.1.16. Deve possuir botão de reset para voltar para configuração default de fábrica;

2.9.1.17. Deve implementar o padrão IEE 802.3az (Energy-Efficient Ethernet);

2.9.1.18. Deve possuir certificado de homologação junto à ANATEL de acordo a resolução 242 com documentos disponíveis publicamente no sítio público dessa agência na Internet;

2.9.2. **Funções de Camada 2**

2.9.2.1. Deve possuir capacidade de no mínimo 32.000 (trinta e dois mil) endereços MAC;

2.9.2.2. Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad. Deve permitir a configuração de pelo menos 128 (cento e vinte oito) grupos de LACP com pelo menos 8 (oito) portas dentro de um mesmo grupo;

2.9.2.3. Deve implementar o protocolo IEEE 802.1Q para criação de pelo menos 4000 (quatro mil) vlans ativas;

2.9.2.4. Deve implementar o protocolo IEEE 802.1s (Multiple Spanning Tree), IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1D (MAC Bridging, Spanning Tree);

2.9.2.5. Deve ser compatível com o protocolo PVST / PVST+ e PRST;

2.9.2.6. Deve permitir a configuração de pelo menos 250 (duzentas e cinquenta) instâncias de Spanning Tree;

2.9.2.7. Deve implementar BPDU Guard e Root Guard;

2.9.2.8. Deve permitir a configuração de VLANs “trunking” de acordo com o protocolo 802.1Q e VLANs nativas (sem tag) simultaneamente na mesma porta;

2.9.2.9. Deve permitir a criação VLANs privadas;

2.9.2.10. Deve permitir a configuração de VLAN Q-in-Q Tagging de acordo com o padrão IEEE802.1ad ou IEEE802.1QinQ;

2.9.2.11. Deve implementar selective QinQ;

2.9.2.12. Deve implementar para o protocolo UDLD (Uni-Directional Link Detection) ou DLDP (Device Link Detection Protocol) ou similar;

2.9.2.13. Deve implementar jumbo frames até 9000 bytes nas portas Gigabit Ethernet;

2.9.2.14. Deve implementar mecanismos para controle do tráfego broadcasts, multicast e unknown unicast;

2.9.2.15. Deve implementar mecanismo de detecção ativa de loops através do envio frames de detecção. Na detecção de um evento de loop, deve ser capaz de realizar o bloqueio da porta (port shutdown);

2.9.2.16. Deve permitir a configuração de endereços MAC unicast e multicast estáticos em múltiplas portas ethernet simultaneamente, para permitir a configuração de “clusters” de firewalls;

2.9.2.17. Deve implementar IGMP Snooping para IGMPv1, IGMPv2 e IGMPv3;

2.9.2.18. Deve implmenetar MLD snooping v1 e v2;

2.9.2.19. Deve implementar protocolo de proteção de topologia em anel;

2.9.2.20. Deve possuir DHCP Server para IPv4 e IPv6;

2.9.3. **Qualidade de Serviço**

2.9.3.1. Deve permitir priorização de tráfego usando 8 (oito) filas de priorização por porta;

2.9.3.2. Deve permitir priorização de tráfego baseado no padrão IEEE 802.1p e no campo DSCP do protocolo Diffserv;

2.9.3.3. Deve implementar pelos menos os seguintes métodos para configuração das filas de priorização: ponderada, prioridade estrita e ambas combinadas;

2.9.3.4. Implementar priorização de tráfego baseado em porta física, protocolo IEEE 802.1p, endereços IP de origem e destino e portas TCP/UDP de origem e destino;

2.9.3.5. Deve permitir a configuração de Rate Limiting de entrada;

2.9.3.6. Deve permitir a configuração de Rate Shaping de saída;

2.9.3.7. Deve implementar os seguintes algoritmos de fila: Strict Priority e Round Robin com distribuição de pesos WRR (Weighted Round Robin) e uma combinação entre os dois métodos SP e WRR;

2.9.4. **Segurança**

2.9.4.1. Deve permitir autenticação de usuários usando o padrão IEEE 802.1x, permitindo associação dinâmica de VLANs e ACLs usando profiles definidas por um servidor RADIUS externo;

2.9.4.2. Deve permitir a associação de VLANs restritas para usuários que falhem durante a autenticação 802.1X;

2.9.4.3. Implementar método de autenticação baseado em endereço MAC para os dispositivos que não possuírem suplicantes 802.1X;

2.9.4.4. Deve possuir capacidade de autenticação 802.1x com atribuição de VLAN, regras de acesso de segurança e QoS individuais para, no mínimo, 02 (dois) dispositivos (Ex.: Telefone IP e PC) conectados em uma única porta e usando VLANs distintas;

2.9.4.5. Deve permitir, no mínimo e em cada porta, os seguintes tipos de autenticação usando VLANs distintas:

2.9.4.5.1. 2 (dois) dispositivos que suportam o padrão IEEE 802.1x;

2.9.4.5.2. 2 (dois) dispositivos MAC que não suportam o padrão IEEE 802.1x;

2.9.4.5.3. 1 (um) dispositivo que suporta o padrão IEEE 802.1x e 1 (um) dispositivo MAC que não suporta o padrão IEEE 802.1x;

2.9.4.6. O equipamento deve permitir a configuração de reautenticação 802.1x periódica;

2.9.4.7. O equipamento ofertado deve permitir a autenticação via Web Authentication para usuários que não possuem 802.1x;

2.9.4.8. Deve implementar “Change of Authorization” de acordo com a RFC 5176;

2.9.4.9. Deve permitir a autenticação de usuários para acesso às funções de gerenciamento usando-se os protocolos RADIUS, TACACS ou TACACS+;

2.9.4.10. Deve permitir a criação de ACLs para a filtragem de tráfego IPv4 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, bits do protocolo 802.1p e campo DSCP do protocolo Diffserv;

2.9.4.11. Deve permitir a criação de ACLs para a filtragem de tráfego IPv6 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, campo PCP do protocolo 802.1p e campo DSCP do protocolo Diffserv;

2.9.4.12. Deve implementar ACLs de entrada e ACLs de saída para IPv4;

2.9.4.13. Deve implementar ACLs de entrada e ACLs de saída para IPv6;

2.9.4.14. Permitir a filtragem do tráfego através de pelo menos 500 (quinhentas) regras de ACL (Access Control List);

2.9.4.15. Deve implementar segurança de acesso baseada em endereços MAC de origem, com a possibilidade de bloqueio permanente ou temporário das portas onde for detectada uma violação de segurança;

2.9.4.16. Deve permitir a criação de filtros de endereço MAC de origem e destino;

2.9.4.17. Deve possuir protocolos para proteção de ataques de Denial of Service;

2.9.4.18. Deve possuir funcionalidade de proteção contra servidores DHCP não autorizados DHCPv4 snooping e DHCPv6 snooping;

2.9.4.19. Deve possuir funcionalidade de proteção contra-ataques do tipo “ARP Poisoning”;

2.9.4.20. Deve implementar IP Source Guard em IPv4 e IPv6;

2.9.4.21. Deve implementar proteção contra-ataques do tipo TCP SYN e ataques do tipo Smurf;

2.9.4.22. Deve permitir o monitoramento da movimentação de um endereço MAC de uma porta para outra, facilitando a distinção entre um movimento legítmo com um movimento malicioso de um ataque de MAC spoofing;

2.9.4.23. Deve implementar RADsec conforme RFC6614;

2.9.5. **Gerenciamento**

2.9.5.1. Deve permitir monitoração e configuração usando SNMP v1, v2 e v3;

2.9.5.2. Deve permitir o gerenciamento via SNMPv3 com as seguintes opções: sem autenticação e sem privacidade, com autenticação e sem privacidade e com autenticação e com privacidade;

2.9.5.3. Deve ser possível enviar “traps” e realizar o gerenciamento via SNMP através das redes IPv4 e IPv6;

2.9.5.4. Deve permitir a configuração de porta para espelhamento de tráfego, para a coleta de pacotes em analisadores de protocolo ou detecção de intrusão;

2.9.5.5. Deve permitir espelhamento de tráfego baseado em Porta, VLAN, Filtro MAC e ACL;

2.9.5.6. Deve permitir a configuração de porta para espelhamento de tráfego para uma porta em um switch remoto;

2.9.5.7. Deve implementar gerenciamento usando SSH v2 utilizando os algoritmos de criptografia 3DES e AES. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

2.9.5.8. Deve implementar gerenciamento via Telnet. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

2.9.5.9. Deve implementar pelo menos 4 (quatro) grupos de RMON;

2.9.5.10. Deve permitir o monitoramento dos transceivers óticos, retornando informação de temperatura, potência de transmissão (dBm), potência de recepção (dBm) e status;

2.9.5.11. Deve implementar funcionalidade de diagnóstico do cabo de par trançado, retornando informação de comprimento do cabo, status do link;

2.9.5.12. Deve permitir a atualização de arquivos de configuração e imagens de firmware usando TFTP ou FTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

2.9.5.13. Deve permitir a atualização de imagens de firmware dos equipamentos de uma pilha sem a necessidade de reinicialização simultânea de todos os equipamentos da pilha, permitindo a continuidade do tráfego de dados durante o processo de atualização;

2.9.5.14. Deve permitir configuração automática do seu próprio endereço IP e a seguir carga automática de um arquivo de configuração pré-definido, usando um servidor DHCP e um servidor TFTP ou FTP;

2.9.5.15. Deve implementar o protocolo LLDP conforme o padrão IEEE 802.1AB, bem como LLDP-MED;

2.9.5.16. Deve permitir a configuração de seu relógio interno de forma automática através do protocolo NTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

2.9.5.17. Deve permitir armazenamento simultâneo de duas imagens de firmware em memória flash.

2.9.5.18. Deve permitir o envio de mensagens de syslog à pelo menos 2 servidores distintos. Deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

2.9.5.19. Deve permitir o envio de syslog com formato conforme RF5424 para prover mais informações no seu header;

2.9.5.20. Deve implementar funcionalidade de rollback automático de configuração, permitindo que o switch retorne automaticamente para uma configuração estável prévio caso o administrador não confirmar a alteração realizada dentro de um prazo de tempo configurável.

3. PONTOS DE ACESSO COORPORATIVO, INDOOR E OUTDOOR - REQUISITOS GERAIS PARA PONTOS DE ACESSO WIFI TIPOS 1, 2, 3, 4 e 5:

3.1. Todos os Pontos de Acesso Wi-fi do Lote 1 especificados no presente documento devem ser do mesmo fabricante, compondo uma solução única de rede, para assegurar a compatibilidade funcional de todos os recursos e permitir o gerenciamento unificado.

3.2. Todos os acessórios que serão utilizados na prestação do serviço, tais como cabos de força (padrão ABNT NBR 14136) e cabos de interconexões (DAC/AOC/FIBRAS e etc), assim como transceivers e conversores de mídia deverão estar inclusos na solução.

3.3. O fornecedor poderá utilizar injetores PoE (Power over Ethernet), limitando-se a até 10% (dez porcento) do volume total de Pontos de Acesso wi-fi, devendo atender todas as demais especificações técnicas descritas.

3.4. Caso o fornecedor opte pelo fornecimento na modalidade prevista no item 3.3, os injetores PoE deverão necessariamente serem do mesmo fabricante dos pontos de acesso wi-fi.

3.5. Esses pontos de acesso wi-fi deverão possuir a mesma console de gerência dos switches.

3.6. A controladora dos Pontos de Acesso Wi-fi deve ser centralizada e fornecida em ambiente de nuvem como serviço (**SaaS**).

3.7. Todos os modelos-tipo de pontos de acesso WiFi apresentados abaixo deverão atender aos seguintes requisitos:

3.7.1. Desenho de solução com alta disponibilidade e tolerância a falhas;

3.7.2. Gerenciamento dos recursos de rádio que permitem que os pontos de acesso automaticamente ajustem a cobertura em caso de fala em um dos pontos de acesso;

3.7.3. Os pontos de acesso deverão ser fornecidos com kit de fixação em parede ou teto (indoor e outdoor).

3.8. PONTO DE ACESSO - TIPO 1

3.8.1. ESPECIFICAÇÕES GERAIS

3.8.2. Deverá ser do mesmo fabricante do controlador WLAN.

3.8.3. Deverá ser apresentado certificado válido de interoperabilidade fornecido pela Wi-Fi Alliance na categoria de Enterprise Access Point.

3.8.4. Suportar, no mínimo, 256 (duzentos e cinquenta e seis) usuários wireless simultâneos, sem nenhum tipo de licença adicional.

3.8.5. Possuir suporte a pelo menos 16 (dezesseis) SSIDs por ponto de acesso.

3.8.6. Possibilitar alimentação elétrica local via fonte de alimentação com seleção automática de tensão (100-240V) e via padrão PoE (IEEE 802.3af ou 802.3at).

3.8.7. Deve suportar temperatura de operação entre 0°C a 40°C.

3.8.8. Deverá possuir estrutura que permita a utilização do equipamento em locais internos, com fixação em teto e parede.

3.8.9. Não serão aceitos equipamentos com antenas aparentes (externas ao ponto de acesso) rosqueáveis, permitindo sua remoção.

3.8.10. Deve possuir LEDs para a indicação do status das portas ethernet, rede wireless, gerenciamento via controladora, indicador de conexão sem fio Mesh e da atividade do equipamento.

3.8.11. Deverá ser fornecido com todas as funcionalidades de segurança habilitadas.

3.8.12. Deverá ser fornecido com a versão mais recente de software.

3.8.13. **Características dos Rádios**

3.8.14. O ponto de acesso deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax com operação nas frequências 2.4 GHz e 5 GHz de forma simultânea.

3.8.15. Implementar as seguintes taxas de transmissão com fallback automático:

3.8.15.1. IEEE 802.11b: 11, 5.5, 2 e 1 Mbps
3.8.15.2. IEEE 802.11a e IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps
3.8.15.3. IEEE 802.11n: 6.5 Mbps a 300 Mbps
3.8.15.4. IEEE 802.11ac: 6.5 Mbps a 867 Mbps
3.8.15.5. IEEE 802.11ax: 4 até 1200 Mbps

3.8.16. Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio em 2.4GHz e 5GHz e com ganhos máximos combinados de no mínimo, 3 dBi.

3.8.17. Deve suportar potência de saída agregada somando todas as cadeias de transmissão de, no mínimo, 17 dBm para 5 GHz e de, no mínimo, 20 dBm para 2.4 GHz.

3.8.18. Deverá suportar canalização de 20 MHz, 40 MHz e 80 MHz.

3.8.19. Deverá possuir mecanismo de rádio com suporte a MIMO 2x2 com 2 spatial streams.

3.8.20. Deverá possuir suporte a Multi User MIMO (MU-MIMO)

3.8.21. Deverá possuir suporte a MRC – Maximal Ratio Combining ou similar

3.8.22. Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2.4GHz livre para dispositivos que trabalhem somente nesta frequência.

3.8.23. Permitir ajustes dinâmicos de RF de modo a otimizar o tamanho da célula de abrangência de RF.

3.8.24. Deve ser capaz de operar no modo Mesh sem adição de novo hardware ou alteração do sistema operacional, sendo que a comunicação até o controlador pode ser feita via wireless ou pela rede local.

3.8.25. Deve suportar autocura por meio de Mesh em caso de falha da conexão cabeada de dados, bem como permitir que os pontos de acesso gerenciados estabeleçam automaticamente uma rede mesh sem fio.

3.8.26. Possuir capacidade de selecionar automaticamente o canal de transmissão.

3.8.27. **Rede e Serviços**

3.8.28. Deverá possuir 01 (uma) interface IEEE 802.3 10/100/1000 Mbps Base-T Ethernet, auto-sensing, com conector RJ-45, para conexão à rede local fixa.

3.8.29. Deverá possuir ao menos uma porta USB para inserção de dispositivos voltados à implementação de redes IoT com suporte aos padrões BLE ou ZigBee

3.8.30. Deve suportar, em conjunto com o controlador de rede sem fio, a identificação e controle de aplicações dos dispositivos clientes conectados ao ponto de acesso.

3.8.31. Deve suportar, em conjunto com o controlador de rede sem fio, a configuração de limite de banda (rate limit) por usuário e por SSID.

3.8.32. Deve suportar, em conjunto com o controlador, suporte ao mecanismo de localização e rastreamento de usuários (Location Based Service).

3.8.33. O ponto de acesso poderá estar conectado diretamente ou remotamente ao controlador WLAN, inclusive através de roteamento em Camada 3.

3.8.34. Implementar cliente DHCP, para configuração automática de seu endereço IP e implementar também suporte à endereçamento IP estático.

3.8.35. Deve suportar VLANs conforme o padrão IEEE 802.1Q.

3.8.36. Deverá permitir atribuir uma VLAN para cada SSID.

3.8.37. Deverá suportar o uso de VLANs dinâmicas em conjunto com o controlador de rede sem fio.

3.8.38. Deverá suportar as seguintes funcionalidades wireless:

3.8.38.1. IEEE 802.11r
3.8.38.2. IEEE 802.11v
3.8.38.3. IEEE 802.11k
3.8.38.4. WMM e Power Save
3.8.38.5. LPDC e STBC

3.8.39. Deve suportar limitação de banda por grupo de usuários ou por SSID.

3.8.40. Deve implementar balanceamento de usuários por ponto de acesso e por rádio (2.4GHz e 5 GHz).

3.8.41. Deve implementar mecanismo para otimização de roaming entre pontos de acesso.

3.9. **Segurança e Gerenciamento**

3.9.1. Deve suportar a utilização de sistema antifurto do tipo Kensington lock ou similar que permita a instalação de um cabo de segurança com a finalidade de evitar furto do equipamento.

3.9.2. Implementar, pelo menos, os seguintes padrões de segurança wireless:

3.9.2.1. (WPA) Wi-Fi Protected Access
3.9.2.2. (WPA2) Wi-Fi Protected Access 2
3.9.2.3. (WPA3) Wi-Fi Protected Access 3
3.9.2.4. (AES) Advanced Encryption Standard
3.9.2.5. (TKIP) Temporal Key Integrity Protocol
3.9.2.6. IEEE 802.1x
3.9.2.7. IEEE 802.11i

3.9.3. Deverá permitir a criação de filtros de MAC address de forma a restringir o acesso à rede wireless.

3.9.4. Permitir habilitar e desabilitar a divulgação do SSID.

3.9.5. Deve implementar autenticação de usuários usando portal de captura.

3.9.6. Deve implementar autenticação de usuários usando redes baseadas em portal captivo WISPr

3.9.7. Deve implementar autenticação de usuários usando redes baseadas em padrão Hotspot 2.0.

3.9.8. Permitir a configuração e gerenciamento direto através de browser padrão (HTTPS), SSH, SNMPv2c e SNMPv3, ou através do controlador, a fim de se garantir a segurança dos dados.

3.9.9. Permitir gerenciamento através de plataformas de software que sigam padrões SNMPv2c e SNMPv3.

3.9.10. Implementar funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, das políticas de segurança, QoS, autenticação e monitoramento de RF.

3.9.11. Permitir que sua configuração seja realizada automaticamente quando este for conectado ao controlador WLAN do mesmo fabricante.

3.9.12. Permitir que o processo de atualização de software seja realizado manualmente através de interface web, FTP ou TFTP e automaticamente através de controlador WLAN do mesmo fabricante.

3.9.13. Deverá ser fornecido com todas as funcionalidades de segurança, incluindo WIDS, e Wi-Fi Mesh habilitadas, incluindo autocura via Mesh.

3.10. **PONTO DE ACESSO - TIPO 2**

3.10.1. **ESPECIFICAÇÕES GERAIS**

3.10.1.1. Deverá ser do mesmo fabricante do controlador WLAN para fins de compatibilidade.

3.10.1.2. Deverá possuir estrutura que permita a utilização do equipamento em locais internos, com fixação em teto e parede.

3.10.1.3. Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto, com data anterior à publicação do edital, conforme a resolução 242. Não serão aceitos protocolos de entrada ou outros documentos diferentes do certificado, uma vez que os mesmos não garantem o fornecimento de equipamentos homologados e em conformidade com as leis brasileiras.

3.10.1.4. Visando a plena compatibilidade do ponto de acesso com o padrão WiFi 6 e suas respectivas funcionalidades, a citar, de forma não-exaustiva, DL OFDMA, UL OFDMA, DL MU-MIMO e se faz necessário que o equipamento ofertado esteja listado como Wi-Fi CERTIFIED 6 no programa da WiFi Alliance na data do pregão.

3.10.1.5. Deve possuir a certificação IEC 61373 para uso em ambientes sujeitos à vibração e impactos.

3.10.1.6. Deve ser compatível com o padrão UL 2043, que regula os componentes dos materiais com o intuito de proteger contra danos causados por fogo, bem como pela fumaça.

3.10.1.7. Suportar, no mínimo, 500 (quinhentos) usuários wireless simultâneos, sem nenhum tipo de licença adicional.

3.10.1.8. Possuir suporte a pelo menos 16 (dezesseis) SSIDs por ponto de acesso.

3.10.1.9. Possibilitar alimentação elétrica local via fonte de alimentação com seleção automática de tensão (100-240V) e via padrão PoE (IEEE 802.3at ou 802.3bt). Ademais, para PoE, a alimentação elétrica deve ocorrer através de uma única interface de rede, sem perda de funcionalidade e de desempenho.

3.10.1.10. Deve suportar temperatura de operação entre 0°C a 40°C.

3.10.1.11. O equipamento ofertado não deverá possuir antenas aparentes externas ao ponto de acesso, evitando desta forma que as mesmas sejam removidas, o que ocasionaria na degradação do desempenho da rede sem fio.

3.10.1.12. Deverá possuir 2 (duas) interfaces ethernet, sendo 1 (uma) 10/100/1000 Mbps e 1 (uma) 1/2.5 Gbps, utilizando conector RJ-45, para conexão à rede local.

3.10.1.13. Deve suportar LLDP na interface ethernet.

3.10.1.14. Deverá possuir, no mínimo, um rádio embarcado para IoT, o qual deve ser compatível com BLE ou ZigBee.

3.10.1.15. Deverá dispor de uma porta USB para inserção de módulo IoT compatível com BLE e ZigBee.

3.10.1.16. Deverá possuir múltiplos LEDs para a indicação do status da alimentação do ponto de acesso, rádios de 2.4 GHz e 5 GHz, operação em Mesh e gerenciamento via controladora.

3.10.1.17. Deverá ser fornecido com todas as funcionalidades de segurança, incluindo WIPS/WIDS, e Wi-Fi Mesh habilitadas, incluindo autocura via Mesh.

3.10.1.18. Deve ser compatível com IPv4, IPv6 e dual-stack.

3.10.2. **Características dos Rádios**

3.10.2.1. O ponto de acesso deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax, com operação nas frequências de 2.4 GHz e 5 GHz de forma simultânea.

3.10.2.2. Implementar as seguintes taxas de transmissão com fallback automático: IEEE 802.11b: 1 Mbps a 11 Mbps, IEEE 802.11a e IEEE 802.11g: 6 Mbps a 54 Mbps, IEEE 802.11n: 6.5 Mbps a 600 Mbps, IEEE 802.11ac: 6.5 Mbps a 1732 Mbps e IEEE 802.11ax: 4 Mbps a 2400 Mbps.

3.10.2.3. Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax, com ganhos de, no mínimo, 3 dBi para 2.4GHz e 5GHz.

3.10.2.4. Deverá suportar potência agregada de saída, considerando todas as cadeias MIMO, de, no mínimo, 24 dBm na frequência de 5 GHz e 23 dBm na frequência de 2.4 GHz.

3.10.2.5. Deverá suportar canalização de 20 MHz, 40 MHz, 80 MHz e 160 MHz.

3.10.2.6. Deverá possuir mecanismo de rádio com suporte a 6 (seis) fluxos espaciais, sendo 4x4:4 em 5 GHz e 2x2:2 em 2.4 GHz para SU-MIMO e MU-MIMO.

3.10.2.7. Deve permitir ajustes dinâmicos do sinal de rádio frequência para otimizar o tamanho da célula de abrangência do ponto de acesso.

3.10.2.8. Deve possuir capacidade de selecionar automaticamente o canal de transmissão.

3.10.2.9. Deve suportar os padrões IEEE 802.11r, IEEE 802.11k e IEEE 802.11v.

3.10.3. **Serviços, Segurança e Gerenciamento**

3.10.3.1. Deve permitir controle e gerenciamento pelo controlador WLAN através de Camada 2 ou 3 do modelo OSI.

3.10.3.2. Deve ser capaz de operar no modo Mesh sem adição de novo hardware ou alteração do sistema operacional, sendo que a comunicação até o controlador pode ser feita via wireless ou pela rede local.

3.10.3.3. Deve suportar autocura por meio de Mesh em caso de falha da conexão cabeada de dados, bem como permitir que os pontos de acesso gerenciados estabeleçam automaticamente uma rede mesh sem fio.

3.10.3.4. Em caso de falha de comunicação entre os pontos de acesso e o controlador WLAN, os usuários associados à rede sem fio devem continuar conectados com acesso à rede. Além disso, deve ser possível que novos usuários se associem à rede sem fio utilizando autenticação do tipo IEEE 802.1x mesmo que os pontos de acesso estejam sem comunicação com a controladora.

3.10.3.5. Deve suportar, somente por meio do ponto de acesso em conjunto com o controlador de rede sem fio, a identificação e controle de aplicações dos dispositivos clientes conectados ao ponto de acesso, levando em consideração a camada 7 do modelo OSI.

3.10.3.6. Deve suportar a configuração de limite de banda por usuário ou por SSID.

3.10.3.7. Deve oferecer suporte a mecanismo de localização e rastreamento de usuários (Location Based Services).

3.10.3.8. Implementar cliente DHCP, para configuração automática de seu endereço IP e implementar também suporte a endereçamento IP estático.

3.10.3.9. Deve suportar VLANs conforme o padrão IEEE 802.1Q.

3.10.3.10. Deve suportar atribuição dinâmica de VLAN por usuário.

3.10.3.11. Deve implementar balanceamento de usuários por ponto de acesso.

3.10.3.12. Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2.4 GHz livre para dispositivos que trabalhem somente nesta frequência.

3.10.3.13. Deve implementar mecanismo para otimização de roaming entre pontos de acesso.

3.10.3.14. Deve suportar HotSpot 2.0, Captive Portal e WISPr.

3.10.3.15. Implementar, pelo menos, os seguintes padrões de segurança wireless: (WPA) Wi-Fi Protected Access, (WPA2) Wi-Fi Protected Access 2, (WPA3) Wi-Fi Protected Access 3, (AES) Advanced Encryption Standard, (TKIP) Temporal Key Integrity Protocol, PSK por dispositivo, IEEE 802.1X e IEEE 802.11i.

3.10.3.16. Deverá permitir a criação de filtros de endereços MAC de forma a restringir o acesso à rede sem fio.

3.10.3.17. Deverá permitir a criação de listas de controle de acesso de Camada 3 e 4 do modelo OSI.

3.10.3.18. Deverá ser possível criar políticas de controle com base no tipo ou sistema operacional do dispositivo.

3.10.3.19. Deve permitir habilitar e desabilitar a divulgação do SSID.

3.10.3.20. Deverá implementar autenticação de usuários usando portal de captura;

3.10.3.21. Deve implementar autenticação de usuários usando WISPr e Hotspot 2.0.

3.10.3.22. Deverá suportar funções para análise de espectro.

3.10.3.23. Deve disponibilizar uma página local acessível pelo cliente conectado ao ponto de acesso para visualização de estatísticas de conexão e informações do respectivo ponto de acesso.

3.10.3.24. Deve suportar conversão de tráfego multicast para unicast.

3.10.3.25. Permitir a configuração e gerenciamento direto através de navegador padrão (HTTPS), SSH, SNMPv2c, SNMPv3.

3.10.3.26. Permitir que sua configuração seja realizada automaticamente quando este for conectado ao controlador WLAN do mesmo fabricante.

3.10.3.27. Implementar funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, das políticas de segurança, QoS, autenticação e monitoramento de RF.

3.10.3.28. Permitir que o processo de atualização de software seja realizado manualmente através de interface Web, FTP ou TFTP e automaticamente através de controlador WLAN do mesmo fabricante.

3.11. **PONTO DE ACESSO - TIPO 3**

3.11.1. **ESPECIFICAÇÕES GERAIS**

3.11.1.1. Deverá ser do mesmo fabricante do controlador WLAN para fins de compatibilidade.

3.11.1.2. Deverá possuir estrutura que permita a utilização do equipamento em locais internos, com fixação em teto e parede, devendo ser fornecidos todos os acessórios necessários para estas montagens.

3.11.1.3. Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto, com data anterior à publicação do edital, conforme a resolução 242. Não serão aceitos protocolos de entrada ou outros documentos diferentes do certificado, uma vez que os mesmos não garantem o fornecimento de equipamentos homologados e em conformidade com as leis brasileiras.

3.11.1.4. Deve ser compatível com o padrão UL2043, que regula os componentes dos materiais com o intuito de proteger contra danos causados por fogo, bem como pela fumaça.

3.11.1.5. Suportar, no mínimo, 256 (duzentos e cinquenta e seis) usuários wireless simultâneos, sem nenhum tipo de licença adicional.

3.11.1.6. Possuir suporte a pelo menos 16 (dezesseis) SSIDs por ponto de acesso.

3.11.1.7. Possibilitar alimentação elétrica local via fonte de alimentação DC e via padrão PoE (IEEE 802.3at ou 802.3bt). Ademais, para PoE, a alimentação elétrica deve ocorrer através de uma única interface de rede, sem perda de funcionalidade e de desempenho.

3.11.1.8. Deve suportar temperatura de operação entre 0°C a 40°C.

3.11.1.9. O equipamento ofertado não deverá possuir antenas aparentes externas ao ponto de acesso, evitando desta forma que as mesmas sejam removidas, o que ocasionaria na degradação do desempenho da rede sem fio.

3.11.1.10. Deverá possuir 1 (uma) interface ethernet multi-gigabit 1/2.5Gbps utilizando conector RJ-45, para conexão à rede local.

3.11.1.11. Deverá possuir LED para a indicação do status de operação do ponto de acesso.

3.11.1.12. Deverá ser fornecido com todas as funcionalidades de segurança, incluindo WIDS, e Wi-Fi Mesh habilitadas.

3.11.1.13. Deverá ser fornecido com a versão mais recente de software.

3.11.1.14. Deve ser compatível com IPv4 e IPv6.

3.11.2. **Características dos Rádios**

3.11.2.1. O ponto de acesso deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11ax e IEEE 802.11be, com operação nas frequências de 2.4 GHz, 5 GHz de forma simultânea.

3.11.2.2. Implementar as seguintes taxas de transmissão com fallback automático: IEEE 802.11b: 1 Mbps à 11 Mbps, IEEE 802.11a e IEEE 802.11g: 6 Mbps à 54 Mbps, IEEE 802.11n: 6.5 Mbps à 300 Mbps, IEEE 802.11ac: 6.5 Mbps à 860 Mbps, IEEE 802.11ax: 4 Mbps à 1774 Mbps e IEEE 802.11be: 4Mbps à 3570 Mbps.

3.11.2.3. Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11ax e IEEE 802.11be, com ganhos de no mínimo 3dBi nas frequências de 2,4GHz e 5GHz.

3.11.2.4. Deverá suportar potência agregada de saída, considerando todas as cadeias MIMO, de, no mínimo, 23 dBm nas frequências de 2,4 GHz e 5 GHz.

3.11.2.5. Deverá suportar canalização de 20 MHz, 40 MHz, 80 MHz e 160 MHz.

3.11.2.6. Deverá possuir mecanismo de rádio com suporte a 4 (quatro) fluxos espaciais simultâneos, sendo 2x2:2 em 2.4 GHz e 2x2:2 em 5 GHz, para SU-MIMO e MU-MIMO.

3.11.2.7. Deve permitir ajustes dinâmicos do sinal de rádio frequência para otimizar o tamanho da célula de abrangência do ponto de acesso.

3.11.2.8. Deve possuir capacidade de selecionar automaticamente o canal de transmissão.

3.11.2.9. Deve suportar os padrões IEEE 802.11r, IEEE 802.11k e IEEE 802.11v.

3.11.3. **Serviços, Segurança e Gerenciamento**

3.11.3.1. Deve permitir controle e gerenciamento pelo controlador WLAN através de Camada 2 ou 3 do modelo OSI.

3.11.3.2. Deve ser capaz de operar no modo Mesh sem adição de novo hardware ou alteração do sistema operacional, sendo que a comunicação até o controlador pode ser feita via wireless ou pela rede local.

3.11.3.3. Deve suportar auto cura por meio de Mesh em caso de falha da conexão cabeada de dados, bem como permitir que os pontos de acesso gerenciados estabeleçam automaticamente uma rede mesh sem fio.

3.11.3.4. Em caso de falha de comunicação entre os pontos de acesso e o controlador WLAN, os usuários associados à rede sem fio devem continuar conectados com acesso à rede. Além disso, deve ser possível que novos usuários se associem à rede sem fio utilizando autenticação do tipo IEEE 802.1X mesmo que os pontos de acesso estejam sem comunicação com a controladora.

3.11.3.5. Deve suportar, somente por meio do ponto de acesso em conjunto com o controlador de rede sem fio, a identificação e controle de aplicações dos dispositivos clientes conectados ao ponto de acesso, levando em consideração a camada 7 do modelo OSI.

3.11.3.6. Deve suportar a configuração de limite de banda por usuário ou por SSID.

3.11.3.7. Implementar cliente DHCP, para configuração automática de seu endereço IP e implementar também suporte a endereçamento IP estático.

3.11.3.8. Deve suportar VLANs conforme o padrão IEEE 802.1Q.

3.11.3.9. Deve suportar atribuição dinâmica de VLAN por usuário.

3.11.3.10. Deve implementar balanceamento de usuários por ponto de acesso.

3.11.3.11. Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2.4 GHz livre para dispositivos que trabalhem somente nesta frequência.

3.11.3.12. Deve implementar mecanismo para otimização de roaming entre pontos de acesso.

3.11.3.13. Implementar, pelo menos, os seguintes padrões de segurança wireless: (WPA) Wi-Fi Protected Access, (WPA2) Wi-Fi Protected Access 2, (WPA3) Wi-Fi Protected Access 3, (AES) Advanced Encryption Standard, (TKIP) Temporal Key Integrity Protocol, PSK privada (por usuário), IEEE 802.1X, IEEE 802.11i.

3.11.3.14. Deverá suportar MLO (Multi-Link Operation) e Preamble Puncturing.

3.11.3.15. Deverá permitir a criação de listas de controle de acesso de Camada 3 e 4 do modelo OSI.

3.11.3.16. Deverá ser possível criar políticas de controle com base no tipo ou sistema operacional do dispositivo.

3.11.3.17. Deve permitir habilitar e desabilitar a divulgação do SSID.

3.11.3.18. Deverá implementar autenticação de usuários usando portal de captura.

3.11.3.19. Deve implementar autenticação de usuários usando WISPr e Hotspot 2.0.

3.11.3.20. Deve suportar conversão de tráfego multicast para unicast.

3.11.3.21. Permitir a configuração e gerenciamento direto através de navegador padrão (HTTPS), SSH, SNMPv2c, SNMPv3 ou através do controlador, a fim de se garantir a segurança dos dados.

3.11.3.22. Deve suportar o protocolo LLDP.

3.11.3.23. Permitir que sua configuração seja realizada automaticamente quando este for conectado ao controlador WLAN do mesmo fabricante.

3.11.3.24. Implementar funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, das políticas de segurança, QoS, autenticação e monitoramento de RF.

3.11.3.25. Permitir que o processo de atualização de software seja realizado manualmente através de interface Web, FTP ou TFTP e automaticamente através de controlador WLAN do mesmo fabricante.

3.11.3.26. Deve permitir a formação de grupo de Pontos de Acesso gerenciados em modo cluster, sem necessidade de controlador WLAN dedicado, onde o próprio Ponto de Acesso atua como controlador e gerenciador dos outros APs do grupo. Nesse modo, deve permitir o gerenciamento de grupo de no mínimo 100 (cem) pontos de acesso que se comuniquem e compartilhem das mesmas configurações.

3.12. **PONTO DE ACESSO - TIPO 4**

3.12.1. **ESPECIFICAÇÕES GERAIS**

3.12.1.1. Deverá ser do mesmo fabricante do controlador WLAN para fins de compatibilidade.

3.12.1.2. Deverá possuir estrutura que permita a utilização do equipamento em locais internos, com fixação em teto e parede, devendo ser fornecidos todos os acessórios necessários para estas montagens.

3.12.1.3. Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto, com data anterior à publicação do edital, conforme a resolução 242. Não serão aceitos protocolos de entrada ou outros documentos diferentes do certificado, uma vez que os mesmos não garantem o fornecimento de equipamentos homologados e em conformidade com as leis brasileiras.

3.12.1.4. Deve ser compatível com o padrão UL2043, que regula os componentes dos materiais com o intuito de proteger contra danos causados por fogo, bem como pela fumaça.

3.12.1.5. Suportar, no mínimo, 700 (setecentos) usuários wireless simultâneos, sem nenhum tipo de licença adicional.

3.12.1.6. Possuir suporte a pelo menos 32 (trinta e dois) SSIDs por ponto de acesso.

3.12.1.7. Possibilitar alimentação elétrica local via fonte de alimentação DC e via padrão PoE (IEEE 802.3at ou 802.3bt). Ademais, para PoE, a alimentação elétrica deve ocorrer através de uma única interface de rede, sem perda de funcionalidade e de desempenho.

3.12.1.8. Deve suportar temperatura de operação entre 0°C a 50°C.

3.12.1.9. O equipamento ofertado não deverá possuir antenas aparentes externas ao ponto de acesso, evitando desta forma que as mesmas sejam removidas, o que ocasionaria na degradação do desempenho da rede sem fio.

3.12.1.10. Deverá possuir 2 (duas) interfaces ethernet, sendo 1 (uma) multi-gigabit 1/2.5/5 Gbps e 1 (uma) 10/100/1000 Mbps, utilizando conector RJ-45, para conexão à rede local.

3.12.1.11. Deverá possuir um rádio embarcado para IoT, o qual deve ser compatível com BLE e ZigBee, e deverá ter capacidade para Matter & Thread.

3.12.1.12. Deverá dispor de uma porta USB para inserção de módulo IoT compatível com BLE e ZigBee.

3.12.1.13. Deverá possuir LEDs para a indicação do status de operação do ponto de acesso.

3.12.1.14. Deverá ser fornecido com todas as funcionalidades de segurança, incluindo WIDS, e Wi-Fi Mesh habilitadas.

3.12.1.15. Deverá ser fornecido com a versão mais recente de software.

3.12.1.16. Deve ser compatível com IPv4 e IPv6.

3.12.2. **Características dos rádios**

3.12.2.1. O ponto de acesso deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11ax e IEEE 802.11be, com operação nas frequências de 2.4 GHz, 5 GHz e 6 GHz de forma simultânea.

3.12.2.2. Implementar as seguintes taxas de transmissão com fallback automático: IEEE 802.11b: 1 Mbps à 11 Mbps, IEEE 802.11a e IEEE 802.11g: 6 Mbps à 54 Mbps, IEEE 802.11n: 6.5 Mbps à 300 Mbps, IEEE 802.11ac: 6.5 Mbps à 860 Mbps, IEEE 802.11ax: 4 Mbps à 4800 Mbps e IEEE 802.11be: 4Mbps à 5760 Mbps.

3.12.2.3. Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11ax e IEEE 802.11be, com ganhos de no mínimo 3dBi nas frequências de 2,4GHz, 5GHz e 6GHz.

3.12.2.4. Deverá suportar potência agregada de saída, considerando todas as cadeias MIMO, de, no mínimo, 24 dBm nas frequências de 2,4 GHz, 5 GHz e 6 GHz.

3.12.2.5. Deverá suportar canalização de 20 MHz, 40 MHz, 80 MHz, 160 MHz e 320 MHz.

3.12.2.6. Deverá possuir mecanismo de rádio com suporte a 6 (seis) fluxos espaciais simultâneos, sendo 2x2:2 em 2.4 GHz, 2x2:2 em 5 GHz e 2x2:2 em 6 GHz, para SU-MIMO e MU-MIMO.

3.12.2.7. Deve permitir que o AP opere em MIMO 4x4:4 em 5GHz, mesmo que para isso o AP deva ser configurado em modo dual-band (2.4GHz e 5GHz).

3.12.2.8. Deve permitir ajustes dinâmicos do sinal de rádio frequência para otimizar o tamanho da célula de abrangência do ponto de acesso.

3.12.2.9. Deve possuir capacidade de selecionar automaticamente o canal de transmissão.

3.12.2.10. Deve suportar os padrões IEEE 802.11r, IEEE 802.11k e IEEE 802.11v.

3.12.3. **Serviços, segurança e gerenciamento**

3.12.3.1. Deve permitir controle e gerenciamento pelo controlador WLAN através de Camada 2 ou 3 do modelo OSI.

3.12.3.2. Deve ser capaz de operar no modo Mesh sem adição de novo hardware ou alteração do sistema operacional, sendo que a comunicação até o controlador pode ser feita via wireless ou pela rede local.

3.12.3.3. Deve suportar auto cura por meio de Mesh em caso de falha da conexão cabeada de dados, bem como permitir que os pontos de acesso gerenciados estabeleçam automaticamente uma rede mesh sem fio.

3.12.3.4. Em caso de falha de comunicação entre os pontos de acesso e o controlador WLAN, os usuários associados à rede sem fio devem continuar conectados com acesso à rede. Além disso, deve ser possível que novos usuários se associem à rede sem fio utilizando autenticação do tipo IEEE 802.1X mesmo que os pontos de acesso estejam sem comunicação com a controladora.

3.12.3.5. Deve suportar, somente por meio do ponto de acesso em conjunto com o controlador de rede sem fio, a identificação e controle de aplicações dos dispositivos clientes conectados ao ponto de acesso, levando em consideração a camada 7 do modelo OSI.

3.12.3.6. Deve suportar a configuração de limite de banda por usuário ou por SSID.

3.12.3.7. Implementar cliente DHCP, para configuração automática de seu endereço IP e implementar também suporte a endereçamento IP estático.

3.12.3.8. Deve suportar VLANs conforme o padrão IEEE 802.1Q.

3.12.3.9. Deve suportar atribuição dinâmica de VLAN por usuário.

3.12.3.10. Deve implementar balanceamento de usuários por ponto de acesso.

3.12.3.11. Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2.4 GHz livre para dispositivos que trabalhem somente nesta frequência.

3.12.3.12. Deve implementar mecanismo para otimização de roaming entre pontos de acesso.

3.12.3.13. Implementar, pelo menos, os seguintes padrões de segurança wireless: (WPA) Wi-Fi Protected Access, (WPA2) Wi-Fi Protected Access 2, (WPA3) Wi-Fi Protected Access 3, (AES) Advanced Encryption Standard, (TKIP) Temporal Key Integrity Protocol, PSK privada (por usuário), IEEE 802.1X, IEEE 802.11i e OWE.

3.12.3.14. Deverá suportar TPM 2.0.

3.12.3.15. Deverá suportar MLO (Multi-Link Operation) e Preamble Puncturing.

3.12.3.16. Deverá permitir a criação de filtros de endereços MAC de forma a restringir o acesso à rede sem fio.

3.12.3.17. Deverá permitir a criação de listas de controle de acesso de Camada 3 e 4 do modelo OSI.

3.12.3.18. Deverá ser possível criar políticas de controle com base no tipo ou sistema operacional do dispositivo.

3.12.3.19. Deve permitir habilitar e desabilitar a divulgação do SSID.

3.12.3.20. Deverá implementar autenticação de usuários usando portal de captura.

3.12.3.21. Deve implementar autenticação de usuários usando WISPr e Hotspot 2.0.

3.12.3.22. Deve suportar conversão de tráfego multicast para unicast.

3.12.3.23. Permitir a configuração e gerenciamento direto através de navegador padrão (HTTPS), SSH, SNMPv2c, SNMPv3 ou através do controlador, a fim de se garantir a segurança dos dados.

3.12.3.24. Deve suportar o protocolo LLDP.

3.12.3.25. Permitir que sua configuração seja realizada automaticamente quando este for conectado ao controlador WLAN do mesmo fabricante.

3.12.3.26. Implementar funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, das políticas de segurança, QoS, autenticação e monitoramento de RF.

3.12.3.27. Permitir que o processo de atualização de software seja realizado manualmente através de interface Web, FTP ou TFTP e automaticamente através de controlador WLAN do mesmo fabricante.

3.12.3.28. Deve permitir a formação de grupo de Pontos de Acesso gerenciados em modo cluster, sem necessidade de controlador WLAN dedicado, onde o próprio Ponto de Acesso atua como controlador e gerenciador dos outros APs do grupo. Nesse modo, deve permitir o gerenciamento de grupo de no mínimo 100 (cem) pontos de acesso que se comuniquem e compartilhem das mesmas configurações.

3.13. **PONTO DE ACESSO - TIPO 5**

3.13.1. **ESPECIFICAÇÕES GERAIS**

3.13.1.1. Equipamento de ponto de acesso para rede local sem fio deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax com operação nas frequências de 2.4 GHz e 5 GHz de forma simultânea

3.13.1.2. Deverá ser do mesmo fabricante do Controlador WLAN

3.13.1.3. Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto, com data anterior à publicação do edital, conforme a resolução 242. Não serão aceitos protocolos de entrada ou outros documentos diferentes do certificado, uma vez que os mesmos não garantem o fornecimento de equipamentos homologados e em conformidade com as leis brasileira

3.13.1.4. Possuir antenas internas e integradas com padrão de irradiação omnidirecional, compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax.

3.13.1.5. Não serão aceitos equipamentos com antenas aparentes (externas ao ponto de acesso) que sejam rosqueáveis, permitindo a remoção das antenas

3.13.1.6. Deve suportar potência de saída de no mínimo 22 dBm com operação na frequência 5GHz e de no mínimo 22 dBm com operação na frequência 2.4GHz

3.13.1.7. Deve suportar ganho de antena de no mínimo 2 dBi para 2.4GHz e 3dBi para 5GHz

3.13.1.8. Deverá atender aos padrões IEEE 802.11d e IEEE 802.11h

3.13.1.9. Deverá suportar canalização de 20 MHz, 40 MHz e 80MHz

3.13.1.10. Deverá possuir mecanismo de rádio com suporte à MIMO 2x2 com 2 Spatial Streams

3.13.1.11. Deverá suportar Multi User MIMO (MU-MIMO)

3.13.1.12. Deverá, em conjunto com o controlador de rede sem fio, permitir a análise de espectro do ambiente em modo dedicado ou simultâneo ao fornecimento de serviço aos dispositivos clientes.

3.13.1.13. Deverá suportar meio de direcionamento de sinal para ganho de desempenho

3.13.1.14. Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2,4 GHz livre para dispositivos que trabalhem somente nesta frequência.

3.13.1.15. Deve suportar, em conjunto com o controlador de rede sem fio, a identificação e controle de aplicações dos dispositivos clientes conectados ao ponto de acesso.

3.13.1.16. Deve suportar, em conjunto com o controlador de rede sem fio, a configuração de limite de banda (rate limit) por usuário e por SSID.

3.13.1.17. Deve oferecer suporte ao mecanismo de localização e rastreamento de usuários (Location Based Service)

3.13.1.18. Deverá possuir, no mínimo, 01 (uma) interface IEEE 802.3 10/100/1000 Mbps Base-T Ethernet, auto-sensing, com conector RJ-45, para conexão à rede local fixa.

3.13.1.19. É desejável possuir LEDs para a indicação do status: portas ethernets, rede wireless, gerenciamento via controladora e atividades do equipamento

3.13.1.20. Deverá possuir o padrão de alimentação IEEE 802.3af (PoE) ou IEEE 802.3at (PoE).

3.13.1.21. Deve suportar temperatura de operação entre -20°C a 65°C com PoE ativado

3.13.1.22. Deverá possuir certificação IP67

3.13.1.23. Deverá possuir estrutura que permita a utilização do equipamento em locais internos e externos, com fixação em teto, parede e também em poste e fornecer acessórios para que possa ser feita a fixação

3.13.1.24. Deverá ser fornecido com todas as funcionalidades de segurança instaladas. Não deve haver licença restringindo itens de segurança do equipamento e nem a quantidade de usuários conectados

3.13.1.25. Funcionar via configuração do controlador no modo de MESH (WiFi Mesh) sem adição de novo hardware ou alteração do sistema operacional, sendo a comunicação até o controlador efetuada via wireless ou por pelo menos 02 pontos ethernet conectados ao controlador ou a uma rede local

3.13.1.26. Deverá ser fornecido com todas as licenças para funcionamento em MESH (WiFi Mesh)

3.13.2. **GERENCIAMENTO**

3.13.2.1. Permitir a configuração e gerenciamento direto através de browser padrão (HTTPS), SSH, SNMPv2c e SNMPv3, ou através do controlador, a fim de garantir a segurança dos dados

3.13.2.2. Permitir gerenciamento através de plataformas de software que sigam padrões SNMPv2c e SNMPv3

3.13.2.3. Implementar funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, das políticas de segurança, QoS, autenticação e monitoramento de RF

3.13.2.4. Permitir que sua configuração seja automaticamente realizada quando este for conectado no ambiente de rede do Controlador WLAN.

3.13.2.5. O ponto de acesso poderá estar diretamente ou remotamente conectado ao controlador WLAN, inclusive via roteamento da camada 3 de rede OSI

3.13.2.6. O ponto de acesso deverá conectar-se ao controlador WLAN através de túnel seguro padrão ou através de protocolo de comunicação seguro que ofereça controle total do equipamento

3.13.2.7. Permitir ajustes dinâmicos de RF modo a otimizar o tamanho da célula de abrangência de RF

3.13.2.8. Permitir que o processo de atualização de versão seja realizado manualmente através da WEB ou FTP ou TFTP e automaticamente através do Controlador WLAN descrito neste documento.

3.13.3. **REDE**

3.13.3.1. Implementar cliente DHCP, para configuração automática do seu endereço IP e implementar também endereçamento IP estático

3.13.3.2. Deve suportar VLAN seguindo a norma IEEE 802.1q

3.13.3.3. Possuir suporte a pelo menos 30 SSIDs por ponto de acesso

3.13.3.4. Permitir habilitar e desabilitar a divulgação do SSID

3.13.3.5. Possuir capacidade de selecionar automaticamente o canal de transmissão

3.13.3.6. Suportar, no mínimo, 500 (quinhentos) usuários wireless simultâneos

3.13.3.7. Deve suportar limitação de banda por grupo de usuário ou SSID

3.13.3.8. Implementar, pelo menos, os seguintes padrões de segurança wireless:

3.13.3.8.1. (WPA) Wi-Fi Protected Access

3.13.3.8.2. (WPA2) Wi-Fi Protected Access 2

3.13.3.8.3. (WPA3) Wi-Fi Protected Access 3

3.13.3.8.4. (AES) Advanced Encryption Standard

3.13.3.8.5. (TKIP) Temporal Key Integrity Protocol

3.13.3.8.6. IEEE 802.1x

3.13.3.8.7. IEEE 802.11i

3.13.3.9. Implementar as seguintes taxas de transmissão e com fallback automático:

3.13.3.9.1. IEEE 802.11b: 11 Mbps

3.13.3.9.2. IEEE 802.11a e IEEE 802.11g: 54 Mbps

3.13.3.9.3. IEEE 802.11n: 300Mbps

3.13.3.9.4. IEEE 802.11ac: 867Mbps

3.13.3.9.5. IEEE 802.11ax: 1200Mbps

3.13.3.10. Deverá permitir a criação de filtros de MAC address de forma a restringir o acesso à rede wireless

4. GESTÃO DE ATIVOS DE REDE, MONITORAMENTO E SEGURANÇA - REQUISITOS GERAIS:

4.1. **Especificações Gerais**

4.1.1. A solução deve vir acompanhada de todos os acessórios necessários para sua operacionalização, tais como softwares, licenças, documentações técnicas e manuais que contenham informações suficientes, que possibilite a instalação, configuração e operacionalização da solução.

4.1.2. O controlador WLAN deverá ser do tipo virtual e compatível com os ambientes VMWare 6.7 e superiores, Hyper-V Windows 2016 e 2019, KVM CentOS 7.4 e superiores, AWS, MS Azure ou GCE. O ambiente virtualizado deverá ser disponibilizado em servidor ou servidores da Contratante com as especificações recomendadas pelo fabricante da solução;

4.1.3. Não serão aceitas soluções baseadas nas premissas de pontos de acesso autônomos ou controladores agregados a outros equipamentos, tais como Switches, Firewalls, Roteadores ou até mesmo controlador virtual dentro do próprio ponto de acesso;

4.1.4. Não serão aceitos sistemas implementados em virtualizadores de desktop, tais como Oracle VM VirtualBox ou VMware Workspace;

4.1.5. Deverá ser do mesmo fabricante dos pontos de acesso e switches fornecidos pela Contratada, para fins de compatibilidade e gerenciamento.

4.1.6. Deverá suportar a operação como um cluster (N+1) para prover resiliência e desempenho, podendo o mesmo ser composto por, no mínimo, 2 (dois) controladores e expansível até 4 (quatro) controladores.

4.1.7. Deve ser acompanhado de todos os acessórios necessários para operacionalização da solução, tais como softwares, documentações técnicas e manuais que contenham informações suficientes, que possibilitem a instalação, configuração e operacionalização da solução.

4.1.8. Deve possuir uma arquitetura modular do tipo multi-tenant, permitindo gestão centralizada, mas com acesso independente e isolado para cada domínio.

4.1.9. Deverá suportar pontos de acesso internos e externos nos padrões 802.11a/b/g/n/ac/ax/be.

4.1.10. Deverá suportar switches de camada 2 e camada 3 com densidade de portas de 1GbE até 100GbE.

4.1.11. Deverá possuir suporte a RESTful API compatível com JSON e disponibilizar suporte às funções GET, POST, DELETE, PUT e PATCH.

4.2. **Gerenciamento dos Pontos de Acesso**

4.2.1. Suportar o gerenciamento de pelo menos 5.000 (cinco mil) Pontos de Acesso na sua capacidade máxima. Caso a solução trabalhe com licenciamento para esse fim, estas deverão ser fornecidas juntamente com cada Ponto de acesso;

4.2.2. Suportar, no mínimo 100.000 (cem mil) dispositivos clientes simultâneos por controlador.

4.2.3. Prover o gerenciamento centralizado dos Pontos de Acesso, suportando versões de firmware diferentes.

4.2.4. Deverá permitir gerenciamento através de Endereço IP, Range de IPs e Sub-Redes pré-configuradas

4.2.5. Permitir a configuração total dos pontos de acesso, assim como os aspectos de segurança da rede wireless (WLAN) e Rádio Frequência (RF)

4.2.6. O controlador WLAN poderá estar diretamente e/ou remotamente conectado aos Pontos de Acesso por ele gerenciados, inclusive via roteamento em camada 3 do modelo OSI

4.2.7. Possibilitar a configuração de envio dos eventos do Controlador WLAN para um servidor de Syslog remoto

4.2.8. Implementar, pelo menos, os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps SNMP

4.2.9. Permitir a visualização de alertas da rede em tempo real

4.2.10. Implementar, no mínimo, dois níveis de acesso administrativo ao equipamento (apenas leitura e leitura/escrita) protegidos por senhas independentes

4.2.11. Permitir a customização do acesso administrativo através de atribuição de grupo de função do usuário administrador

4.2.12. Permitir a configuração e gerenciamento através de navegador padrão (HTTPS).

4.2.13. Gerenciar de forma centralizada a autenticação de usuários

4.2.14. Permitir o envio de alertas ou alarmes através do protocolo SMTP, sendo que a comunicação com o servidor deverá ser autenticada e cifrada (SMTP/TLS)

4.2.15. Permitir que o processo de atualização de versão seja realizado através de navegador padrão (HTTPS) ou SSH.

4.2.16. Deverá possuir a capacidade de importação de certificados digitais emitidos por uma autoridade certificadora externa;

4.2.17. A disponibilidade da rede sem fio deve ser passível de agendamento para, no mínimo, as opções a seguir:

4.2.17.1. 24 horas por dia, 7 dias na semana

4.2.17.2. Agendamento customizado permitindo escolher os dias da semana e horários

4.2.17.3. Os horários definidos não precisam ser sequenciais, ou seja, a solução deve suportar que o administrador defina o horário de funcionamento das 08:00 às 12:00 e 14:00 às 18:00.

4.2.18. Possuir ferramentas de diagnóstico e log de eventos para depuração e gerenciamento em primeiro nível.

4.2.19. Possuir ferramenta que permite o monitoramento em tempo real de informações de utilização de CPU, memória e estatísticas de rede

4.2.20. Possibilitar cópia “backup” da configuração, bem como a funcionalidade de restauração da configuração através de navegador padrão (HTTPS) ou FTP ou TFTP.

4.2.21. Possuir a capacidade de armazenar múltiplos arquivos de configuração do controlador pertencente à rede sem fio

4.2.22. Monitorar o desempenho da rede sem fio, permitindo a visualização de informações de cada ponto de acesso.

4.2.23. Deve suportar a possiblidade de trabalhar com cluster de controladores WLAN no modo ativo/ativo, com sincronismo automático das configurações entre controladores para suporte a redundância em alta disponibilidade (HA - high availability). Não há necessidade de ofertar a solução de cluster redundantes nesse certame. O cluster deve ter suporte as seguintes funcionalidades:

4.2.24. Deverá suportar o compartilhamento de recursos e licenças de pontos de acesso entre os controladores participantes do cluster

4.2.25. Deverá, em caso de falha, suportar a redundância de forma automática e sem nenhuma necessidade de intervenção do administrador de rede

4.2.26. Deverá possuir a capacidade de geração de informações ou relatórios de, no mínimo, os seguintes tipos: Listagem de clientes Wireless, Listagem de Pontos de Acesso, utilização da rede.

4.2.27. Deverá suportar, somente por meio do controlador e do ponto de acesso, a identificação de aplicações dos clientes conectados com base na camada 7 do modelo OSI, permitindo o controle de acesso, de banda (uplink e/ou downlink) e definição de regra de QoS para estas aplicações.

4.2.28. Permitir visualizar a localização dos pontos de acesso e através desta obter o status de funcionamento dos mesmos.

4.2.29. Deverá possibilitar a importação de plantas baixas nos formatos DWG ou JPG ou PNG, devendo permitir a visualização dos Pontos de Acesso instalados com seu estado de funcionamento, bem como disponibilizar uma visualização da cobertura do sinal em 2.4GHz, 5GHz ou 6GHz.

4.2.30. Deve ser capaz de localizar clientes wireless na planta baixa adicionada no sistema;

4.2.31. Implementar funcionalidade de análise espectral, permitindo a detecção de interferências no ambiente de rede sem fio.

4.2.32. Implementar análise de tráfego por WLAN, Ponto de acesso e dispositivos cliente, apresentando os 10 itens mais usados.

4.2.33. Deve ser possível definir o nível de segurança administrativo da solução suportando, no mínimo:

4.2.33.1. Habilitar Captcha para Acesso

4.2.33.2. Período em dias para alteração obrigatória da senha

4.2.33.3. Política para reutilização de senha

4.2.33.4. Comprimento mínimo da senha e complexidade

4.2.33.5. Segundo Fator de Autenticação via SMS

4.2.34. A solução deve suportar a adição de um serviço de SMS externo, tal como Twilio.

4.2.35. Implementar funcionalidade de análise espectral em tempo real e por frequência, 2.4GHz ou 5GHz permitindo a detecção de interferências e geração de gráficos de uso do ambiente de rede sem fio;

4.2.36. Deve suportar integração com tags da Ekahau e AeroScout/Stanley para Real-Time Location Service (RTLS);

4.3. **REDE**

4.3.1. Deverá implementar suporte aos protocolos IPv4 e IPv6

4.3.2. Deverá suportar tagging de VLANs

4.3.3. Implementar associação dinâmica de usuário a VLAN com base nos parâmetros da etapa de autenticação via IEEE 802.1x.

4.3.4. Suportar associação dinâmica de ACL e de QoS por usuário, com base nos parâmetros da etapa de autenticação.

4.3.5. Deverá suportar, no mínimo, 1030 (mil e trinta) SSIDs simultâneos

4.3.6. Deverá possuir funcionalidade de balanceamento de carga entre VLANs e permitir que clientes sejam designados para diferentes VLANs dentro de um mesmo SSID, com suporte a até 50 VLANs por pool.

4.3.7. Em caso de falha de comunicação entre os pontos de acesso e a controladora, os usuários associados à rede sem fio devem continuar conectados com acesso à rede. Também deve permitir

que novos usuários se associem à rede sem fio utilizando autenticação do tipo 802.1X mesmo que os pontos de acesso estejam sem comunicação com a controladora

4.3.8. Deve ser possível evitar que dispositivos 802.11b se conectem a rede, visando melhorar o desempenho da rede sem fio.

4.3.9. Deve suportar 802.11d e 802.11k.

4.3.10. Deve suportar captura de pacotes por ponto de acesso para resolução de problemas, sendo possível definir a captura nos rádios de 2.4 GHz, 5 GHz e 6GHz, bem como na interface LAN. Ainda, a operação deve ser realizada via interface Web e deve ser possível exportar o arquivo de captura para análise local em software de análise de pacote, tal como Wireshark.

4.3.11. Deve ser possível rastrear a conexão de um cliente wireless em tempo real para analisar problemas de conectividade e identificar em qual estágio o problema aconteceu.

4.3.12. Deve ser possível estabelecer um limite para o nível de sinal visando permitir que o cliente se junte à rede sem fio, o qual deve ser estabelecido em dBm e variar entre -60dBm e -90dBm.

4.3.13. Deverá suportar de forma centralizada a configuração de agregação de portas (LACP) ethernet dos pontos de acesso que possuírem suporte a essa funcionalidade.

4.3.14. Deve suportar auto configuração e auto correção para rede Mesh.

4.4. **SEGURANÇA WLAN**

4.4.1. Os itens a seguir devem estar integrados a solução ofertada, não serão aceitos equipamentos externos à solução. Caso sejam necessárias licenças ou softwares de controle os mesmos devem ser fornecidos de forma que a solução esteja operacional e sem nenhuma restrição no ato de sua implementação (hardware e softwares necessários para implementação)

4.4.2. Implementar, pelo menos, os seguintes padrões e funcionalidades de segurança wireless:

4.4.2.1. (WPA) Wi-Fi Protected Access;

4.4.2.2. (WPA2) Wi-Fi Protected Access 2;

4.4.2.3. (WPA3) Wi-Fi Protected Access 3;

4.4.2.4. (TKIP) Temporal Key Integrity Protocol;

4.4.2.5. (AES) Advanced Encryption Standard;

4.4.2.6. PSK (pre-shared key) único por dispositivo cliente em um mesmo SSID;

4.4.2.7. IEEE 802.1X;

4.4.2.8. IEEE 802.11i;

4.4.2.9. IEEE 802.11w.

4.4.3. Implementar, pelo menos, os seguintes controles/filtros:

4.4.3.1. Baseado em endereço MAC e isolamento de cliente na camada 2 do modelo OSI;

4.4.3.2. Baseado em endereço IP;

4.4.3.3. Baseado em protocolo, tais como TCP, UDP, ICMP e IGMP;

4.4.3.4. Baseado em porta de origem e/ou destino;

4.4.3.5. Baseado em tipo ou sistema operacional do dispositivo.

4.4.4. Permitir a autenticação para acesso dos usuários conectados nas redes WLAN (Wireless) através:

4.4.4.1. MAC Address;

4.4.4.2. Autenticação Local;

4.4.4.3. Captive Portal;

4.4.4.4. Active Directory;

4.4.4.5. RADIUS;

4.4.4.6. IEEE 802.1x;

4.4.4.7. LDAP.

4.4.5. Deverá permitir a seleção/uso de servidor RADIUS específico com base no SSID.

4.4.6. Deverá suportar servidor de autenticação RADIUS redundante. Isto é na falha de comunicação com o servidor RADIUS principal, o sistema deverá buscar um servidor RADIUS secundário.

4.4.7. A solução deverá suportar a criação de uma zona de visitantes, que terá seu acesso controlado através de senha cadastrada internamente, sendo que esta deverá possuir a configuração de tempo pré-determinado de acesso a rede sem fio.

4.4.8. O controlador deverá permitir a criação de múltiplos usuários visitantes (guests) de uma única vez (em lote).

4.4.9. Deve ser possível definir o período de validade da senha de visitantes em quantidade de horas, dias e semanas.

4.4.10. Deve permitir que após o processo de autenticação de usuários visitantes (guests) os mesmos sejam redirecionados para uma página de navegação específica e configurável.

4.4.11. Deve permitir que múltiplos usuários visitantes (guests) compartilhem a mesma senha de acesso à rede.

4.4.12. Deverá dispor de opção para enviar a senha de usuários visitantes (guests) por e-mail ou por SMS.

4.4.13. Deverá permitir que um usuário visitante se cadastre automaticamente através de funcionalidade do tipo “self registration”.

4.4.14. Deverá permitir o encaminhamento do tráfego de saída de usuários visitantes (guests) diretamente para a Internet, de forma totalmente separada do tráfego da rede corporativa.

4.4.15. Deve implementr login social com no mínimo, Linkedin, Google, Microsoft e Facebook.

4.4.16. Deverá permitir o isolamento do tráfego unicast, multicast ou ambos entre usuários visitantes (guests) em uma mesma VLAN/Subnet, sendo possível adicionar exceções com base em endereços MAC e IP.

4.4.17. Deverá ser possível permitir que o ponto de acesso filtre todo o tráfego IPv4 e IPv6 dos tipos multicast e broadcast dos clientes sem fio associados, com exceção de alguns tráfegos pertencentes a uma lista de exclusões, tais como ARP, DHCPv4 e DHCPv6, MLD, IGMP, IPv6 NS, IPv6 NA, IPv6 RS e todos pacotes do tipo unicast.

4.4.18. Deverá ser possível especificar o tipo de serviço Bonjour que será permitido entre VLANs.

4.4.19. Deve suportar mecanismo de acesso de acordo com o padrão Hotspot 2.0

4.4.20. Deve implementar mecanismos de segurança e proteção da rede sem fio contemplando, no mínimo, os recursos abaixo:

4.4.20.1. SSID Spoofing – Detectar APs não pertencentes ao controlador propagando o mesmo SSID;

4.4.20.2. MAC Spoofing – Detectar APs não pertencentes ao controlador propagando o mesmo MAC de um AP válido;

4.4.20.3. Rogue APs – Detectar APs não pertencentes ao controlador;

4.4.20.4. Same Network – Detectar APs não pertencentes ao controlador exibindo qualquer SSID pertencentes ao mesmo segmento de rede LAN;

4.4.20.5. Ad Hoc – Possibilidade de detectar rede Ad Hoc como Rogue;

4.4.20.6. Flood de Deauthentication – Detectar quando há um número excessivo de frames de desautenticação oriundos de um mesmo transmissor;

4.4.20.7. Flood de Disassociation – Detectar quando há um número excessivo de frames de desassociação oriundos de um mesmo transmissor;

4.4.20.8. Excesso de Clear to Send (CTS) – Detectar quando há um número excessivo de frames de CTS para um endereço MAC específico;

4.4.20.9. Excesso de Request to Send (RTS) – Detectar quando há um número excessivo de frames de RTS para um endereço MAC específico;

4.4.20.10. Excesso de Energia – Possibilidade de detectar tráfego com nível de potência de transmissão excessivo;

4.4.20.11. Deve implementar varredura de rádio frequência para identificação de ataques e Pontos de Acesso intrusos não autorizados (rogues);

4.4.20.12. Deve fazer a varredura no canal de operação do Ponto de Acesso sem impacto na performance da rede WLAN;

4.4.20.13. Deve utilizar os Pontos de Acesso para fazer a monitoração do ambiente Wireless procurando por pontos de acesso do tipo rogue de forma automática;

4.4.20.14. Deve ser possível especificar um ponto de acesso ou grupo de pontos de acesso para atuarem somente com a função de monitoramento visando detectar ataques e analisar o ambiente de rádio frequência;

4.4.20.15. Deverá ser capaz de localizar Pontos de Acesso do tipo rogue na planta baixa adicionada ao sistema com informações de, no mínimo:

4.4.20.15.1. Pontos de Acesso que detectam;

4.4.20.15.2. Tipo de Rogue;

4.4.20.15.3. Nome da Rede;

4.4.20.15.4. Nível de sinal de detecção.

4.5. **RECURSOS DE GERENCIAMENTO AUTOMÁTICO DE RÁDIO FREQUÊNCIA (RF)**

4.5.1.1. Na ocorrência de inoperância de um Ponto de Acesso, o controlador WLAN deverá ajustar automaticamente a potência dos Pontos de Acesso adjacentes, de modo a prover a cobertura da área não assistida.

4.5.1.2. Ajustar automaticamente a utilização de canais de modo a otimizar a cobertura de rede e mudar as condições de RF baseado em desempenho.

4.5.1.3. Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura de RF de forma automática.

4.5.1.4. Implementar sistema automático de balanceamento de carga para associação de clientes entre Pontos de Acesso próximos para otimizar o desempenho.

4.5.1.5. Implementar funcionalidade de balanceamento de carga entre os rádios de um mesmo Ponto de Acesso.

4.5.1.6. Permitir que o serviço wireless seja desabilitado de determinado ponto de acesso. Também deve ser possível selecionar o serviço de qual rádio (banda) de determinado ponto de acesso deve ser desabilitado.

4.6. **RECURSOS DE CONVERGÊNCIA E MULTIMÍDIA**

4.6.1.1. Suportar 802.11e

4.6.1.2. Deverá possuir funcionalidade de configuração do limite de banda disponível por usuário ou através de SSID/BSSID.

4.6.1.3. Deverá permitir a configuração de prioridade de um determinado SSID sobre outros SSIDs existentes na controladora.

4.6.1.4. Deve suportar WiFi Calling.

4.7. **GERENCIAMENTO DOS SWITCHES**

4.7.1.1. Deverá ser do mesmo fabricante dos Switches fornecidos neste certame, para fins de compatibilidade;

4.7.1.2. Suportar o gerenciar pelo menos 1000 (mil) switches na sua capacidade máxima. Caso a solução trabalhe com licenciamento para esse fim, estas deverão ser fornecidas juntamente com cada Switch;

4.7.1.3. Deve ser possível gerenciar Switches com perfis de Camada 2 e Camada 3.

4.7.1.4. Deve ser capaz de gerenciar todos os switches fornecidos neste certame.

4.7.1.5. Deve ser possível criar grupos lógicos de switches para facilitar a gestão.

4.7.1.6. Deve ser possível associar um switch automaticamente com um respectivo grupo de switches por meio de regras de registro, as quais devem ser definidas por, pelo menos, um dos meios a seguir: faixa de endereço IP, sub-rede ou modelo do switch.

4.7.1.7. Deve realizar backup da configuração dos switches diariamente, mantendo, no mínimo, um histórico das últimas 7 (sete) versões de arquivos de configurações.

4.7.1.7.1. A configuração só deve ser armazenada se houver alguma alteração entre o último backup e o backup atual.

4.7.1.8. Deve ser possível executar um backup manual.

4.7.1.9. Deve suportar a restauração de um determinado backup.

4.7.1.10. Deve dispor de uma opção para visualizar um determinado arquivo de configuração, bem como permitir analisar as diferenças entre arquivos de configurações distintos realçando-as para fácil identificação.

4.7.1.11. Deve permitir a atualização de firmware dos switches de modo individual e em grupos, bem como manter o histórico das atualizações de cada switch.

4.7.1.12. Deve permitir o agendamento de atualização de firmware dos switches de modo individual e em grupos.

4.7.1.13. Deve ser possível definir configurações comuns a um grupo de switches, tais como configurações de DNS e AAA (Authentication, Authorization e Accounting).

4.7.1.13.1. As configurações de AAA devem permitir habilitar ou desabilitar a autenticação, autorização e accounting para SSH ou Telnet, incluindo a seleção da ordem de preferência dos servidores AAA.

4.7.1.13.2. Para autenticação, deve ser possível definir servidor Radius, TACACS+ e usuário local.

4.7.1.13.3. Para autorização e accounting, deve ser possível definir servidor Radius e TACACS+.

4.7.1.14. Deverá possibilitar a criação de Listas de Controle de Acesso (ACL) do tipo padrão ou estendida e permitir a definição de quando a configuração deve ser aplicada no switch, se imediatamente ou por meio de agendamento.

4.7.1.15. Deverá permitir a criação de VLANs, permitindo atribuir um nome a esta VLAN, bem como definir quais portas devem ser untagged ou tagged.

4.7.1.16. Deve ser possível configurar DHCP Snooping, ARP Inspection e IP Source Guard.

4.7.1.17. Deve ser possível configurar IGMP Snooping Ativo ou Passivo.

4.7.1.18. Deve suportar configurações de Spanning Tree, tais como permitir definir entre STP (802.1d) ou RSTP (802.1w) e sua respectiva prioridade.

4.7.1.19. Deverá ser possível criar rotas estáticas e permitir a definição de quando a configuração deve ser aplicada no switch, se imediatamente ou por meio de agendamento.

4.7.1.20. Deve disponibilizar um histórico das configurações criadas, demonstrando o tipo de configuração, a data e o período em que foram criadas, bem como se a mesma foi implementada com sucesso ou se houve alguma falha.

4.7.1.21. Deve ser possível definir um hostname para cada switch.

4.7.1.22. Deve ser possível habilitar Jumbo Frame.

4.7.1.23. Deve suportar DHCP Server e DHCP Relay.

4.7.1.24. Deve dispor de funcionalidade para copiar configurações de um determinado switch para um ou mais switches.

4.7.1.25. Deve ser possível criar LAGs (Link Aggregation Group) do tipo estático ou dinâmico.

4.7.1.26. Deve ser possível criar empilhamento de switches.

4.7.1.27. Deve ser possível habilitar ou desabilitar uma porta, bem como definir um nome para cada porta.

4.7.1.28. Deve ser possível habilitar ou desabilitar PoE, bem como definir a classe ou prioridade PoE.

4.7.1.29. Deve ser possível definir configurações de camada 3 para uma porta como, por exemplo, área OSPF e endereço IP.

4.7.1.30. Deve permitir a visualização de alarmes relacionados ao switch, incluindo, mas não se limitando a: falha de uma fonte de alimentação, falha de um membro do empilhamento ou falha na alocação de PoE.

4.7.1.31. Deve permitir a detecção e visualização de eventos relacionados ao switch com base em certas condições, bem como permitir o envio de notificações por E-mail e Traps SNMP.

4.7.1.32. Deve ser possível criar eventos customizados, podendo definir o texto que um evento deve conter, condição em quantidade de vezes, janela de tempo em horas e severidade.

4.7.1.33. Deve dispor de painel gráfico com o estado das portas dos switches.

4.7.1.34. Deve disponibilizar um detalhamento das portas de um switch demonstrando, no mínimo, o nome da porta, o estado da porta (UP/DOWN), o estado administrativo da porta (UP/DOWN), a velocidade, a utilização de PoE para portas PoE, a utilização de banda (in/out), total de pacotes multicast (in/out), total de pacotes broadcast (in/out), número de pacotes com erro (in/out), erros de CRC e número de pacotes inbound descartados.

4.7.1.35. Deve disponibilizar graficamente a visão do painel frontal de um determinado switch permitindo visualizar, no mínimo, as seguintes informações de uma determinada porta: nome da porta, estado da porta (UP/DOWN), VLANs Untagged e Tagged, e, para portas PoE, a utilização de PoE.

4.7.1.36. Deve disponibilizar uma visão da topologia dos dispositivos gerenciados.

4.7.1.37. Deve possuir painéis demonstrando o volume de tráfego total para todos os switches ou para os switches de um grupo, bem como listar os principais switches do sistema por volume de tráfego, por erro de porta e por utilização de PoE.

4.7.1.38. Deve monitorar a utilização da CPU, da memória e estado da fonte de alimentação dos switches.

4.7.1.39. Deve permitir o monitoramento da temperatura de operação dos switches.

4.7.1.40. Deve ser possível visualizar os equipamentos vizinhos conectados ao switch, incluindo nome do dispositivo, endereço MAC, tipo do dispositivo e a partir de qual porta física do switch esse dispositivo vizinho pode ser encontrado.

4.7.1.41. Deve dispor de operações remotas para auxílio na resolução de problemas suportando, pelo menos, Ping e Traceroute.

4.7.1.42. Deve dispor de uma ferramenta para análise da conectividade do cliente por meio da inserção do endereço MAC do dispositivo final.

4.8. **Monitoramento**

4.8.1. Requisitos e Manutenção

4.8.2. Coleta de dados, detecção de eventos e geração de alertas.

4.8.3. Monitorar os ativos de rede por meio de SNMP (v2/v3), ICMP e outros protocolos relevantes.

4.8.4. Capacidade de monitoramento de no mínimo a quantidade total de ativos simultâneos informados no *Quadro 01* do Anexo I – Termo de Referência.

4.8.5. Implementação de triggers e actions para geração de alertas personalizados.

4.8.6. Gerar relatórios minimamente em PDF, CSV e Excel.

4.8.7. Monitorar os logs dos dispositivos, e gerar alertas com base nas informações dos logs.

4.8.8. Criar dashboards com gráficos e tabelas para facilitar a análise do desempenho da rede.

4.8.9. Implementação de dashboards específicos para cada tipo de ativo (pontos de acesso wifi e switches).

4.8.10. Coleta de métricas como latência, perda de pacotes, utilização de CPU, memória, temperatura e consumo de energia (quando disponível nos dispositivos).

4.8.11. Alertas configuráveis baseados em thresholds de desempenho.

4.8.12. Suporte a MIBs específicas dos fabricantes dos switches e pontos de acesso Wi-Fi.

4.8.13. A solução de monitoramento deve ser escalável para suportar o crescimento da rede.

4.8.14. A solução de monitoramento deve ser segura, com controle de acesso e criptografia de dados.

4.8.14.1. Monitoramento contínuo da disponibilidade e desempenho dos ativos de rede.

4.8.14.2. Acompanhamento do consumo de largura de banda, taxa de erro, tempo de resposta e utilização de CPU/memória dos dispositivos monitorados.

4.8.14.3. Identificação e registro de incidentes de conectividade e desempenho.

4.8.14.4. Atualização periódica de templates e ajustes em configurações conforme necessário.

4.8.14.5. Geração de dashboards dinâmicos e relatórios.

4.8.14.6. Configuração de agentes SNMP e ICMP para coleta de dados de switches e pontos de acesso WiFi.

4.8.14.7. Definição de templates e criação de triggers para alertas automáticos baseados em métricas predefinidas.

4.8.14.8. Configuração de notificações via e-mail, Telegran ou outras plataformas para alertas de falhas.

4.8.15. Geração de Relatórios e Dashboards

4.8.15.1. Criação de dashboards customizados para visualização em tempo real do estado dos ativos.

4.8.15.2. Emissão de relatórios gerenciais com estatísticas de disponibilidade, desempenho e incidentes.

4.8.15.3. Histórico de alertas e eventos.

4.8.16. Ativos a Serem Monitorados

4.8.16.1. Pontos de Acesso Wi-Fi

4.8.16.1.1. Disponibilidade (online/offline)

4.8.16.1.2. Número de clientes conectados

4.8.16.1.3. Tráfego de dados (upload/download)

4.8.16.1.4. Taxa de erros

4.8.16.1.5. Utilização de CPU e memória

4.8.16.2. Switches

4.8.16.2.1. Disponibilidade (online/offline)

4.8.16.2.2. Tráfego de dados em cada porta

4.8.16.2.3. Taxa de erros em cada porta

4.8.16.2.4. Utilização de CPU e memória

4.8.16.2.5. Status de VLANs

4.8.16.2.6. Status de Spanning Tree

4.9. **Segurança**

4.9.1. Deve realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance) em todos os componentes da infraestrutura de rede sem fio.

4.9.2. Deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede, incluindo pontos de acesso, switches e dispositivos conectados.

4.9.3. Deve suportar varreduras de vulnerabilidades de dispositivos de IoT conectados à infraestrutura sem fio.

4.9.4. Poderá fornecer um modelo de armazenamento integrado que não dependa de um banco de dados externos ou de terceiros. Caso o armazenamento dependa de banco de dados de terceiros, todas as licenças deverão ser fornecidas pela Contratada.

4.9.5. Deverá suportar API (Application Programming Interface) baseada em REST (Representatonal State Transfer) para automação de processos e integração com aplicações terceiras.

4.9.6. Deve possuir integração via API no mínimo com as seguintes linguagens: Python, PowerShell, Ruby, Javascript, Java, Swift e PHP.

4.9.7. Deve possuir métodos de consulta via API e envio, tais como: HTTP METHOD (POST, GET, PUT e DELETE).

4.9.8. Deve permitir o agrupamento de scanners para facilitar o gerenciamento e aplicação de políticas em diferentes localidades da rede sem fio.

4.9.9. O acesso à console de gerenciamento deve ser fornecido para pelo menos 10 usuários simultâneos.

4.9.10. Deve ser capaz de se integrar e disponibilizar insumos para soluções de correlação de eventos externa (SIEM).

4.9.11. Deve apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para correção.

4.9.12. Deve apresentar, para cada vulnerabilidade encontrada, evidências da vulnerabilidade através de saídas das verificações (outputs).

4.9.13. Deve fornecer controle de acesso baseado em função (RBAC - Role Based Access Control) para controlar o acesso do usuário a conjuntos de dados e funcionalidades.

4.9.14. Deve ser capaz de definir e gerenciar grupos de usuários, incluindo limitação de funções de varreduras e acesso a relatórios e dashboards.

4.9.15. Deve ter a capacidade de excluir determinados endereços IP ou dispositivos sem fio do escopo de qualquer varredura ou scan.

4.9.16. Deve criptografar todos resultados de varreduras obtidos e informações inseridas tanto em descanso quanto em trânsito.

4.9.17. Deve suportar métodos de autenticação usando bases de autenticação local, e SAML (Security Assertion Markup Language) para uso de SSO (Single Sign-On).

4.9.18. Deve ser capaz de orquestrar scanners ilimitados dentro da infraestrutura de rede sem fio.

4.9.19. Não deve impor nenhum limite de quantidade de scanners implementados dentro da infraestrutura.

4.9.20. Deverá possuir sistema de alertas para informar a disponibilidade de resultados dos escaneamentos através de e-mail.

4.9.21. Deve oferecer capacidade de configuração dinâmica de grupos de ativos através de no mínimo as seguintes características:

4.9.21.1. Endereço IP, DNS, NetBIOS Host e MAC

4.9.22. Deverá possuir painéis gerenciais (dashboards) pré-definidos para rápida visualização dos resultados, permitindo ainda a criação de painéis personalizados.

4.9.23. Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento.

4.9.24. Os relatórios devem ser disponibilizados sob demanda no console de gerência da solução.

4.9.25. Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um exploit disponível e informações do ativo na infraestrutura sem fio.

4.9.26. Deve permitir a customização de dashboards/relatórios específicos para a infraestrutura de rede sem fio.

4.9.27. Deve concentrar todos os relatórios na plataforma central de gerenciamento, não sendo aceitas soluções fragmentadas.

4.9.28. Deve ser capaz de produzir relatórios, pelo menos, nos seguintes formatos: HTML, PDF e CSV.

4.9.29. Deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e alvos específicos da rede sem fio.

4.9.30. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável).

4.9.31. Deve suportar o envio automático de relatórios para destinatários específicos.

4.9.32. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual.

4.9.33. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos.

4.9.34. Deve suportar varredura com ou sem agente, de maneira ativa e passiva, distribuídas em diferentes localidades e regiões da rede sem fio e gerenciar todos por uma console central.

4.9.35. Deve ser configurável para permitir a otimização das configurações de varredura, minimizando o impacto na performance da rede sem fio.

4.9.36. Deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux.

4.9.37. Deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo.

4.9.38. Deve suportar o agendamento de scans personalizados, incluindo a capacidade de executar varreduras em tempos designados, com frequência pré-determinada.

4.9.39. Deve ser capaz de identificar novos hosts no ambiente sem fio sem a necessidade de scan.

4.9.40. Deve possuir recurso de monitoria passiva do tráfego de rede sem fio para identificação de anomalias, novos dispositivos e desvios de padrões observados.

4.9.41. Ser capaz de identificar a comunicação de malwares na rede sem fio de forma passiva.

4.9.42. Deve em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede através da infraestrutura sem fio.

4.9.43. Deve ser capaz de exibir ambos severidade e pontuação, com base em CVSS (Common Vulnerability Scoring System) e inteligência de ameaças.

4.9.44. Deve utilizar sistema de pontuação e priorização das vulnerabilidades que utilize no mínimo:

4.9.44.1. CVSS Impact Score

4.9.44.2. Idade da Vulnerabilidade

4.9.44.3. Maturidade de códigos de exploração da vulnerabilidade encontrada

4.9.44.4. Frequência de uso da vulnerabilidade em ataques e campanhas atuais

4.9.44.5. Disponibilidade do código de exploração da vulnerabilidade

4.9.44.6. Presença de módulos de exploração de vulnerabilidade em frameworks automatizados de exploração de vulnerabilidades como CANVAS, Metasploit e Core Impact

4.9.44.7. Popularidade da vulnerabilidade em fóruns e comunicações na Darkweb

4.9.45. O mecanismo de priorização deve ser sujeito a modificações e atualizações diárias com base em inteligência de ameaças e observação de tendências na Internet.

4.9.46. Deve identificar e priorizar vulnerabilidades específicas dos equipamentos e protocolos de redes sem fio, incluindo vulnerabilidades em protocolos como WPA2, WPA3 e WEP.

4.9.47. Deve detectar configurações inseguras específicas de redes sem fio, como criptografia inadequada, exposição de SSIDs, canais inseguros e outros riscos próprios de ambientes wireless.

5. Acessórios – Transceivers, Cabos e Conectores Injetores PoE

5.1. **TRANSCEIVER MULTIMODO**

5.2. **GERAL**

5.2.1. Taxa de Transferência:

5.2.2. Suportar taxas de transferência de até 10 Gigabits por segundo.

5.2.3. Tipo de Fibra: Multimodo:

5.2.4. Alcance:

5.2.5. 300 metros: Em fibras multimodo OM3.

5.2.6. 400 metros: Em fibras multimodo OM4.

5.2.7. Formato: SFP+

5.2.8. LC Duplex: Utiliza conectores LC com uma interface full duplex para a transmissão e recepção de dados.

5.2.9. Hot-pluggable:

5.2.10. Deve ser do mesmo fabricante dos demais equipamentos

5.2.11. Temperatura de Operação: 0°C a 70°C: Operação típica em ambientes controlados.

5.2.12. Normas e Conformidades: IEEE 802.3ae: Conformidade com o padrão 10GBaseSR.

5.2.13. RoHS: Conformidade com a diretiva de restrição de substâncias perigosas.

5.2.14. DDM (Digital Diagnostics Monitoring): Capacidade de monitoramento em tempo real dos parâmetros do transceiver, como temperatura, tensão de alimentação, corrente de polarização do laser, potência óptica transmitida e recebida.

5.3. **TRANSCEIVER MONOMODO**

5.4. **GERAL**

5.4.1. Taxa de Transferência:

5.4.2. Suportar taxas de transferência de até 10 Gigabits por segundo.

5.4.3. Tipo de Fibra: Monomodo:

5.4.4. Alcance: 10KM

5.4.5. Formato: SFP+

5.4.6. LC Duplex: Utiliza conectores LC com uma interface full duplex para a transmissão e recepção de dados.

5.4.7. Hot-pluggable:

5.4.8. Deve ser do mesmo fabricante dos demais equipamentos

5.4.9. Temperatura de Operação: 0°C a 70°C: Operação típica em ambientes controlados.

5.4.10. Normas e Conformidades: IEEE 802.3ae: Conformidade com o padrão 10GBaseSR.

5.4.11. RoHS: Conformidade com a diretiva de restrição de substâncias perigosas.

5.4.12. 0DDM (Digital Diagnostics Monitoring): Capacidade de monitoramento em tempo real dos parâmetros do transceiver, como temperatura, tensão de alimentação, corrente de polarização do laser, potência óptica transmitida e recebida.

5.5. **CABO DAC**

5.6. **GERAL**

5.6.1. Cabo tipo DAC (Direct Attach Copper) 10Gbps, padrão SFPP para SFPP, com comprimento mínimo de 1m.

5.6.2. Deve ser do mesmo fabricante dos switches.

5.6.3. Transceivers SFP+ no padrão SFP+10G-BASE-T, suportando até 100 (cem) metros, com conectores RJ45 para cabos de rede par metálico CAT5e e/ou 6.

5.6.4. Os transceivers deverão ser plenamente compatíveis com os equipamentos do objeto disposto neste Termo de Referência".

5.7. **Características Injetor PoE**

5.7.1. Adaptador Power-over-Ethernet (PoE) para produtos com entradas PoE 1,0/2,5/5,0/10,0-BaseT. Classificado para uso em ambientes interiores.

5.7.2. Suporte a até 60W.

5.7.3. (1) Cabo de específico do país, IEC, 6 pés

5.7.4. (1) Módulo PoE (10/ 100/ 1000/ 2500/ 5000/ 10000Mbps)

5.7.5. Entrada: 100-24VCA ~ 50/60Hz 1,2A

5.7.6. Saída: 54VCC 1,12A (60W)

5.7.7. Porta de dados: Entrada RJ-45

5.7.8. Porta PoE/dados: Entrada RJ-45

6. Implementação - Instalação e Configuração

6.1.1. Todos os equipamentos e solução de gestão deverão ser entregues, instalados, configurados e postos em operação em consonância com o projeto aprovado;

6.1.2. Os equipamentos entregues deverão passar por testes de hardware do fabricante para assegurar a conformidade com os requisitos técnicos especificados. Estes testes deverão ser conduzidos e validados pela Contratada nas instalações da USCS, garantindo que o equipamento funcione conforme esperado antes de ser colocado em operação;

6.1.3. Os procedimentos envolvidos nos processos de instalação e configuração deverão ser previamente aprovados pela USCS, de forma a garantir intervalos de paralisação localizados que impactem o mínimo possível as atividades da USCS;

6.1.4. Sempre que a equipe técnica da USCS julgar necessário, ela poderá determinar que os procedimentos de instalação, totalmente ou em partes, sejam realizados em feriados, sábados ou domingos.

6.2. **Suporte e Garantia**

6.2.1. O suporte técnico da Contratada será iniciado a partir da emissão do Termo de Recebimento Provisório. A Contratada deverá prestar suporte aos elementos da solução por intermédio de sua sede, filiais ou escritórios, estando obrigada a:

6.2.2. Corrigir defeitos de fabricação ou projeto;

6.2.3. A Contratada será obrigada a substituir os equipamentos que apresentarem defeito de fabricação, dentro dos prazos estabelecidos nos demais subitens deste Termo de Referência;

6.2.4. Acondicionar adequadamente os equipamentos cujo reparo não possa ser realizado nas dependências da USCS de forma a permitir sua completa segurança e identificação durante o transporte, responsabilizando-se pela sua remoção e devolução ao local em que deve ser instalado e pelas despesas operacionais decorrentes;

6.2.5. Os custos relativos ao deslocamento de técnicos, transporte de componentes e equipamentos, dentre outros, são de responsabilidade da Contratada;

6.2.6. Detectar problemas e limitações de desempenho da solução relacionados a Software e/ou firmware instalados nos elementos que fazem parte do objeto deste Termo de Referência,

substituindo-os por nova versão que implemente suas correções; quando esta implementar correções a possíveis problemas ou limitações de desempenho da solução.

6.2.7. O suporte técnico da Contratada deve estar disponível para abertura de chamados 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, mediante e-mail ou outro sistema de abertura que permita o registro com histórico;

6.2.8. Os chamados deverão ser atendidos por técnico(s) certificado(s)/capacitado(s) pelo fabricante. A comprovação da certificação/capacitação do(s)técnico(s) poderá ser exigida pela USCS a qualquer momento durante a prestação do suporte.

6.2.9. O prazo de atendimento inicial inicia-se com a primeira intervenção pelo representante da Contratada, local ou remotamente;

6.2.10. A solução de contorno, se adotada, requererá a aplicação da solução definitiva no prazo a ser estabelecido pela USCS, a depender de cada caso;

6.2.11. O prazo de solução será contabilizado de acordo com o Termo de Referência;

6.2.12. Encaminhar aa USCS relatório contendo descrição do chamado aberto após solucionado, incluindo procedimento de resolução adotado e eventuais informações adicionais que poderão ser executadas para que o problema ocorrido não se repita;

6.2.13. Excepcionalmente, a critério exclusivo da USCS, mediante justificativa tecnicamente fundamentada que demonstre a impossibilidade de atendimento dos prazos acima, poderá ser concedido prazo adicional à Contratada para resolução de problemas;

6.2.14. O suporte será utilizado para desempenhar as seguintes tarefas:

6.2.15. Prestar todo e qualquer tipo de suporte a todos os elementos integrantes da solução adquirida;

6.2.16. Subsidiar a equipe técnica da USCS na abertura de chamados, através da identificação de imperfeições, vícios, defeitos, incorreções ou excesso de defeitos e diagnóstico de problemas;

6.2.17. Auxiliar a equipe técnica da Contratada na resolução de problemas, fornecendo informações do ambiente e suas particularidades assim como ações adotadas e diagnósticos realizados;

6.2.18. Abrir chamados com o fabricante, caso o problema não seja da alçada de solução da Contratada, interagir, provendo as informações necessárias, até a sua conclusão;

6.2.19. Prestar todo e qualquer tipo de esclarecimento técnico à equipe da USCS, inclusive documentar e repassar os procedimentos de instalação, atualização, administração e configuração da solução, quando solicitados;

6.2.20. Manter sempre atualizado e completo o conjunto de procedimentos operacionais entregues pela Contratada à USCS;

6.2.21. Manter sempre atualizado as rotinas de automação para integração da solução com a gestão de configuração da USCS entregues pela Contratada;

6.2.22. Subsidiar a equipe técnica com dados referentes à solução instalada para que sejam mantidas atualizadas as bases de dados relativas à solução Contratada;

6.2.23. A garantia deverá abranger os elementos da solução pelo período mínimo de vigência do contrato, contados a partir da implementação de todos os equipamentos ou a partir da aprovação do plano de inserção pela USCS, o que ocorrer por último, com todos os custos inclusos;

6.2.24. A garantia deverá abranger todos os equipamentos, softwares, cabos, conectores e demais elementos da solução, conforme especificações do Termo de Referência;

6.2.25. No caso de substituição de peças ou de todo o equipamento, o RMA deverá ocorrer em até 1 dia útil após o diagnóstico de falha em chamado aberto;

6.2.26. A Contratada deverá providenciar permissão de acesso ao sítio do fabricante para acompanhamento pela USCS de chamados, download e acesso a documentações, patches, fixes, firmwares, arquivos de qualquer tipo e/ou qualquer outro material referente à solução.

6.3. **Serviço técnico especializado, gestão, monitoramento e segurança da solução**

6.3.1. O serviço de suporte operacional especializada deverá garantir a disponibilidade, desempenho e segurança dos switches e pontos de acessos WiFi da instituição, através do monitoramento contínuo de ativos de rede. O serviço deverá contemplar a instalação, configuração, manutenção e suporte técnico da solução, garantindo a disponibilidade e desempenho dos ativos de rede, conforme requisitos especificados no Projeto Básico.

6.3.2. Deverá ser disponibilizado pela Contratada para apoiar as necessidades oriundas dos objetos dos itens deste documento, podendo ser realizado de forma presencial e/ou remota.

6.3.3. Trabalhar em estreita colaboração com a Diretoria de Tecnologia da Informação e Inovação, como equipes de suporte técnico, analistas de rede e equipes de segurança cibernética, para resolver problemas complexos, implementar mudanças e melhorias na infraestrutura de rede da universidade;

6.3.4. Acompanhar o monitoramento e segurança dos ativos de rede, receber alertas e notificações de problemas de rede, como interrupções de serviço e quedas de conexão. Investigar e resolver esses alertas/notificações, garantindo o mínimo de tempo de inatividade e impacto nos serviços;

6.3.5. Realizar verificações regulares de rotina, atualizações de firmware, instalação de patches de segurança e outras atividades para manter a rede em bom estado de funcionamento;

6.3.6. Avaliar novas funcionalidades e sugerir ajustes que possam melhorar a eficiência e a segurança da rede;

6.3.7. Realizar novas instalações, configurações, suporte técnico, manutenções preventivas e corretivas dos softwares e equipamentos (soluções, plataformas, switches e pontos de acessos WiFi);

6.3.8. Reportar e elaborar notas técnicas sobre problemas graves para a DTI;

6.3.9. Criação e acompanhamento no preenchimento de Requisição de Mudança (RDM) na infraestrutura de rede, seguindo os procedimentos de gerenciamento de mudanças estabelecidos pela USCS. Isso envolve a análise de impacto, planejamento, execução e documentação das alterações realizadas;

6.3.10. Monitorar e garantir a segurança e que os Níveis Mínimos de Serviços (NMS) sejam cumpridos;

6.3.11. Colaborar com equipes de projeto para implementar novas soluções de rede, como expansões, migrações ou atualizações tecnológicas.

7. ATENDIMENTO E SUPORTE DA SOLUÇÃO

7.1. A Contratada deverá disponibilizar telefone com atendimento mínimo dentro do horário comercial (8:00h às 18:00h) de segunda a sexta-feira para prover a necessidade da Universidade USCS.

7.2. O suporte técnico deverá ser prestado em caso de falhas, dúvidas e/ou esclarecimentos de qualquer um dos produtos, módulos e programas referentes aos componentes da solução.

7.3. Para garantia da qualidade de atendimento a central de atendimento deverá permitir acesso 24 horas através dos canais: portal web, e-mail, telefone e Whatsapp, onde a Contratante possa:

7.3.1. Abrir chamados de atendimento;

7.3.2. Receber numeração do chamado de forma automática;

7.3.3. Acompanhar o andamento do chamado.

8. ETAPAS DO SERVIÇO

8.1. ETAPA 1 – IMPLEMENTAÇÃO

8.1.1. A implementação definida para os itens (1.1.4; 1.2.6 e 1.3.3) se dará respeitando os seguintes aspectos:

8.1.1.1. Os equipamentos que compõe a solução ofertada pela licitante vencedora, devem ser todos entregues em até 45 (quarenta e cinco) dias corridos após a emissão da Ordem de Serviço, na sede da USCS (Campus Barcelona), aos cuidados do gestor do contrato, com respectiva indicação de patrimônio da contratada, bem como com planilha indicativa dos quantitativos dos itens entregues e respectivas características (marca/modelo).

8.1.1.2. No ato do recebimento o gestor irá verificar se os equipamentos recebidos correspondem aos indicados na proposta vencedora, e no mesmo ato atestará o recebimento provisório dos itens.

8.1.1.3. Os equipamentos entregues poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações ou critérios de aceitação, devendo ser substituídos às suas custas, sem prejuízo da aplicação das penalidades cabíveis.

8.1.2. No prazo descrito no item 8.1.1.1. a contratada deverá encaminhar, também, à Diretoria de Tecnologia da Informação e Inovação da USCS, plano de execução (cronograma) contendo informações a respeito do planejamento para implementação da solução.

8.1.3. O plano de execução deverá contemplar obrigatoriamente, os seguintes aspectos:

8.1.3.1. Prazo para implementação dos equipamentos entregues na sede da USCS, que compõe a solução, será de até 45 (quarenta e cinco) dias corridos, a ser iniciado quando da aprovação do plano de inserção até o aceite provisório da etapa de implementação;

8.1.3.2. Prazo para implementação por Campus e/ou prédios/salas/áreas, desde que respeitado o prazo do item anterior;

8.1.3.3. Topologia sugerida para atendimento às necessidades da USCS;

8.1.3.4. Indicar o prazo para validação definitiva de 10 (quinze) dias corridos pela equipe de DTI da Universidade USCS, após o aceite provisório da etapa de implementação.

8.1.4. A implementação da solução será recebida/concluída provisoriamente, conforme plano de inserção, momento em que passará por validação e testes pela Diretoria de Tecnologia da Informação e Inovação da USCS. Após validação, sendo concluído satisfatoriamente será expedido termo de recebimento definitivo da implementação, no prazo de 10 (dez) dias corridos, podendo ser prorrogado por igual período, desde que, por motivo justificado.

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

8.1.4.2. Entregáveis desta etapa:

8.1.4.2.1. Plano de execução;

8.1.4.2.2. Relatório de entrega provisório e definitivo;

8.2. **ETAPA 2 - SUSTENTAÇÃO - SERVIÇO CONTINUADO POR 24 MESES**

8.2.1. Após expedição do termo de recebimento definitivo da etapa de implementação, dará início automaticamente a etapa 2 que terá vigência de 24 (vinte e quatro) meses conforme previsto neste instrumento.

8.2.2. Entregáveis nessa etapa se limita ao relatório mensal.

9. FORMA DE MEDIÇÃO E PAGAMENTO

9.1. **ETAPA 1 - IMPLEMENTAÇÃO – Prazo de até 90 dias corridos**

9.1.1. Os valores relativos a etapa de implantação representados pela instalação, configuração e ativação física dos itens descritos como 1.1.1; 1.1.2; 1.1.3; 1.2.1; 1.2.2; 1.2.3; 1.2.4; 1.2.5; 1.3.1 e 1.3.2, após recebimento provisório e emissão do termo de aceite pelo gestor do instrumento de contrato, a contratada deverá emitir nota fiscal que corresponderá aos serviços descritos nos itens 1.1.4, 1.2.6 e 1.3.3 do quadro 01 deste termo de referência, respeitando-se a definição percentual estabelecida no cronograma apresentado pela contratada no ato de entrega física dos equipamentos na sede da Universidade USCS. O pagamento será efetuado em parcela única, ressalvadas eventuais glosas ou penalidades contratuais.

9.2. **ETAPA 2 - SUSTENTAÇÃO – Serviço Continuado por 24 meses.**

9.2.1. Os valores relativos a esta etapa serão pagos mensalmente, e terão seu início definido após a ativação dos equipamentos, o que corresponde ao momento de emissão do termo de aceite, respeitando-se o cronograma de execução definido entre a Ccontratada e a Universidade Municipal de São caetano do Sul.

10. CRITÉRIOS DE ACEITAÇÃO

10.1. A avaliação da qualidade dos produtos entregues, para fins de aceitação, consiste na verificação dos critérios relacionados a seguir:

10.1.1. Todos os equipamentos fornecidos deverão ser novos (incluindo todas as peças e componentes presentes nos produtos), de primeiro uso (sem sinais de utilização anterior), não recondicionados e em fase de comercialização normal através dos canais de venda do fabricante no Brasil (não serão aceitos produtos *end-of-sale e/ou end-of-life).*

10.1.2. Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si, sem a utilização de adaptadores, frisagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos não previstos nas especificações técnicas ou, ainda, com emprego de materiais inadequados ou que visem adaptar forçadamente o produto ou suas partes que sejam fisicamente ou logicamente incompatíveis.

10.1.3. Todos os componentes internos do(s) equipamento(s) deverá(ão) estar instalado(s) de forma organizada e livres de pressões ocasionados por outros componentes ou cabos, que possam causar desconexões, instabilidade, ou funcionamento inadequado.

10.1.4. Serão recusados os equipamentos que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos, sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado como novos pelo fornecedor dos produtos.

10.1.5. Os equipamentos, considerando a marca e modelo apresentados na licitação, não poderão estar fora de linha comercial, considerando a data de implementação e ativação. Os equipamentos devem ser fornecidos completos e prontos para a utilização, com todos os acessórios, componentes, cabos etc.

10.1.6. Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização da contratante, legalizado, não sendo admitidas versões "*shareware*" ou "*trial*". O modelo do produto ofertado pelo licitante deverá estar em fase de produção (no Brasil ou no exterior), com *datasheet* oficial disponibilizado em site oficial do fabricante e sem previsão de encerramento de produção, até a data de entrega da proposta.

11. NÍVEIS MÍNIMOS DE SERVIÇOS EXIGIDOS - Service Level Agreement SLA

11.1. Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pela Universidade USCS para aferir objetivamente os resultados pretendidos com a contratação.

11.2. Para a medição dos índices de nível de serviços, serão considerados os seguintes conceitos:

11.2.1. **Incidente:** É uma interrupção não planejada de um serviço de Tecnologia da Informação ou uma redução de qualidade de um serviço de TI;

11.2.2. **Problema:** é a causa desconhecida de um ou mais incidentes ou os problemas são a causa de um ou mais incidentes;

11.2.3. **Severidade:** Solicitações de alteração do nível de severidade poderá ser submetida à Contratada e, quando julgadas pertinentes, serão prontamente atendidas, conforme quadro a seguir.

Severidade	Descrição
Crítica	Indisponibilidade total dos serviços.
Alto	Degradação dos serviços.
Normal	Falha parcial dos serviços.

Quadro 02

11.3. **IMPLEMENTAÇÃO - Serviços de Entrega, Instalação e Configuração da Solução**

11.3.1. Todos os produtos deverão ser entregues nos quantitativos e localidades indicadas, instalados e configurados em conformidade com a especificação, dentro dos prazos máximos estipulados neste Termo, assim como previsto no termo de inserção (cronograma).

11.3.2. Será verificada a conformidade com as especificações técnicas, assim como mensurado o prazo de entrega da solução, conforme detalhamento dos indicadores de nível de serviço indicados a seguir.

11.3.3. Em caso de eventual falta de instalação ou configuração, decorrentes de falha de infraestrutura que deva ser provida pela USCS, por exemplo, mas não limitado a falha no cabeamento estruturado, de energia, ou *links* de internet, não caberá nenhum tipo glosa ou penalidade a contratada.

11.3.4. Em caso de eventual vício ou defeito no cabeamento estruturado, exclusivamente, seja para *uplink* (interconexão entre switches) ou para conexão de pontos de acesso de rede sem fio (equipamento WiFi), deverá a contratada prover a solução técnica às suas expensas.

11.3.5. A manutenção/substituição prevista no item imediatamente anterior se limita a substituição de cabeamento, em pontos de até 100 metros ou múltiplos de 100 m.

11.3.6. Para fins de atendimento ao item 11.3.4, deverá a contratada, caso necessário, realizar a infraestrutura e/ou fornecer cabos, minimamente CAT6 ou fibra óptica (multimodo/monomodo) compatíveis com a necessidade do projeto.

11.3.7. A contratada a seu critério poderá prover protetores elétricos tais como mecanismos, acessórios e/ou equipamentos de proteção contra quedas, interrupções e distúrbios elétricos, para provimento e continuidade dos serviços do objeto.

11.4. **SERVIÇOS DE GARANTIA, MANUTENÇÃO E SUPORTE TÉCNICO**

11.4.1. **Severidade 1 - Crítica**: Serviço indisponível para grande número de usuários e/ou com alta degradação de performance. Serviço indisponível para o público interno/externo (docentes, discentes, colaboradores, terceirizados, e público externo), deverá ser iniciado em até 2 (duas) horas e o chamado solucionado em até 4 (quatro) horas corridas;

11.4.2. **Severidade 2 - Alta:** Serviço degradado, com risco iminente de indisponibilidade ou indisponível. Incidentes relacionados a usuários de alta prioridade (limitado a 3% dos usuários), deverá ser iniciado em até 4 (quatro) horas e o chamado solucionado em até 8 (oito) horas úteis;

11.4.3. **Severidade 3- Normal:** Serviço apresentando problemas sem indisponibilidade ou degradação de performance para os usuários, eventos de alertas proativos sem impacto de negócios, deverá ser iniciado em até 12 (doze) horas e o chamado solucionado em até 24 horas úteis;

11.4.4. **Rotineiro:** Operações das ferramentas e equipamentos em geral tais como configuração em geral, parametrização de ferramentais, criação e/ou configurações de usuários e novas redes, deverá ser iniciado em até 24 horas e o chamado solucionado em até 48 horas úteis;

11.4.5. Para atendimento a chamados em que não haja necessidade de troca de peças ou intervenção local, será admitido o atendimento remoto, ao invés de presença no local de instalação da solução;

11.4.6. Horas comerciais, para fins de cálculo do NMS, são as compreendidas entre 8h e 18h, horário de Brasília, em dias úteis;

11.4.7. Por início de atendimento entende-se o registro do chamado em ferramenta própria para início da tratativa, a fim de efetuar a correção do incidente, requisição ou o *troubleshooting* preciso, com interlocução direta com a equipe da USCS;

11.4.8. Um chamado técnico somente poderá ser fechado após o aceite da USCS e o término de atendimento se dará com a disponibilidade do recurso para uso em perfeitas condições de funcionamento;

11.4.9. Um chamado fechado, sem anuência da USCS ou sem que o problema tenha sido de fato resolvido, será reaberto e os prazos serão contados a partir da data de abertura original do chamado, inclusive para efeito de aplicação das multas e sanções previstas;

11.4.10. No final do atendimento, o técnico da Contratada deverá elaborar um relatório de ocorrência onde conste o problema causador do chamado, a solução encontrada, as pendências, a data e hora do chamado, do início e do fim do atendimento. Esse relatório deve ter a concordância e assinatura de um técnico da Universidade USCS.

11.5. **DETALHAMENTO DOS INDICADORES DE NÍVEL DE SERVIÇO**

11.5.1. Caso a Contratada não atinja os níveis mínimos de serviço fixados neste Termo de Referência, não venha a produzir os resultados esperados, deixe de executar as atividades contratadas, deixe de utilizar os materiais e recursos humanos exigidos qualitativamente e/ou quantitativamente para fornecimento da solução ou, utilize-os com qualidade aquém da expectativa demandada, estará, conforme cada caso, sujeita a aplicação de glosas nos valores estabelecidos para multas e/ou penalidades ou retenção do pagamento até que as pendências sejam sanadas.

11.5.2. Indicador de Verificação de Atraso na Entrega do Objeto:

Indicador 01 – Indicador de Atraso na Entrega do Objeto (IAEO)		
Tópico	**Descrição**	
Finalidade	Medir eventual tempo de atraso de implementação da solução constante na Ordem de Serviço.	
Meta a cumprir	**IAEO <= 0**	A meta definida visa garantir a entrega da implementação da solução constante nas Ordens de Serviço dentro do prazo previsto.
Instrumento de medição	Registro de assinatura da Ordem de Serviço - OS e seus respectivos Termos de Recebimento Provisório e Definitivo emitidos.	
Forma de acompanhamento	A avaliação será feita considerando o cronograma de execução e os prazos previstos neste Termo. Será subtraída a data de entrega definitiva da implementação da solução da OS ou a data do início da prestação dos serviços (desde que o fiscal reconheça aquela data, com registro em Termo de Recebimento Provisório ou Definitivo), pela data da assinatura da OS.	

Periodicidade	Execução única ao início do contrato, para cada Ordem de Serviço.
Mecanismo de Cálculo (métrica)	IAOE = (TEX – TEST) / TEST Onde: **IAEO** – Indicador de Atraso de Entrega do Objeto; **TEX** – Tempo de Execução – corresponde ao período de execução da OS, da sua data de início até a data de entrega dos produtos da OS. **TEST** – Tempo Estimado para a execução da OS – constante na OS, conforme estipulado no Termo de Referência. A data de início será aquela constante na Ordem de Serviço; caso não esteja explícita, será o primeiro dia útil após a sua emissão. A data de entrega da OS deverá ser aquela reconhecida pelo fiscal, conforme critérios constantes no TR. Para os casos em que o fiscal rejeita a entrega, o prazo de execução da OS continua a correr, findando-se apenas quando a contratada entregar os equipamentos da OS e haja aceitação por parte do fiscal.
Observações	Obs1.: Serão utilizados dias corridos na medição. Obs2.: Os dias com expediente parcial na Universidade USCS serão considerados no cômputo do indicador. Obs3.: Não se aplicará este indicador para as OS de Manutenções Corretivas do tipo Garantia e aquelas com execução interrompida ou cancelada por solicitação da USCS. Obs4.: Esse indicador será aplicado para aferição dos seguintes níveis mínimos de serviços: •Recebimento Provisório (Entrega dos equipamentos) – Itens 1 e 2 •Recebimento Definitivo (Término da Instalação, Configuração e Entrega de documentação) – Itens 1 e 2
Início de Vigência	Data da assinatura da Ordem de Serviço – OS
Faixas de ajuste no pagamento e Sanções	De 0 a 0,10 – Pagamento integral da OS; De 0,11 a 0,20 – Glosa de 0,5% sobre o valor da OS; De 0,21 a 0,30 – Glosa de 1,0% sobre o valor da OS; De 0,31 a 0,50 – Glosa de 5,0% sobre o valor da OS; De 0,51 a 1,00 – Glosa de 10,0% sobre o valor da OS; Acima de 1 – Será aplicada Glosa de 12,5% sobre o valor da OS e Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento deste Termo de Referência.

Quadroa 03

11.5.3. Indicador de Verificação de Suporte Atendido dentro do Prazo (SADPN)

Indicador 02 – Suporte Atendido dentro do Prazo – Severidade 3 - Normal (SADPN)	
Tópico	**Descrição**
Finalidade	Assegurar que os chamados estejam dentro do nível mínimo de serviço exigido neste Termo.
Meta a cumprir	90% dos chamados atendidos dentro do prazo.
Instrumento de medição	Através das ferramentas disponíveis para a gestão de demandas, por controle próprio da USCS ou registros de abertura e encerramento de chamados, desde que aceitos pelo fiscal como meio formal de comunicação com a contratada.
Forma de acompanhamento	Cálculo de prazo de cada chamado ao Nível Mínimo de Serviço exigido, conforme previsto neste Termo.
Periodicidade	Sob demanda.
Mecanismo de Cálculo (métrica)	SADP = (TEX – TEST) / TEST Onde: **SADP** – Suporte Atendido dentro do Prazo; **TEX** – Tempo de Execução – corresponde ao período de execução do chamado, da sua data de início até a data de sua conclusão definitiva. **TEST** – Tempo Estimado para a execução do chamado. A data de início será aquela em que foi registrado o chamado junto à contratada em ferramenta própria para início da tratativa. A data de início será aquela em que foi registrado o chamado junto à contratada em ferramenta própria.

	A data de conclusão do chamado deverá ser aquela reconhecida pelo fiscal, conforme critérios constantes no Termo de Referência. Para os casos em que o fiscal rejeita o encerramento do chamado, o prazo de execução continua a correr, findando-se apenas quando a contratada solucionar definitivamente o chamado e haja aceitação por parte do fiscal.
Observações	Obs1: Serão utilizados dias úteis na medição. Obs2: Os dias com expediente parcial na USCS serão considerados como dias úteis no cômputo do indicador. Obs3: Não se aplicará este indicador para as OS ou chamados com execução interrompida ou cancelada por solicitação da USCS. Obs4: Este indicador será aplicado a chamados de Garantia e/ou de Suporte Técnico, considerando os prazos indicados no TR para correção de falhas de hardware ou software. Obs5.: Esse indicador será aplicado para aferição dos níveis mínimos de serviços de garantia e assistência técnica dos Itens 1 e 2
Início de Vigência	A partir do primeiro dia útil da emissão do Termo de Recebimento Definitivo - TRD.
Faixas de ajuste no pagamento e Sanções	De <=0 a 0,10 – Glosa de 0,0%; De 0,11 a 0,20 – Glosa de 0,5%; De 0,21 a 0,30 – Glosa de 1,0%; De 0,31 a 0,50 – Glosa de 3,0%; De 0,51 a 1,00 – Glosa de 5,0%; Acima de 1 – Será aplicada Glosa de 10% e aplicadas Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento previstas neste Termo de Referência. Obs1.: As glosas incidirão sobre o valor da obrigação não cumprida no item faturado;

Quadroa 04

11.5.4. Indicador de Verificação de Suporte Atendido dentro do Prazo (SADPN)

Indicador 03 – Suporte Atendido dentro do Prazo – Severidade 2 - Alta (SADPA)	
Tópico	**Descrição**
Finalidade	Assegurar que os chamados estejam dentro do nível mínimo de serviço exigido neste Termo.
Meta a cumprir	95% dos chamados atendidos dentro do prazo.
Instrumento de medição	Através das ferramentas disponíveis para a gestão de demandas, por controle próprio da USCS ou registros de abertura e encerramento de chamados, desde que aceitos pelo fiscal como meio formal de comunicação com a contratada.
Forma de acompanhamento	Cálculo de prazo de cada chamado ao Nível Mínimo de Serviço exigido, conforme previsto neste Termo.
Periodicidade	Sob demanda.
Mecanismo de Cálculo (métrica)	$$SADP = \frac{(TEX - TEST)}{TEST}$$ Onde: **SADP** – Suporte Atendido dentro do Prazo; **TEX** – Tempo de Execução – corresponde ao período de execução do chamado, da sua data de início até a data de sua conclusão definitiva. **TEST** – Tempo Estimado para a execução do chamado. A data de início será aquela em que foi registrado o chamado junto à contratada em ferramenta própria. A data de conclusão do chamado deverá ser aquela reconhecida pelo fiscal, conforme critérios constantes no Termo de Referência. Para os casos em que o fiscal rejeita o encerramento do chamado, o prazo de execução continua a correr, findando-se apenas quando a contratada solucionar definitivamente o chamado e haja aceitação por parte do fiscal.
Observações	Obs1: Serão utilizados dias úteis na medição. Obs2: Os dias com expediente parcial na Universidade USCS serão considerados como dias úteis no cômputo do indicador. Obs3: Não se aplicará este indicador para as OS ou chamados com execução interrompida ou cancelada por solicitação da USCS. Obs4: Este indicador será aplicado a chamados de Garantia e/ou de Suporte Técnico, considerando os prazos indicados no TR para correção de falhas de hardware ou software. Obs5.: Esse indicador será aplicado para aferição dos níveis mínimos de serviços de garantia e assistência técnica dos Itens 1 e 2

Início de Vigência	A partir do primeiro dia útil da emissão do Termo de Recebimento Definitivo - TRD.
Faixas de ajuste no pagamento e Sanções	De <=0 a 0,10 – Glosa de 0,0%; De 0,11 a 0,20 – Glosa de 5%; De 0,21 a 0,30 – Glosa de 6,0%; De 0,31 a 0,50 – Glosa de 8,0%; De 0,51 a 1,00 – Glosa de 11,0%; Acima de 1 – Será aplicada Glosa de 15% e aplicadas Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento previstas neste Termo de Referência. Obs1.: As glosas incidirão sobre o valor da obrigação não cumprida no item faturado;

Quadroa 05

11.5.5. Indicador de Verificação de Suporte Atendido dentro do Prazo (SADPN)

Indicador 04 – Suporte Atendido dentro do Prazo – Severidade 1 - Crítica (SADPC)	
Tópico	**Descrição**
Finalidade	Assegurar que os chamados estejam dentro do nível mínimo de serviço exigido neste Termo.
Meta a cumprir	98% dos chamados atendidos dentro do prazo.
Instrumento de medição	Através das ferramentas disponíveis para a gestão de demandas, por controle próprio da USCS ou registros de abertura e encerramento de chamados, desde que aceitos pelo fiscal como meio formal de comunicação com a USCS.
Forma de acompanhamento	Cálculo de prazo de cada chamado ao Nível Mínimo de Serviço exigido, conforme previsto neste Termo.
Periodicidade	Sob demanda.
Mecanismo de Cálculo (métrica)	$$SADP = \frac{(TEX - TEST)}{TEST}$$ Onde: **SADP** – Suporte Atendido dentro do Prazo; **TEX** – Tempo de Execução – corresponde ao período de execução do chamado, da sua data de início até a data de sua conclusão definitiva. **TEST** – Tempo Estimado para a execução do chamado. A data de início será aquela em que foi registrado o chamado junto à contratada em ferramenta própria. A data de conclusão do chamado deverá ser aquela reconhecida pelo fiscal, conforme critérios constantes no Termo de Referência. Para os casos em que o fiscal rejeita o encerramento do chamado, o prazo de execução continua a correr, findando-se apenas quando a contratada solucionar definitivamente o chamado e haja aceitação por parte do fiscal.
Observações	Obs1: Serão utilizados dias úteis na medição. Obs2: Os dias com expediente parcial na Universidade USCS serão considerados como dias úteis no cômputo do indicador. Obs3: Não se aplicará este indicador para as OS ou chamados com execução interrompida ou cancelada por solicitação da USCS. Obs4: Este indicador será aplicado a chamados de Garantia e/ou de Suporte Técnico, considerando os prazos indicados no TR para correção de falhas de hardware ou software. Obs5.: Esse indicador será aplicado para aferição dos níveis mínimos de serviços de garantia e assistência técnica dos Itens 1 e 2
Início de Vigência	A partir do primeiro dia útil da emissão do Termo de Recebimento Definitivo - TRD.
Faixas de ajuste no pagamento e Sanções	De <=0 a 0,10 – Glosa de 0,0%; De 0,11 a 0,20 – Glosa de 11%; De 0,21 a 0,30 – Glosa de 12,0%; De 0,31 a 0,50 – Glosa de 14,0%; De 0,51 a 1,00 – Glosa de 16,0%; Acima de 1 – Será aplicada Glosa de 20% e aplicadas Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento previstas neste Termo de Referência. Obs1.: As incidirão sobre o valor da obrigação não cumprida no item faturado;

Quadroa 06

11.6. Indicador de Verificação de Saúde Operacional (IRSO)

Indicador 05 – Relatório de Saúde Operacional (IRSO)	
Tópico	**Descrição**
Finalidade	Apresentar um relatório com a percepção de regras conflitantes ou mal configuradas, apontamento de melhores práticas a serem aplicadas, visão crítica das configurações aplicadas e apontar melhorias, avaliação do consumo dos recursos dos equipamentos e propor, caso necessário, cenários de melhor aproveitamento dos recursos, entre outros apontamentos que a Contratada achar pertinente para melhor desempenho da solução.
Meta a cumprir	Entrega do relatório dentro do prazo de 5 dias úteis.
Instrumento de medição	Através das ferramentas disponíveis para a gestão de demandas, por controle próprio da USCS ou registros de abertura e encerramento de chamados, desde que aceitos pelo fiscal técnico como meio formal de comunicação com a contratada.
Forma de acompanhamento	Cálculo de prazo de cada chamado ao Nível Mínimo de Serviço exigido, conforme previsto neste Termo.
Periodicidade	Sob demanda ou em periodicidade indicada no Termo para realização de manutenção preventiva
Mecanismo de Cálculo (métrica)	$SADP = \frac{(TEX - TEST)}{TEST}$ Onde: **SADP** – Suporte Atendido dentro do Prazo; **TEX** – Tempo de Execução – corresponde ao período de execução do chamado, da sua data de início até a data de sua conclusão definitiva. **TEST** – Tempo Estimado para a execução do chamado. A data de início será aquela em que foi registrado o chamado junto à contratada em ferramenta própria. A data de conclusão do chamado deverá ser aquela reconhecida pelo fiscal, conforme critérios constantes no Termo de Referência. Para os casos em que o fiscal rejeita o encerramento do chamado, o prazo de execução continua a correr, findando-se apenas quando a contratada solucionar definitivamente o chamado e haja aceitação por parte do fiscal.
Observações	Obs1: Serão utilizados dias úteis na medição. Obs2: Os dias com expediente parcial na Universidade USCS serão considerados como dias úteis no cômputo do indicador. Obs3: Não se aplicará este indicador para as OS ou chamados com execução interrompida ou cancelada por solicitação da USCS. Obs4: Este indicador será aplicado a chamados de Garantia e/ou de Suporte Técnico, considerando os prazos indicados no TR para correção de falhas de hardware ou software. Obs5.: Esse indicador será aplicado para aferição dos níveis mínimos de serviços de garantia e assistência técnica dos Itens 1, e 2.
Início de Vigência	A partir do primeiro dia útil da emissão do Termo de Recebimento Definitivo - TRD.
Faixas de ajuste no pagamento e Sanções	De <=0 a 0,10 – Glosa de 0,0%; De 0,11 a 0,20 – Glosa de 5%; De 0,21 a 0,30 – Glosa de 7%; De 0,31 a 0,50 – Glosa de 10,0%; De 0,51 a 1,00 – Glosa de 13,0%; Acima de 1 – Será aplicada Glosa de 20% e aplicadas Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento previstas neste Termo de Referência. Obs1.: As glosas incidirão sobre o valor da obrigação não cumprida no item faturado;

Quadroa 07

11.7. Indicador de Permanência de Equipamento, Peça ou Componente Backup

Indicador 06 – Indicador de Permanência de Equipamento, Peça ou Componente Backup (IPEB)	
Tópico	**Descrição**
Finalidade	Assegurar que o equipamento de backup da contratada não ultrapasse os 30 dias corridos contados a partir da comunicação realizada pelo sistema de registro da própria da USCS.
Meta a cumprir	30 dias corridos para cada ocorrência
Instrumento de medição	Através das ferramentas disponíveis para a gestão de demandas, por controle próprio da USCS ou registros de abertura e encerramento de chamados, desde que aceitos pelo Fiscal Técnico como meio formal de comunicação com a contratada.

Forma de acompanhamento	Cálculo de prazo de Registro/Resposta de cada solicitação de suporte técnico de garantia em relação ao Nível de Serviço.
Periodicidade	Sob demanda.
Mecanismo de Cálculo (métrica)	IPEB = (TEX – TEST) / TEST Onde: **IPEB** – Indicador de Permanência de Equipamento, Peça ou Componente Backup (IPEB); **TEX** – Tempo de Execução – corresponde ao período de execução do chamado, da sua data de início até a data de sua conclusão definitiva. **TEST** – Tempo Estimado para a execução do chamado. A data de início será aquela em que foi registrado encerramento do chamado de suporte técnico da contratada e abertura do chamado de garantia junto ao fabricante; A data de início e de conclusão do chamado deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes no Termo de Referência. Para os casos em que o fiscal rejeita o dia e hora de registro ou de encerramento do chamado, o prazo de execução continua a correr, findando-se apenas quando a contratada solucionar definitivamente o chamado junto ao fabricante e haja aceitação por parte do fiscal técnico.
Observações	Obs1: Serão utilizados dias úteis na medição. Obs2: Os dias com expediente parcial na Universidade USCS serão considerados como dias úteis no cômputo do indicador. Obs3: A contagem do prazo de atendimento se inicia após o Fechamento do chamado de Suporte Técnico da Contratada concomitantemente ao registro de chamado de suporte técnico em Garantia junto ao Fabricante; Obs4: Não se aplicará este indicador para as OS com execução interrompida ou cancelada por solicitação da USCS. Obs5.: Esse indicador será aplicado para aferição dos níveis mínimos de serviços de garantia e assistência técnica dos Itens 1 e 2
Início de Vigência	A partir do primeiro dia útil da emissão do Termo de Recebimento Definitivo - TRD.
Faixas de ajuste no pagamento e Sanções	De <=0 a 0,10 – Glosa de 0,0%; De 0,11 a 0,20 – Glosa de 0,5%; De 0,21 a 0,30 – Glosa de 1,0%; De 0,31 a 0,50 – Glosa de 5,0%; De 0,51 a 1,00 – Glosa de 10,0%; Acima de 1 – Será aplicada Glosa de 12,5% e aplicadas Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento previstas neste Termo de Referência. Obs1.: No caso dos itens 1, 2 e 3, as glosas incidirão sobre o valor da obrigação não cumprida no item faturado;

Quadroa 08

12. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

12.1. O fornecedor será selecionado por meio da realização de processo licitatório, modalidade Pregão em sua forma Eletrônica, cujo critério de julgamento de proposta comercial será o de menor preço glabal para o lote único em disputa.

12.2. O proponente interessado deverá apresentar proposta de preços de acordo com modelo disposto no Anexo II deste termo de referência. Na composição da proposta comercial o licitante deverá criar documento a ser exigido em momento apropriado, contendo a especificação técnica da solução, em cada caso, incluindo as licenças e os serviços de implantação, suporte técnico e garantia, conforme requisitos dispostos ao longo do tópico "*Tipologia acerca das especificações e exigências aplicadas ao projeto"* deste documento.

12.3. O proponente deve indicar, em sua proposta, em relação aos equipamentos a marca/fabricante, modelo, e especificação do licenciamento, que compõem a solução a ser contratada pela USCS.

12.4. QUALIFICAÇÃO TÉCNICA

12.4.1. Comprovação de aptidão para o fornecimento de bens similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado. Os atestados apresentados na documentação de habilitação deverão conter, obrigatoriamente, a especificação dos serviços executados com fornecimento que comprove os

quantitativos referente a metade dquilo previsto no termo de referência, inclusive com a indicação de 50% da quantidade de usuários com acesso simultâneo previstas para atendimento nesta contratação (5000 acesso simultâneos rede WiFi).

12.5. **CAPACITAÇÃO PROFISSIONAL**

12.5.1. A empresa a ser contratada deverá apresentar, no ato de celebração de contrato, a comprovação de certificação técnica necessária relativa à equipe de trabalho designada para consecução do projeto, com no mínimo as seguintes certificações:

12.5.1.1. Pelo menos um profissional com certificação expedida pelo fabricante da solução ofertada, não sendo aceito meros certificados de participação em cursos:

- Pelo menos um profissional **Gerente de Projetos**, com uma das seguintes certificações:
  - ✓ PMP (Project Management Professional)
  - ✓ PSM (Professional Scrum Master)
  - ✓ Pós-graduação na área
- **Analista de Monitoramento de Redes e Serviços Jr**
  - ✓ Esse profissional deverá possuir curso superior em uma das áreas de Computação, Informática, Análise de Sistemas, Ciência da Computação, Sistemas de Informação, Engenharia de Software ou Ciências Exatas, ou qualquer outro curso superior combinado com curso de especialização na área de Informática com carga horária mínima de 360 (trezentos e sessenta) horas, ou curso de mestrado na área de Informática, comprovada por cópia do respectivo diploma, devidamente registrado, e fornecido por instituição de ensino superior reconhecida pelo MEC.
  - ✓ Deverá possuir a certificação ITIL V3 Foundation ou superior.
- **Analista de Monitoramento de Redes e Serviços Sênior**
  - ✓ Esse profissional deverá possuir curso superior em uma das áreas de Computação, Informática, Análise de Sistemas, Ciência da Computação, Sistemas de Informação, Engenharia de Software ou Ciências Exatas, ou qualquer outro curso superior combinado com curso de especialização na área de Informática com carga horária mínima de 360 (trezentos e sessenta) horas, ou curso de mestrado na área de Informática, comprovada por cópia do respectivo diploma, devidamente registrado, e fornecido por instituição de ensino superior reconhecida pelo MEC.
  - ✓ Deverá possuir a certificação ITIL V3 Foundation ou superior.
  - ✓ Deverá possuir a certificação CCNP (Cisco Certified Network Professional).

ANEXO II - PROPOSTA COMERCIAL	
Pregão Eletrônico nº 27/2025	**Abertura 27/12/2025 às 11h**
Razão Social:	
Endereço Eletrônico:	
CNPJ:	**Inscrição Estadual:**
Endereço:	**nº**
Bairro:	**Cidade:**
CEP:	**Estado:**
Fone / Fax:	**e-mail:**
Informação para pagamento:	
Banco: **Agência número:**	**Conta Corrente número:**

Para efeito de precificação e apresentação de proposta de preços, o proponente deve considerar todos os requisitos exigidos no termo de referência (anexo I) para a solução proposta concernente ao lote único.

Importante

Os itens neste anexo foram ordenados levando-se em conta a sequência observada na inserção da proposta comercial no sistema de pregão eletrônico da USCS.

Quando do preenchimento da proposta no sistema de pregão eletrônico, considerar somente as variáveis valor mensal x cronograma de pagamento, exceto quando se tratar dos itens 4, 10 e 13, considerar no preenchimento a variável cronograma de pagamento.

Item	Descrição	Fabricante, Marca, Modelo	Quantidade Equipamento	Cronograma Pagamento	Valor Unitário em Reais	Valor Mensal em Reais	Valor Total em Reais
	Serviço gerenciado de solução para gestão ativos de rede, monitoramento e segurança, incluindo fornecimento de softwares, equipamentos, licenciamentos, suporte técnico especializado, acessórios e garantia.						
	Serviço gerenciado de Switch, incluindo fornecimento de equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.						
1	Switch de acesso **tipo 1 (*As a Service*)**, incluindo equipamentos licenciados, suporte específico do fabricante, acessórios e garantia.		28	24 Meses			
2	Switch de acesso **tipo 2 (*As a Service*)**, incluindo equipamentos licenciados, suporte específico do fabricante, acessórios e garantia.		2	24 Meses			
3	Switch de acesso **tipo 3 (*As a Service*)**, incluindo equipamentos licenciados, suporte específico do fabricante, acessórios e garantia.		2	24 Meses			
4	Implementação – instalação e configuração física da solução de Switch.		32	1 Serviço			
	Serviço gerenciado de Ponto de Acesso (AP), incluindo fornecimento de equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.						
5	Ponto de acesso **tipo 1 (*As a Service*)**, incluindo equipamentos licenciados, suporte específico do fabricante, acessórios e garantia.		185	24 Meses			
6	Ponto de acesso **tipo 2 (*As a Service*)**, incluindo equipamentos licenciados, suporte específico do fabricante, acessórios e garantia.		12	24 Meses			
7	Ponto de acesso **tipo 3 (*As a Service*)**, incluindo equipamentos licenciados, suporte específico do fabricante, acessórios e garantia.		12	24 Meses			
8	Ponto de acesso **tipo 4 (*As a Service*)**, incluindo equipamentos licenciados, suporte específico do fabricante, acessórios e garantia.		6	24 Meses			

9	Ponto de acesso **tipo 5 (*As a Service*)**, incluindo equipamentos licenciados, suporte específico do fabricante, acessórios e garantia.		4	24 Meses			
10	Implementação – instalação e configuração física da solução de Ponto de Acesso.		219	1 Serviço			
	Serviço gerenciado de solução para gestão de ativos de rede, monitoramento e segurança, incluindo fornecimento de softwares, controladora (SaaS), licenciamento e suporte técnico especializado, acessórios e garantia.						
11	Solução para gestão de switches, monitoramento e segurança, incluindo fornecimento de softwares, licenciamento e suporte técnico especializado.		1	24 Meses			
12	Solução para gestão de pontos de acesso, monitoramento, e segurança, incluindo fornecimento de softwares, controladora (SaaS), licenciamento e suporte técnico especializado.		1	24 Meses			
13	Instalação, configuração e parametrização da solução para gerenciamento e gestão do parque de ativos de switches e pontos de acessos (251 equipamentos).		251	1 Serviço			

Valor Global da Proposta (em reais)	

Observações:

1 - Declaro que os serviços, equipamentos e licenciamentos ofertados obedecem a todas as condições estabelecidas no Anexo I do Edital de **Pregão Eletrônico 27/2025**, responsabilizando-me, pela veracidade desta informação;

2 - O proponentedeclara total concordância com os termos do edital, da minuta de contrato e das demais disposições e condições nos Anexos da referida licitação, modalidade pregão em sua forma eletrônica;

3 - Declaro que os preços contidos na proposta comercial incluem todos os custos e despesas diretas e indiretas, tributos incidentes, taxa de administração, materiais, serviços, encargos sociais trabalhistas, seguros, lucros e outros necessários ao cumprimento integral do objeto deste Edital e seus Anexos.

5 - Prazos de execução e Vigência do Contrato, em conformidade com os itens 12 e 13 deste Edital.

6 - Do faturamento e do pagamento, em conformidade com o item 14 deste edital.

7 - Prazo de validade da proposta, não inferior a 60 (sessenta) dias corridos, contados da data fixada para apresentação da proposta na sessão pública.

8 - No que se refere aos itens indicados na proposta de números **4, 10** e **13**, para efeito de perspectiva de receita, o proponente deve considerar pagamento único, após a emissão do termo de aceitação do gestor do instrumento de contrato.

_____, ____ de dezembro de 2025.
(Local e data)

_____
Nome e assinatura do responsável

ANEXO III
REDUÇÃO DE LANCES

Pregão Eletrônico nº 27/2025
Processo de Compras nº 873/2025

CRITÉRIO DE JULGAMENTO E LANCE

O critério de julgamento adotado será o de menor preço porá o lote único, conforme anexo II – Proposta Comercial.

O percentual efetivo deve obrigatoriamente ser considerado para aplicação em cada item que compõe a proposta de preços para cada lote disputado.

Os lances obedecerão ao fator de redução de 0,50% (meio por cento)

ANEXO IV
DECLARAÇÃO DE REGULARIDADE PERANTE O MINISTÉRIO DO TRABALHO
(Preferencialmente em papel timbrado da licitante)

Pregão Eletrônico nº 27/2025
Processo de Compras nº 873/2025

Eu,_____(nome completo), representante legal da empresa _____(razão social), interessada em participar do Pregão Eletrônico nº 27/2025, da Reitoria da Universidade Municipal de São Caetano do Sul - USCS, declaro, sob as penas da lei, que, nos termos do artigo 63, Inciso III, da Lei 14.133/2021, a empresa licitante _____(razão social), encontra-se em situação regular perante o Ministério do Trabalho, no que se refere à observância do disposto no Inciso XXXIII do artigo 7° da Constituição Federal.

_____, ____ de dezembro de 2025.
(Local e data)

_____
(Nome e assinatura do representante legal da Licitante)

ANEXO V

DECLARAÇÃO DE CUMPRIMENTO DAS CONDIÇÕES DE HABILITAÇÃO

(Preferencialmente em papel timbrado da licitante)

Pregão Eletrônico nº 27/2025
Processo de Compras nº 873/2025

À

Reitoria da Universidade Municipal de São Caetano do Sul

São Caetano do Sul - SP

Ref.: Pregão eletrônico nº 27/2025

Prezados Senhores,

Pela presente, declaramos para efeito do cumprimento ao estabelecido no inciso I do artigo 63º da Lei Federal nº 14.133/2021, sob as penalidades cabíveis, que cumprimos plenamente os requisitos de habilitação exigidos neste Edital.

_____, ____ de dezembro de 2025.
(Local e data)

_____
(Nome e assinatura do representante legal da Licitante)

ANEXO VI

DECLARAÇÃO DE ENQUADRAMENTO COMO MICROEMPRESA OU EMPRESA DE PEQUENO PORTE PARA FRUIÇÃO DOS BENEFÍCIOS DA LEI COMPLEMENTAR Nº 123/2006 COM AS DEVIDAS ALTERAÇÕES INTRODUZIDAS PELAS LEIS COMPLEMENTARES FEDERAIS Nº 147/2014 E 155/2016, E LEI MUNICIPAL Nº 4.660/2008

(Preferencialmente em papel timbrado da licitante)

Pregão Eletrônico nº 27/2025
Processo de Compras nº 873/2025

_____(nome do licitante), com sede _____(endereço completo), inscrita no CNPJ sob o número _____, Declara, para fins do disposto na Lei Complementar nº 123/2006 com as devidas alterações introduzidas pelas Leis Complementares Federais nº 147/2014 e 155/2016, e Lei Municipal nº 4.660/2008 sob as sanções administrativas cabíveis e sob as penas da lei, que esta Empresa, na presente data, enquadra-se como:

(...) MICROEMPRESA, conforme inciso I do artigo 3º da Lei Complementar nº 123, de 14/12/2006 com as devidas alterações introduzidas pelas Leis Complementares Federais nº 147/2014 e nº 155/2016 e, inciso I do artigo 5º da Lei Municipal nº 4.660/2008.

(...) EMPRESA DE PEQUENO PORTE, conforme inciso II do artigo 3º da Lei Complementar nº 123 de 14/12/2006, com as devidas alterações introduzidas pelas Leis Complementares Federais nº147/2014 e nº 155/2016 e, inciso II do artigo 5º da Lei Municipal nº 4.660/2008.

Declara, ainda, que a empresa está excluída das vedações constantes do § 4º do artigo 3º da Lei Complementar nº 123, de 14 de dezembro de 2006 com as devidas alterações introduzidas pelas Leis Complementares Federais nº 147/2014 e nº 155/2016 e, § 2º do artigo 5º da Lei Municipal nº 4.660/2008.

_____, ____ de dezembro de 2025.
(Local e data)

_____
(Nome e assinatura do representante legal da Licitante)

ANEXO VII

DECLARAÇÃO DE ATENDIMENTO ÀS NORMAS RELATIVAS À SAÚDE E SEGURANÇA NO TRABALHO

(Preferencialmente em papel timbrado da licitante)

Pregão Eletrônico nº 27/2025
Processo de Compras nº 873/2025

A_____(razão social), por seu(s) representante(s) legal(is), interessada em participar do Pregão Eletrônico nº 27/2025, da Reitoria da Universidade Municipal de São Caetano do Sul - USCS, declara, sob as penas da lei, que observa as normas relativas à saúde e segurança no Trabalho, para os fins estabelecidos pelo parágrafo único do artigo 117 da Constituição do Estado de São Paulo.

_____, ____ de dezembro de 2025.
(Local e data)

_____
(Nome e assinatura do representante legal da Licitante)

ANEXO VIII

DECLARAÇÃO DE CONDIÇÕES GERAIS DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

(Preferencialmente em papel timbrado da licitante)

Pregão Eletrônico nº 27/2025
Processo de Compras nº 873/2025

A Licitante declara estar de ciente e de acordo com os termos estabelecidos neste Edital, bem como:

1. Que atende aos padrões tecnológicos para sistemas, aplicações, arquivos de dados e outras ferramentas, garantindo que adota e implementa todas as medidas organizacionais e técnicas de segurança exigidas pela Lei Geral de Proteção de Dados - Lei n 13.709, de 14 de agosto de 2018 e suas alterações, bem como manterá durante o prazo do Contrato, as medidas para proteção dos Dados Pessoais contra destruição indevida, compartilhamento irregular ou não autorizado, perda acidental, alteração, acesso ou divulgação irregulares e/ou qualquer forma de Tratamento inadequado ou ilícito dos Dados Pessoais que lhe forem compartilhados.

2. Que as medidas de segurança e proteção dos Dados Pessoais serão pelo menos iguais ou superiores a cumulativamente a qualquer regulamentação definida pela ANPD ou outro órgão governamental competente, bem como aos padrões do ramo da USCS.

3. Que se encontra plenamente capaz de cumprir com os termos e condições do presente Edital, conforme declarado no Anexo II – Proposta Comercial e que, na eventualidade de uma relevante alteração das normas aplicáveis às atividades de Tratamento de Dados Pessoais que tenha potencial de modificar sua conformidade legal e contratual notificará a USCS.

_____, ____ de dezembro de 2025.
(Local e data)

_____
(Nome e assinatura do representante legal da Licitante)

ANEXO IX

DECLARAÇÃO DE QUE SUA PROPOSTA ECONÔMICA CONSIDERA OS CUSTOS TRABALHISTAS

(Preferencialmente em papel timbrado da licitante)

Pregão Eletrônico nº 27/2025
Processo de Compras nº 873/2025

A_____(razão social), por seu representante legal, interessada em participar do Pregão Eletrônico nº 27/2025, da Reitoria da Universidade Municipal de São Caetano do Sul - USCS, declara, sob as penas da lei, que sua proposta econômica compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal de 1988, 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 comercial, consoante participação no processo licitatório em referência.

_____, ____ de dezembro de 2025.
(Local e data)

_____
(Nome e assinatura do representante legal da Licitante)

ANEXO X

DECLARAÇÃO DE CUMPRIMENTO À EXIGÊNCIA DE RESERVA DE CARGOS

(Preferencialmente em papel timbrado da licitante)

Pregão Eletrônico nº 27/2025
Processo de Compras nº 873/2025

Em cumprimento as determinações contidas no inciso IV do artigo 63 da Lei Federal 14.133/2021, a proponente licitante _____(razão social), por seu representante legal, interessada em participar do Pregão Eletrônico nº 27/2025, da Reitoria da Universidade Municipal de São Caetano do Sul - USCS, declara, sob as penas da lei, que cumpre os requisitos legais pertinentes à habilitação social no que concerne à reserva legal de cargos para pessoas portadores de deficiência e para reabilitados da Previdência Social previstas na Lei Federal 8.213/1991.

_____, ____ de dezembro de 2025.
(Local e data)

_____
(Nome e assinatura do representante legal da Licitante)

ANEXO XI

DECLARAÇÃO DE QUALIFICAÇÃO TÉCNICA DA EQUIPE DE PROFISSIONAIS QUE SERÁ ALOCADA NA EXECUÇÃO DO PROJETO

(preferencialmente em papel timbrado da licitante)

Pregão Eletrônico nº 27/2025
Processo de Compras nº 873/2025

A licitante _____(razão social), por seu representante legal, interessada em participar do Pregão Eletrônico nº 27/2025, da Reitoria da Universidade Municipal de São Caetano do Sul - USCS, declara, sob as penas da lei, que dispõe de profissional técnico qualificado, consonante, especificamente com a necessidade técnica exigida para o projeto de implementação da Solução de Serviços gerenciados para Gestão de ativos de rede WiFi, monitoramento e segurança, cujo quantitativo satisfaz plenamente a demanda necessária para o pleno atendimento das exigências contidas no documento Termo de Referência deste Edital - Anexo I.

_____, ____ de dezembro de 2025.
(Local e data)

_____
Nome e assinatura do representante legal da Licitante

ANEXO XII

DECLARAÇÃO DE QUALIFICAÇÃO DE CREDENCIADO JUNTO AO FABRICANTE DO EQUIPAMENTO

(preferencialmente em papel timbrado da licitante)

Pregão Eletrônico nº 27/2025
Processo de Compras nº 873/2025

A licitante _____(razão social), por seu representante legal, interessada em participar do Pregão Eletrônico nº 27/2025, da Reitoria da Universidade Municipal de São Caetano do Sul, especificamente em relação aos equipamentos ***switch de acesso e pontos de acesso***, **declara**, sob as penas da lei, que detém a condição de parceiro credenciado junto ao fabricante cujo status lhes permite atuar como fornecedor de equipamentos na área de solução de serviço gerenciado de ativos de rede WiFi, ou, que é revendedor autorizado do fabricante, com capacidade para oferecer e fornecer suporte aos equipamentos efertados *as a service*, bem como declara estar apto a realizar suas implantações, de acordo com as exigências contidas no termo de referência do edital.

_____, ____ de dezembro de 2025.
(Local e data)

_____
Nome e assinatura do representante legal da Licitante

ANEXO XIII

ATESTADO DE VISITA TÉCNICA

Pregão Eletrônico nº 27/2025
Processo de Compras nº 873/2025

***Importante*:** Na hipótese de que pelo menos uma das cinco unidades (Barcelona, Centro, Centro II, Conceição e Itapetininga) não seja vistoriada, o proponente deverá preencher o **Anexo XIV** para a unidade não visitada.

(Razão social da empresa)_____, inscrita no CNPJ sob nº_____, por intermédio de seu representante, o senhor_____, portador da do CPF nº _____, declara expressamente, para fins de participação na licitação modalidade Pregão Eletrônico supra citado, em atendimento ao item 2.1.4. do respectivo edital, que visitou as instalações dos Campus (indicar a(s) unidade(s) visitada(s))_____ Barcelona, Campus Centro, Centro II, Conceição e Itapetininga, unidades em que se implementará a Solução de serviço gerenciado para gestão de ativos de rede WiFi, monitoramento e segurança, incluindo fornecimento de softwares, equipamentos e licenciamentos na modalidade *As a Service*, suporte técnico especializado, acessórios e garantias, segundo os critérios estabelecidos no edital, e seus anexos, onde foi perfeitamente cientificado acerca dos locais e as particularidades pertinentes aos serviços a serem executados, de acordo com as condições exigidas na licitação em referência.

São Caetano do Sul, ____ de dezembro de 2025

._____
(assinatura do representante do pretenso licitante)

_____
(assinatura do servidor da USCS)

ANEXO XIV
DECLARAÇÃO DE ABSTENÇÃO DE VISTORIA TÉCNICA
(Preferencialmente em papel timbrado da licitante)

Pregão Eletrônico nº 27/2025
Processo de Compras nº 873/2025

A empresa (razão social) _____, por intermédio de seu representante legal, interessada em participar do Pregão Eletrônico nº 27/2025, da Universidade Municipal de São Caetano do Sul - USCS, declara que se ***Abstem*** de realizar a vistoria técnica na unidade (nome do campus/unidade não visitada, ou todas as unidades) _____ e está ciente que não poderá alegar desconhecimento do local e suas condições, bem como das dificuldades que poderão surgir no curso da execução dos serviços objeto deste processo licitatório.

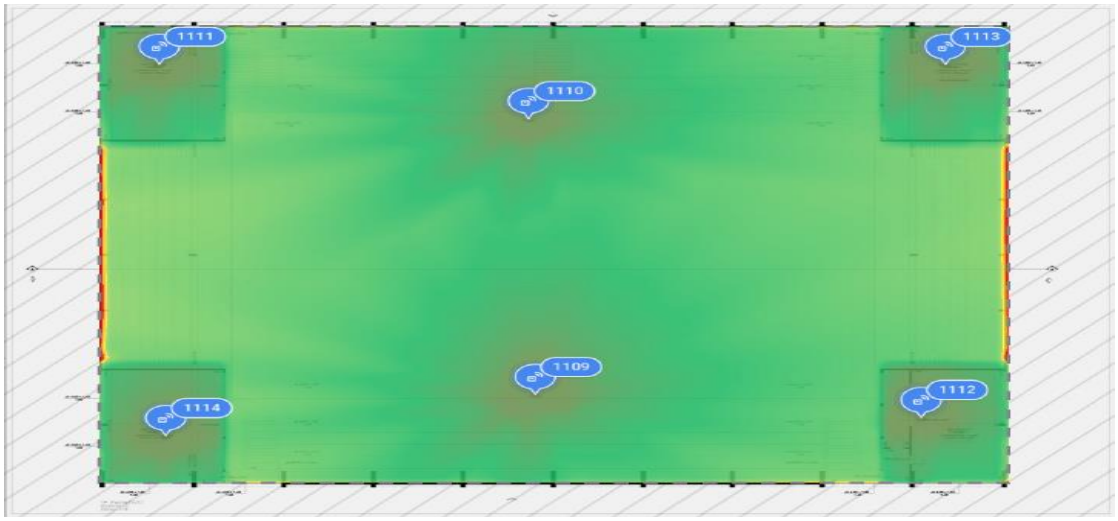
_____, ____ de dezembro de 2025.
(Local) (data)

_____
(Nome e assinatura do representante legal da Licitante)

ANEXO XV
LAY OUT E TOPOLOGIA ACERCA DA SOLUÇÃO PROPOSTA PARA DISTRIBUIÇÃO DOS EQUIPAMENTOS WI-FI
site survey teórico

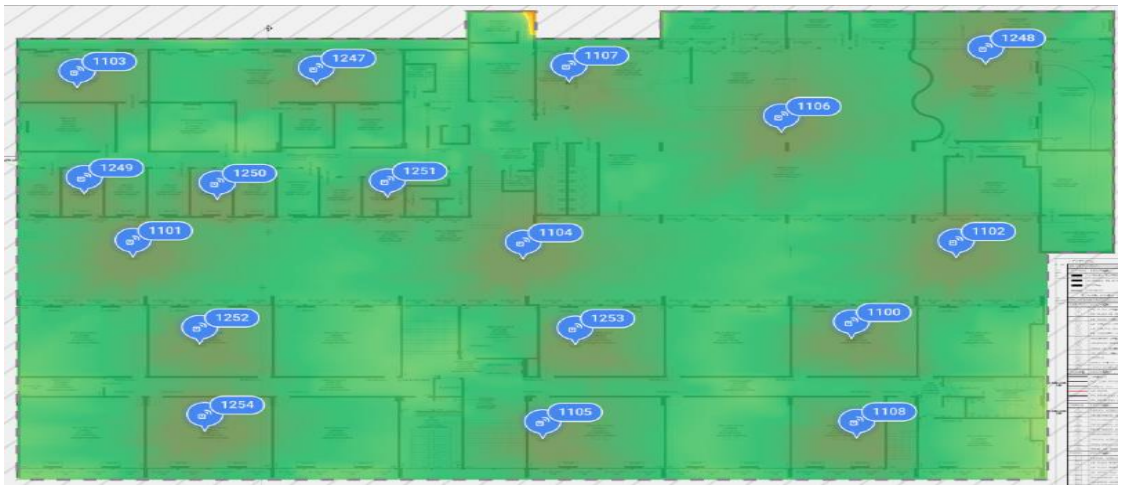
CAMPUS BARCELONA – Disposição dos equipamentos no projeto

Campus Barcelona - Bloco C 1º Pavimento

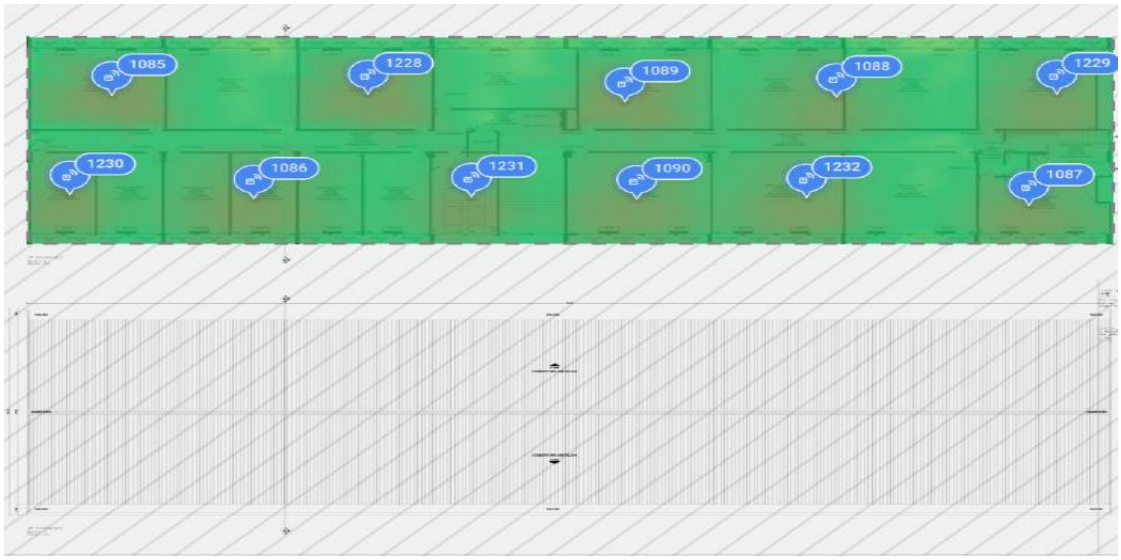


Campus Barcelona - Bloco C 1º e 2º Pavimentos

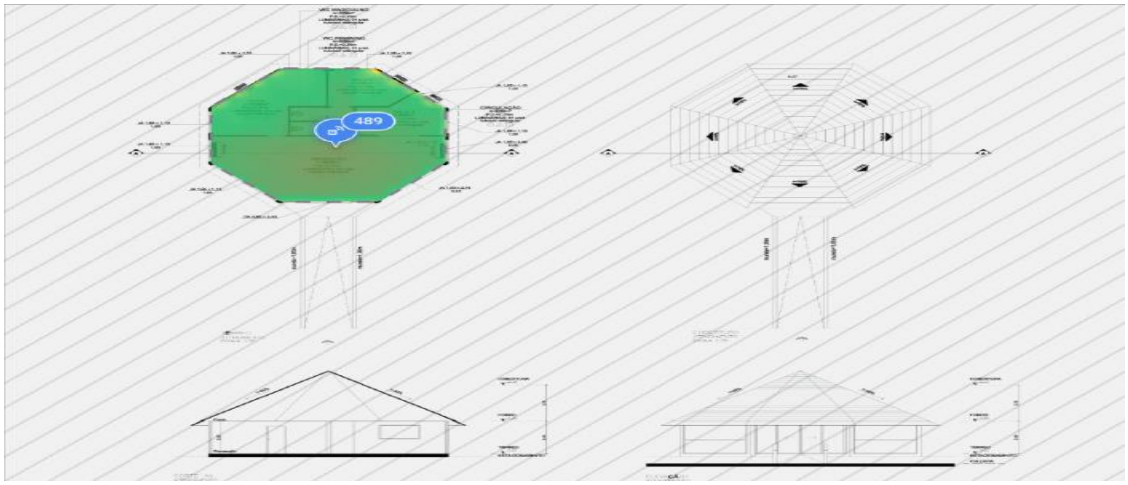
Campus Barcelona - Bloco A e Subsolo - 1º Pavimento



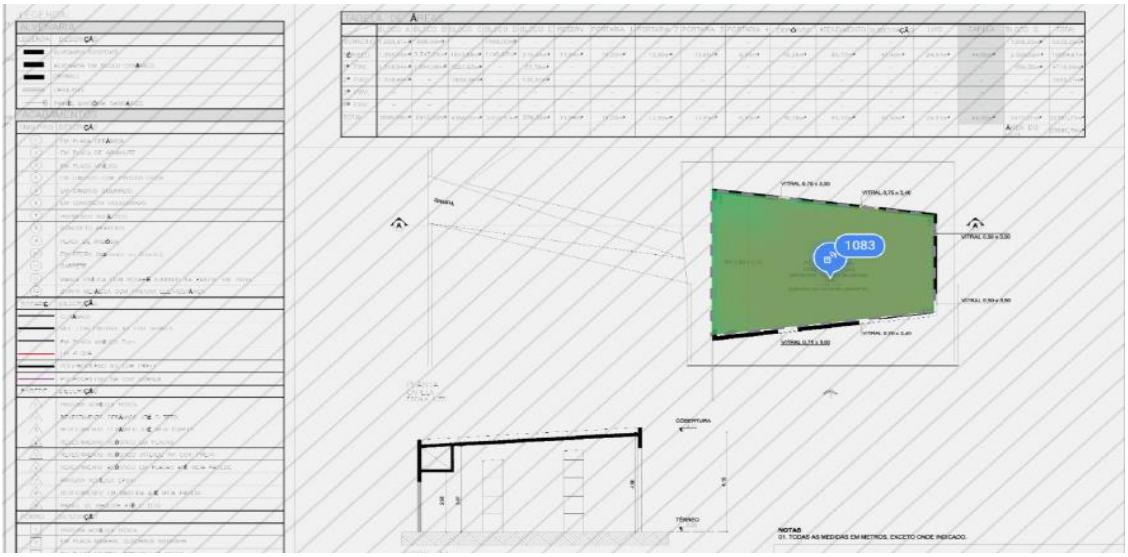
Campus Barcelona - Bloco A - 2º Pavimento e Cobertura



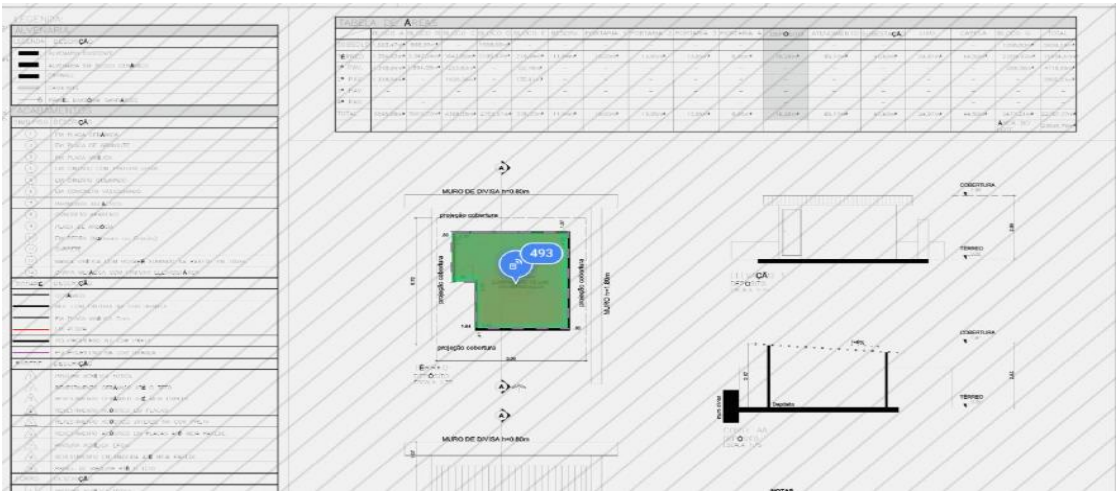
Campus Barcelona - Anexo Atendimento



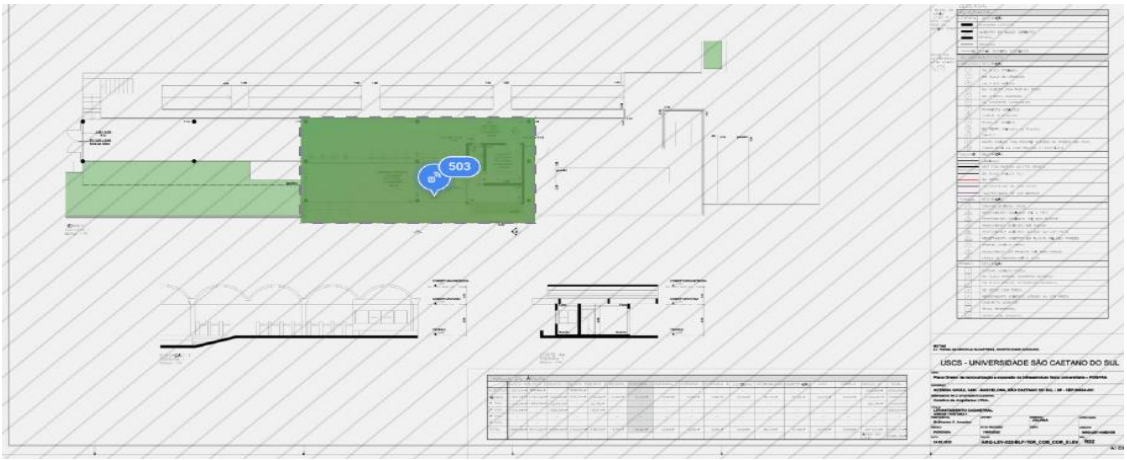
Campus Barcelona - Anexo Capela



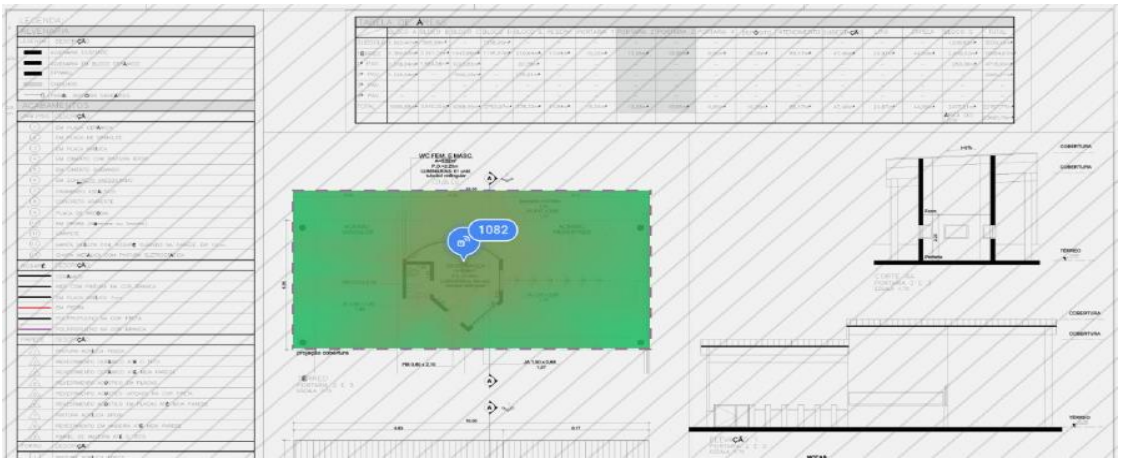
Campus Barcelona - Anexo Depósito



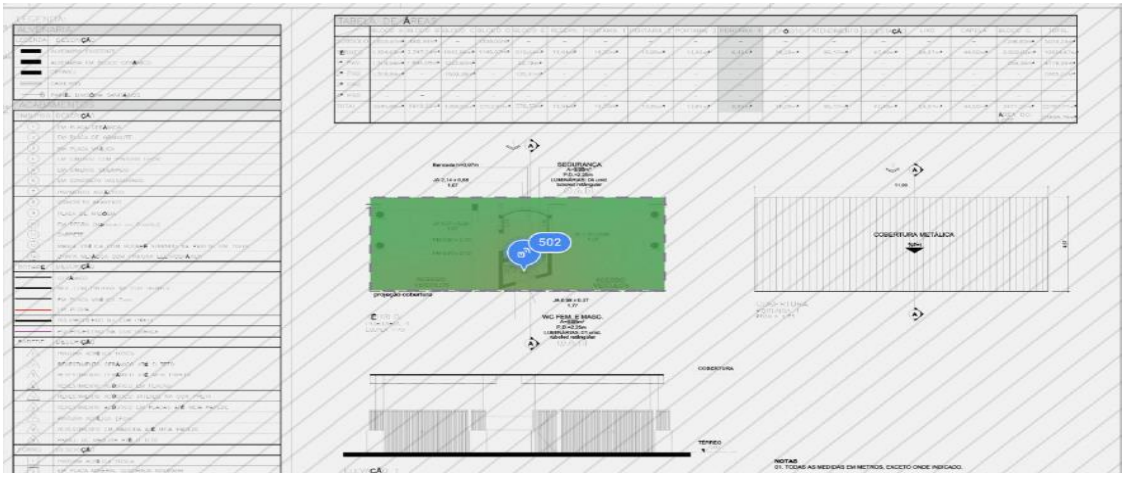
Campus Barcelona - Anexo Portaria 1



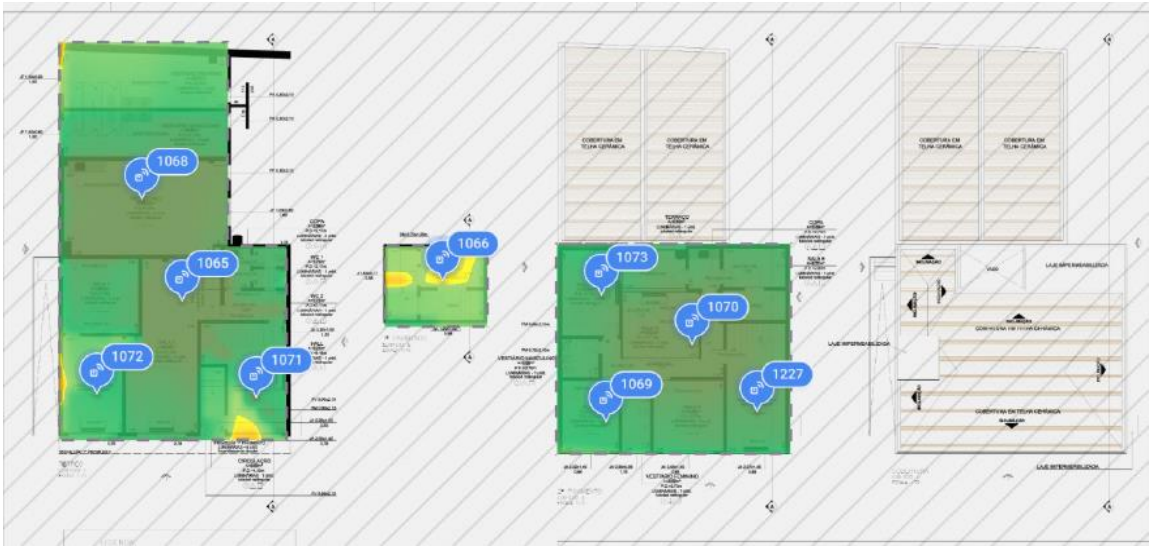
Campus Barcelona - Anexo Portarias 2 e 3



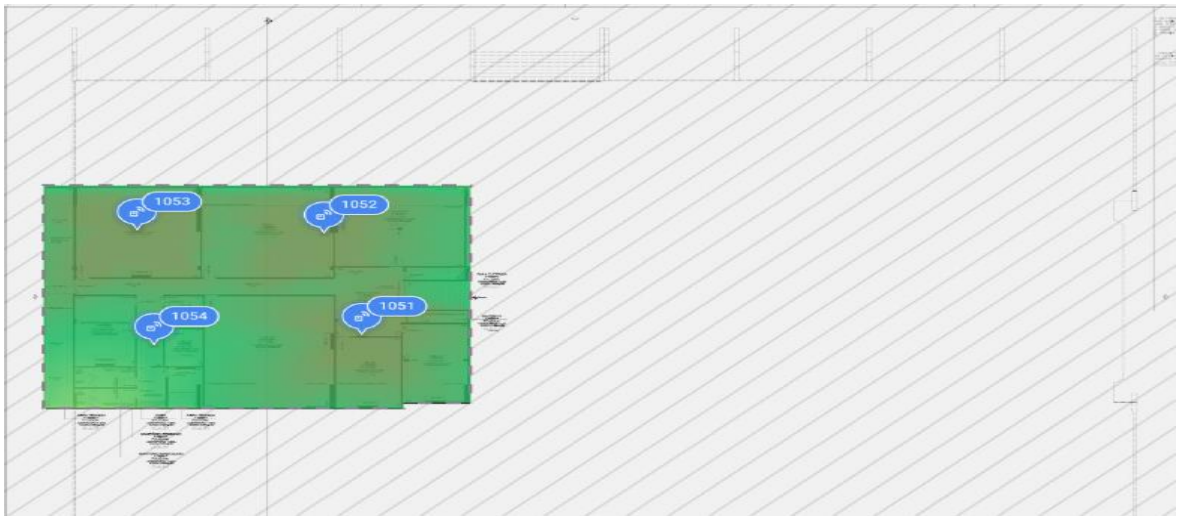
Campus Barcelona - Anexo Portaria 4



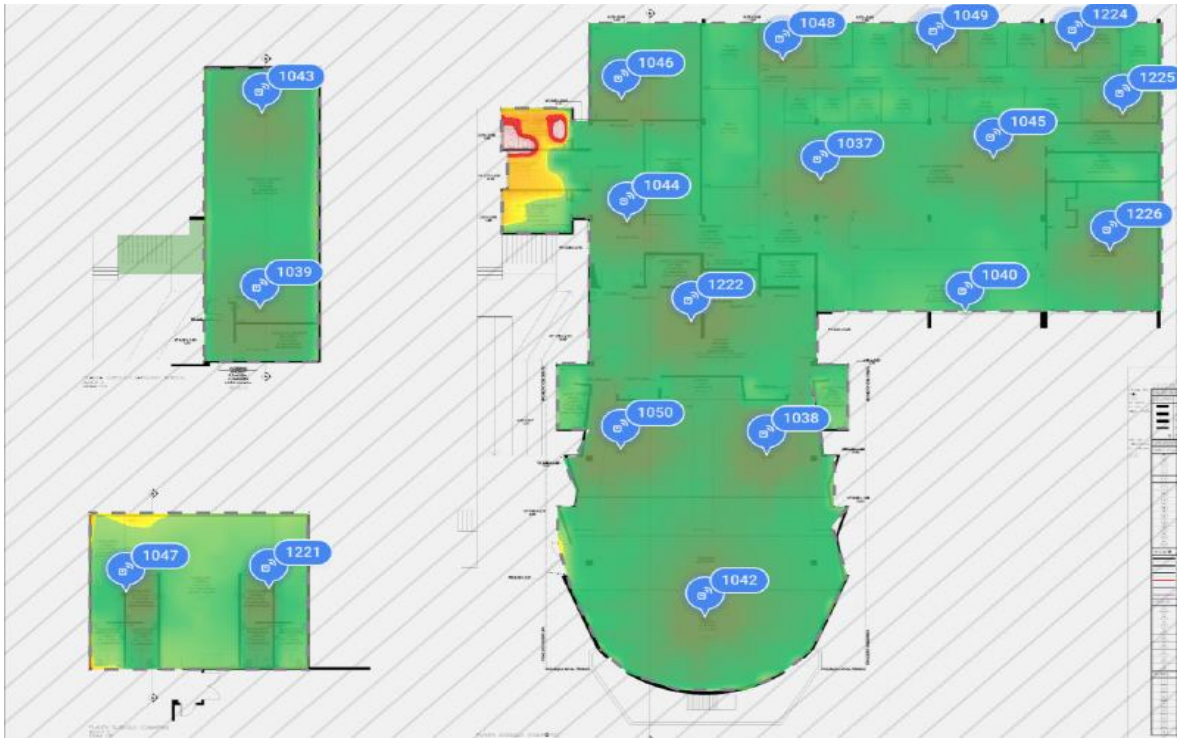
Campus Barcelona – Bloco E



Campus Barcelona – Bloco B - Subsolo

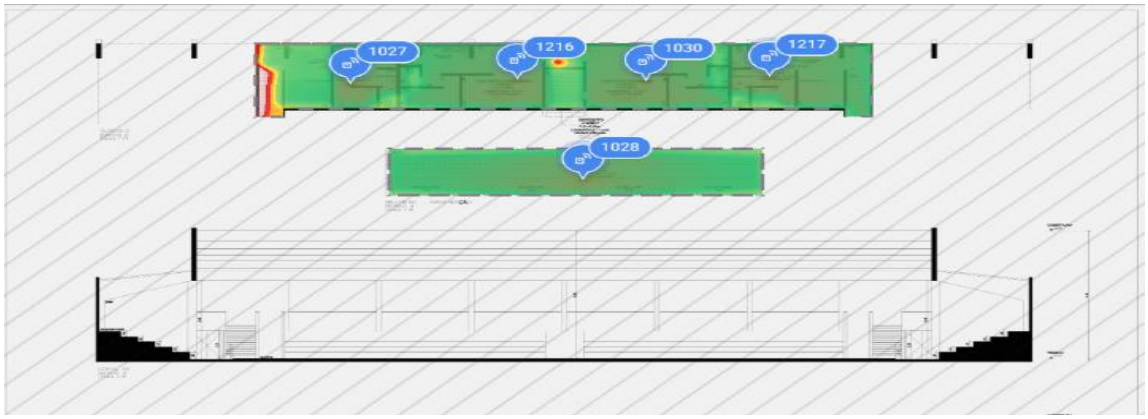


Campus Barcelona – Subsolo Auditório - Bloco D

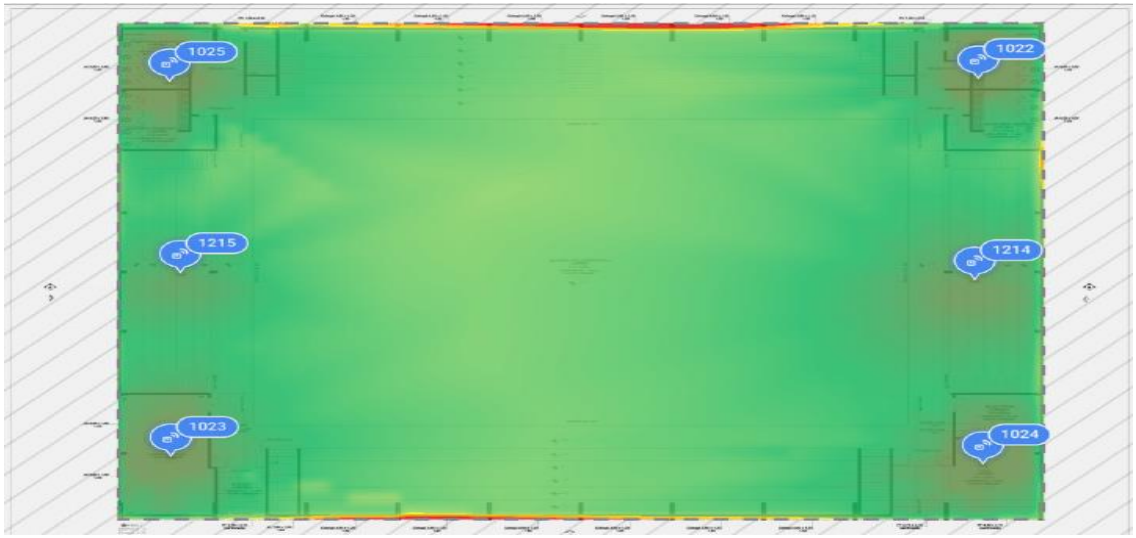


Campus Barcelona – Subsolo Manutenção - Bloco G

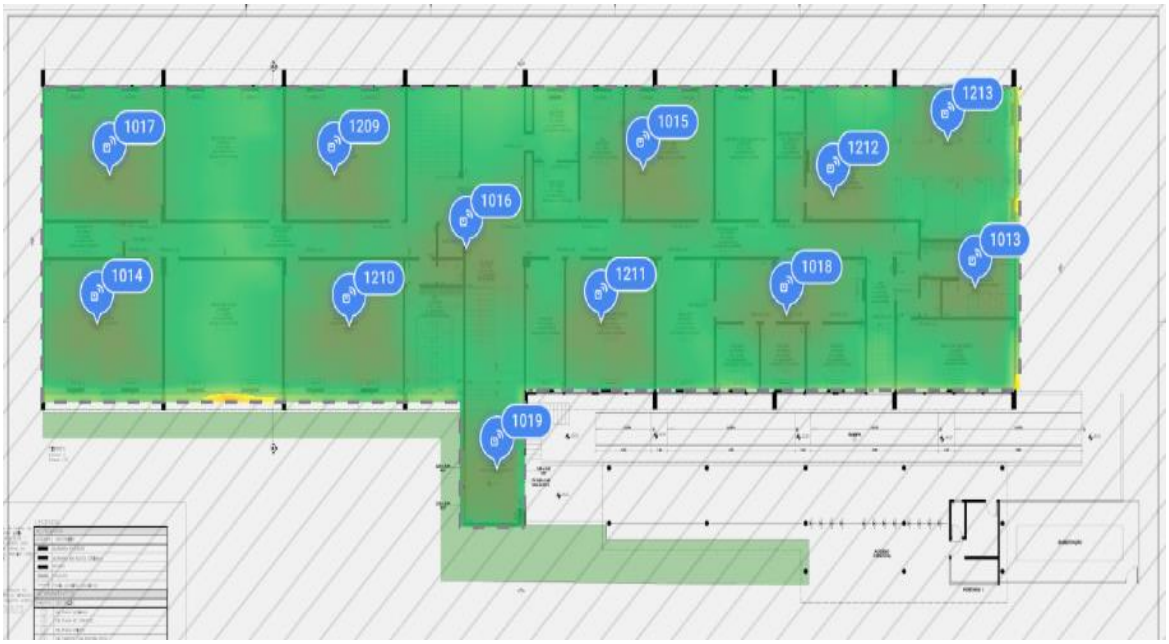
Campus Barcelona – Subsolo Quadra - Bloco G



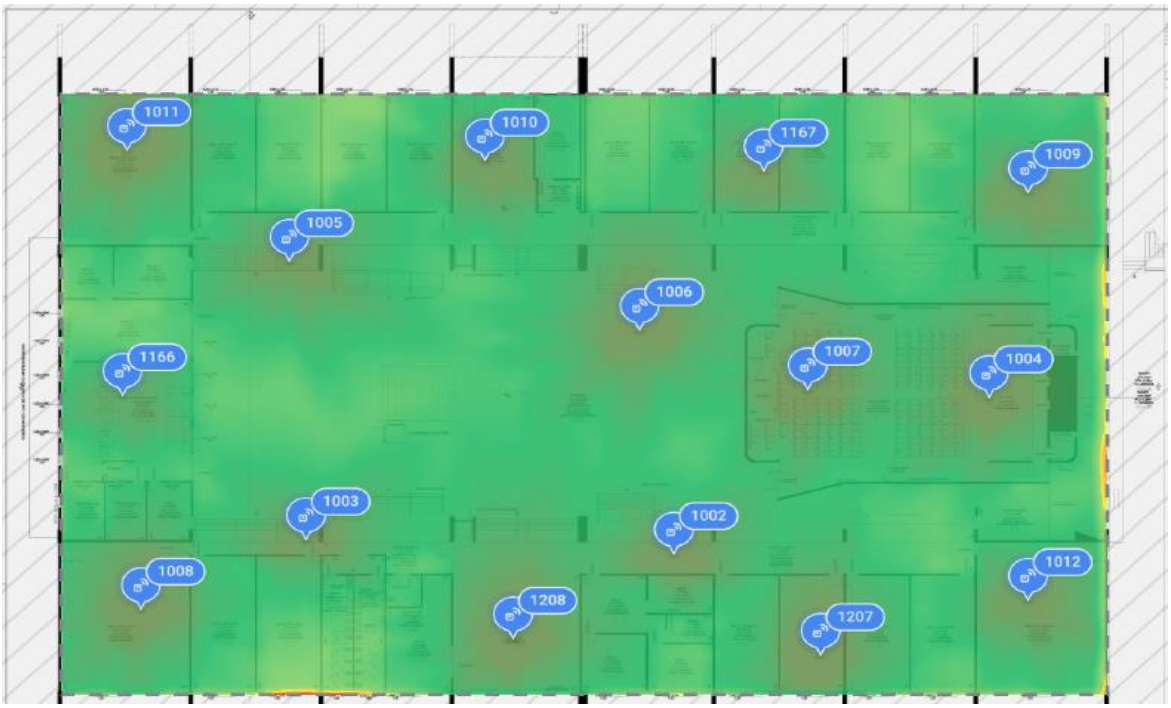
Campus Barcelona – Subsolo Térreo Quadra - Bloco G



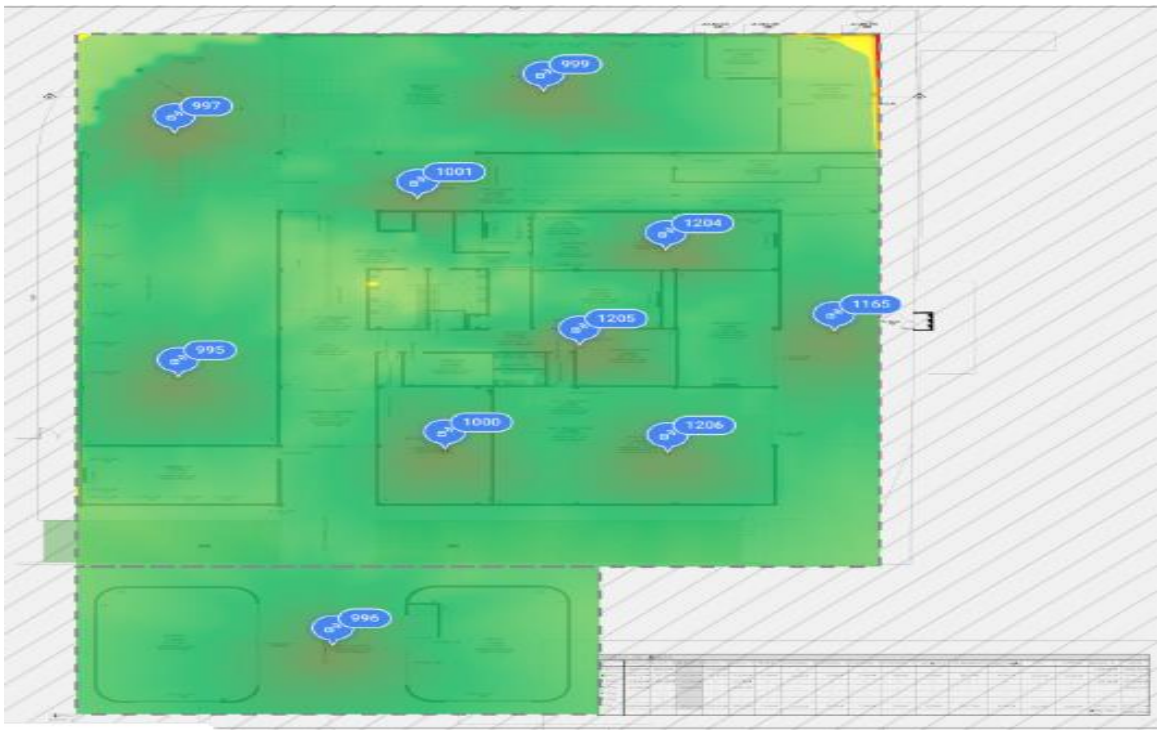
Campus Barcelona – Térreo - Bloco A



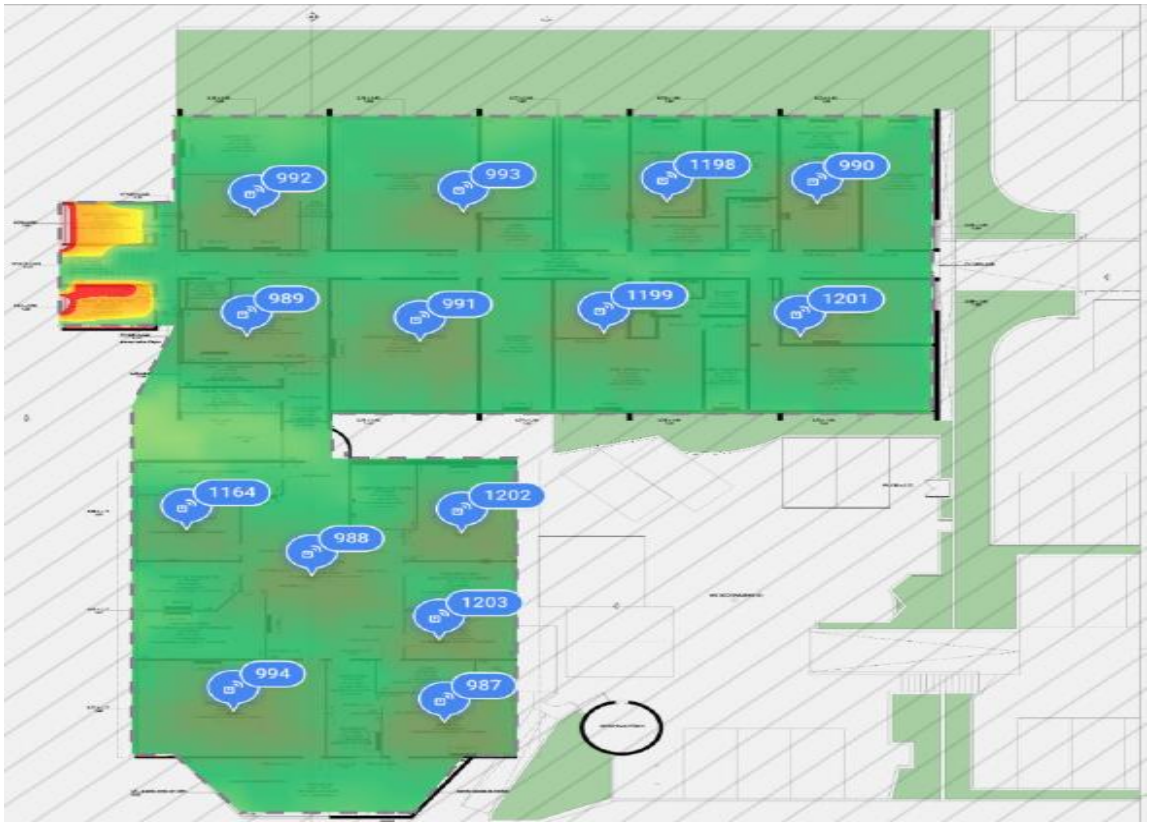
Campus Barcelona – Térreo - Bloco B



Campus Barcelona – Térreo - Bloco C

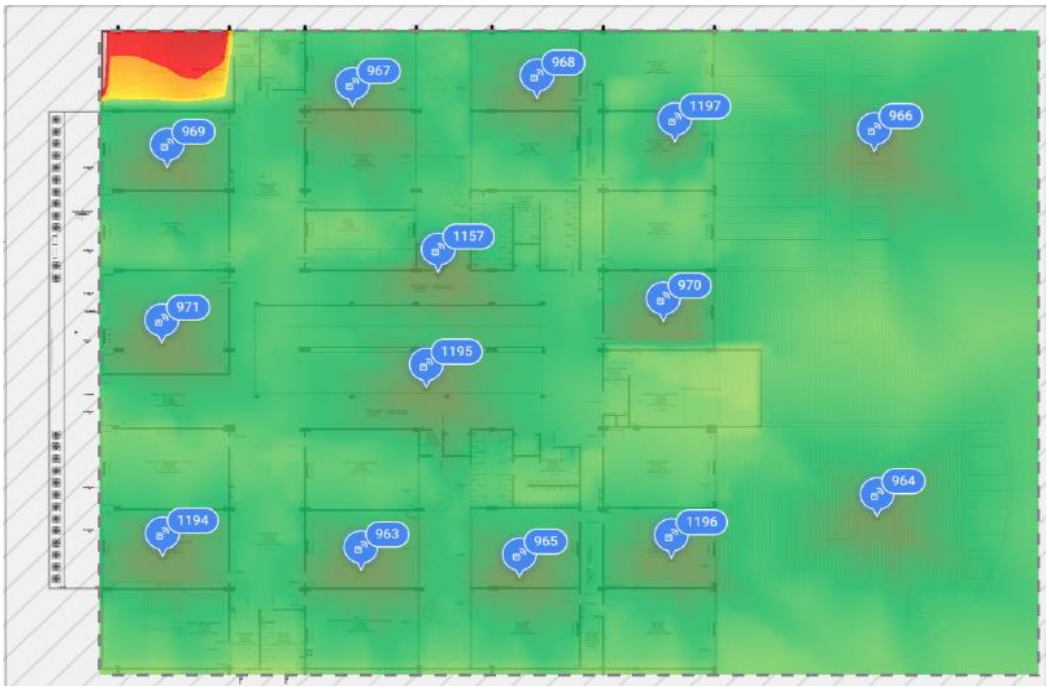


Campus Barcelona – Térreo - Bloco D

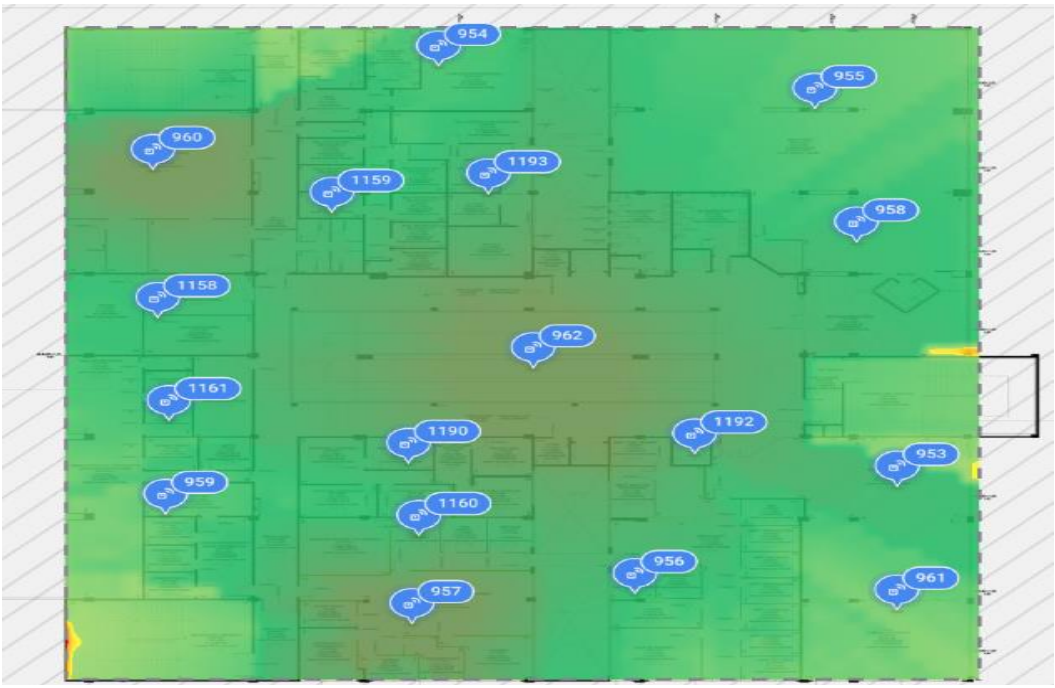


CAMPUS CENTRO – Disposição dos equipamentos no projeto

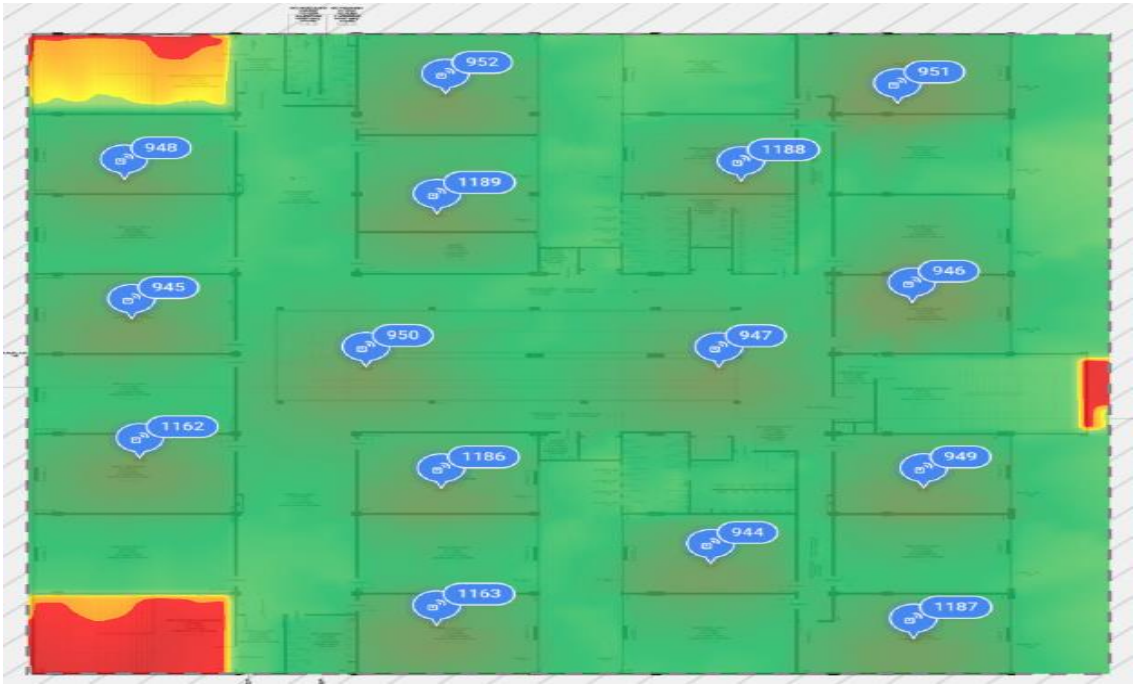
Campus Centro – Primeiro Andar



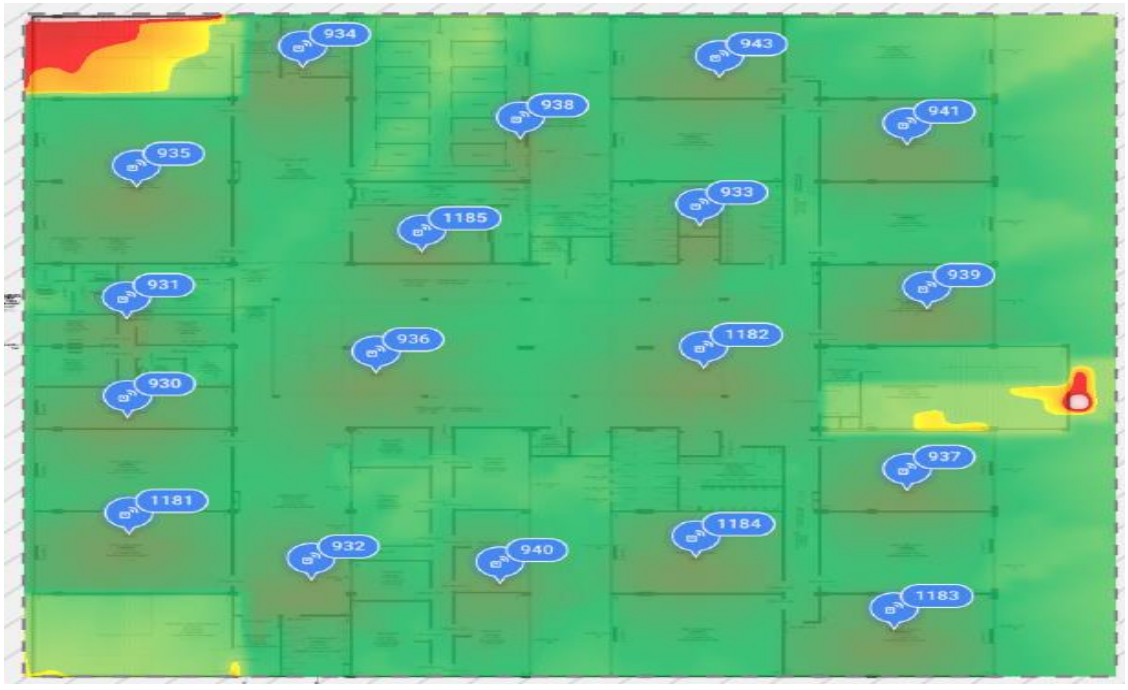
Campus Centro – Segundo Andar



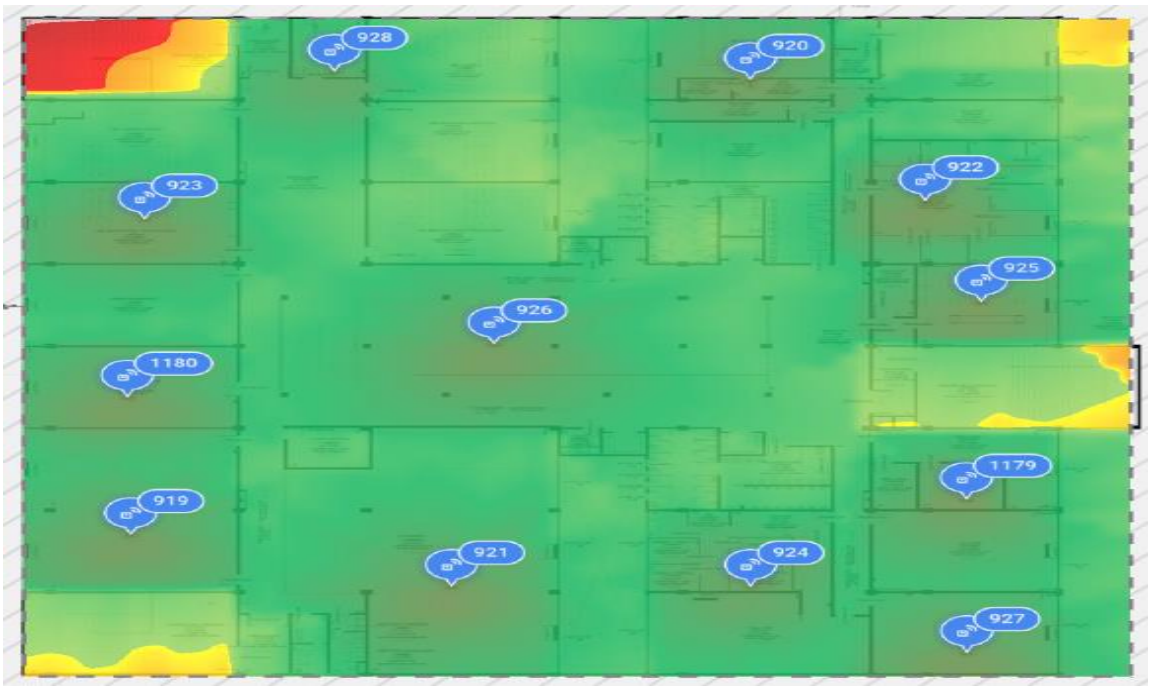
Campus Centro – Terceiro Andar



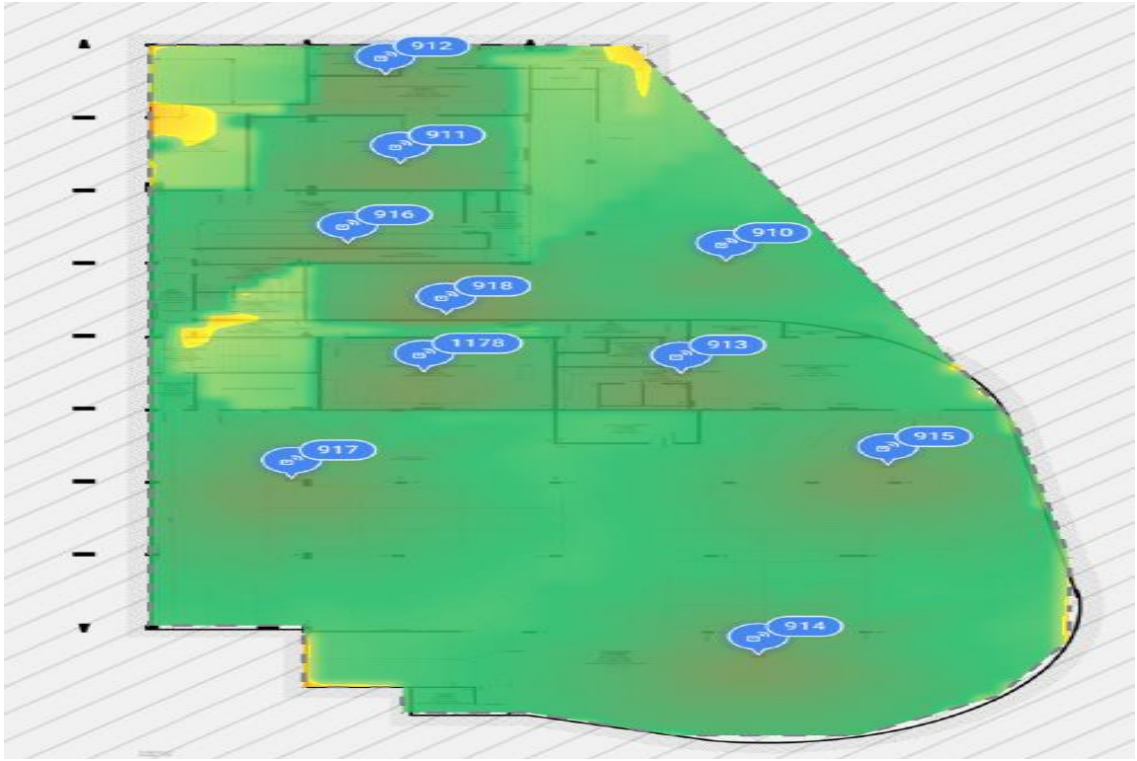
Campus Centro – Quarto Andar



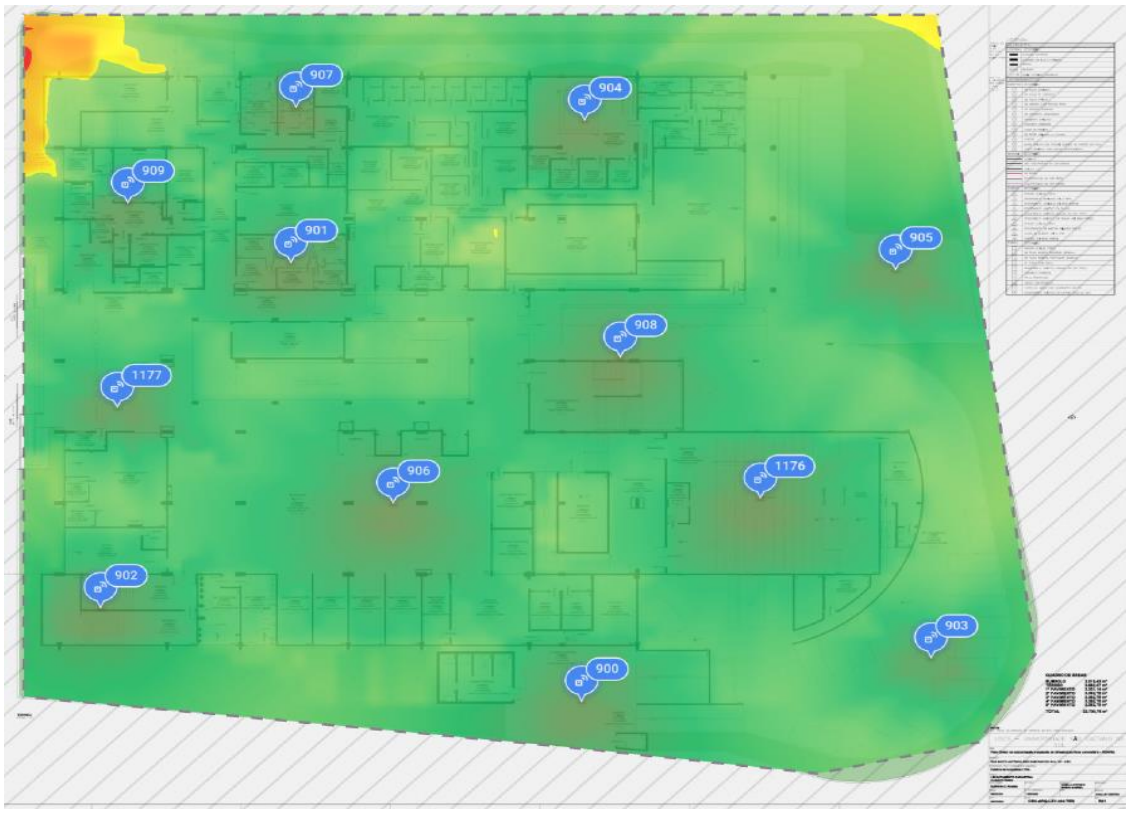
Campus Centro – Quinto Andar



Campus Centro – Subsolo

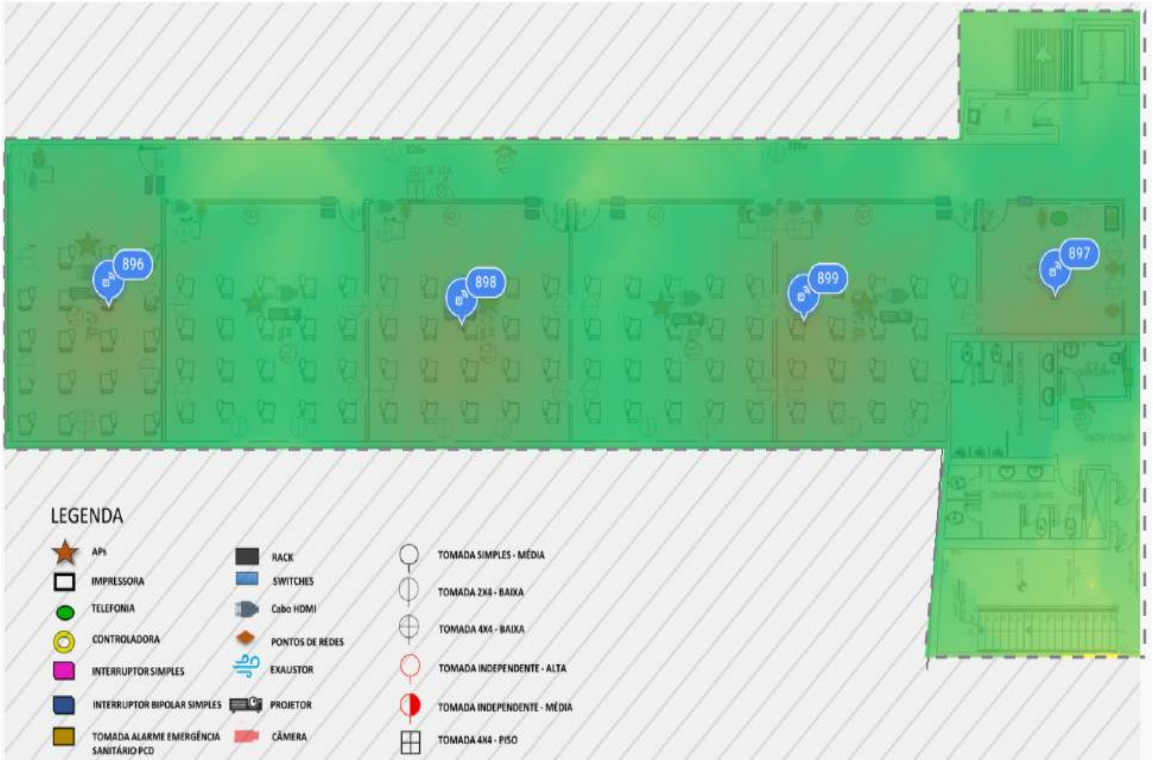


Campus Centro – Térreo

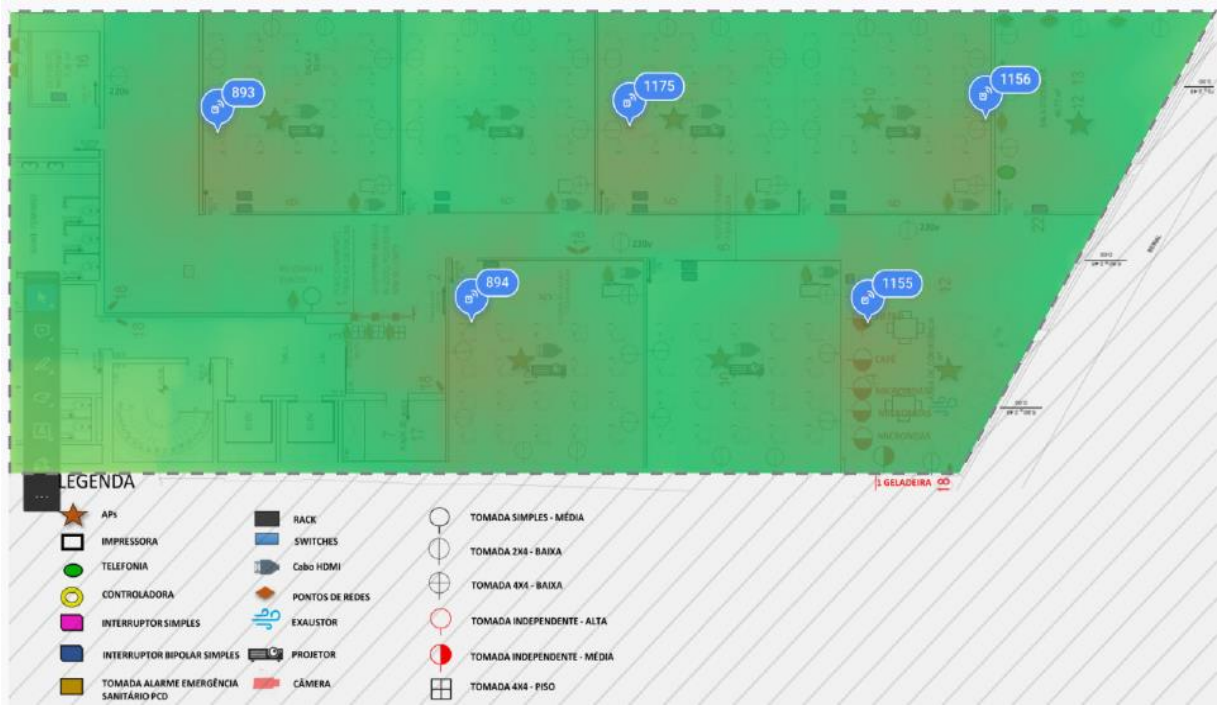


CAMPUS CENTRO II – Disposição dos equipamentos no projeto

Campus Centro II – 1

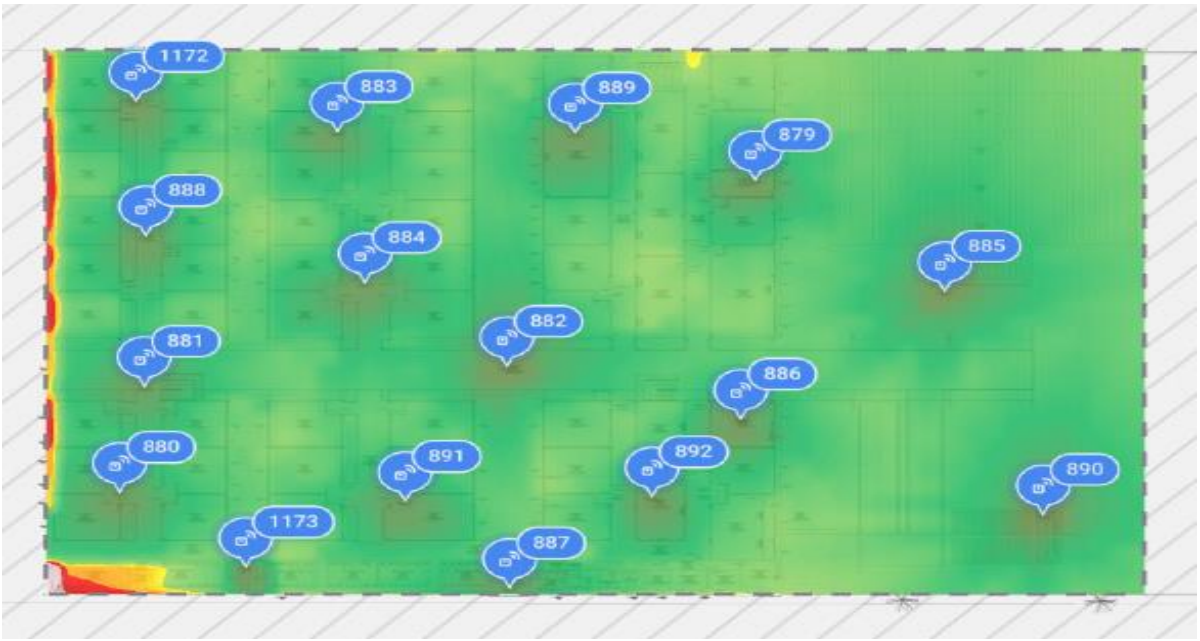


Campus Centro II – 2

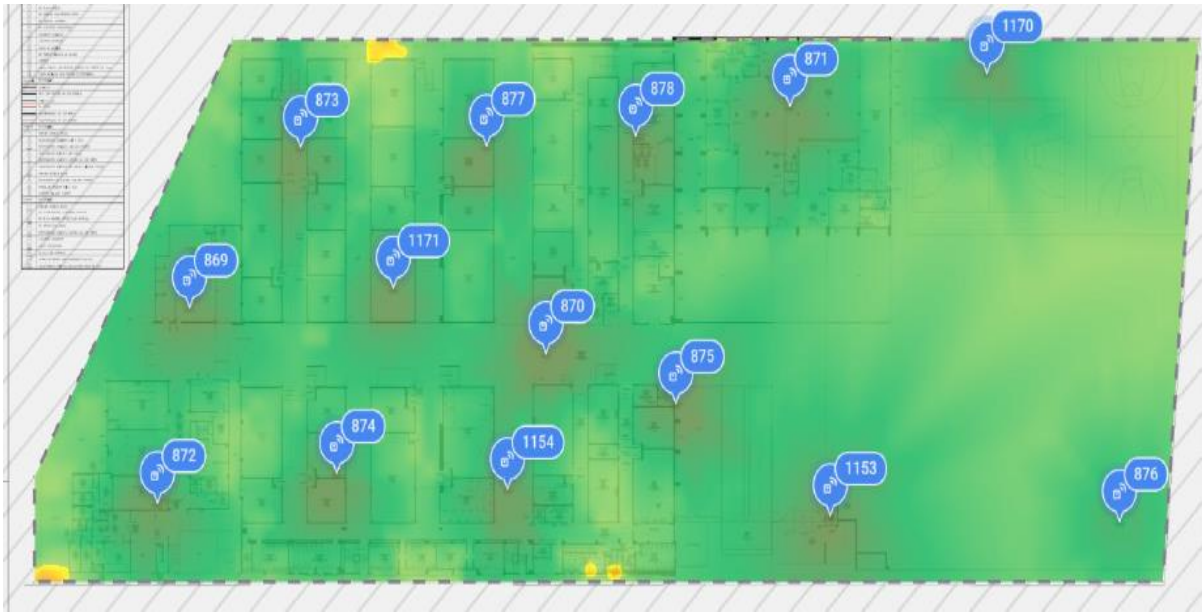


CAMPUS CONCEIÇÃO – Disposição dos equipamentos no projeto

Campus Conceição – Primeiro Andar



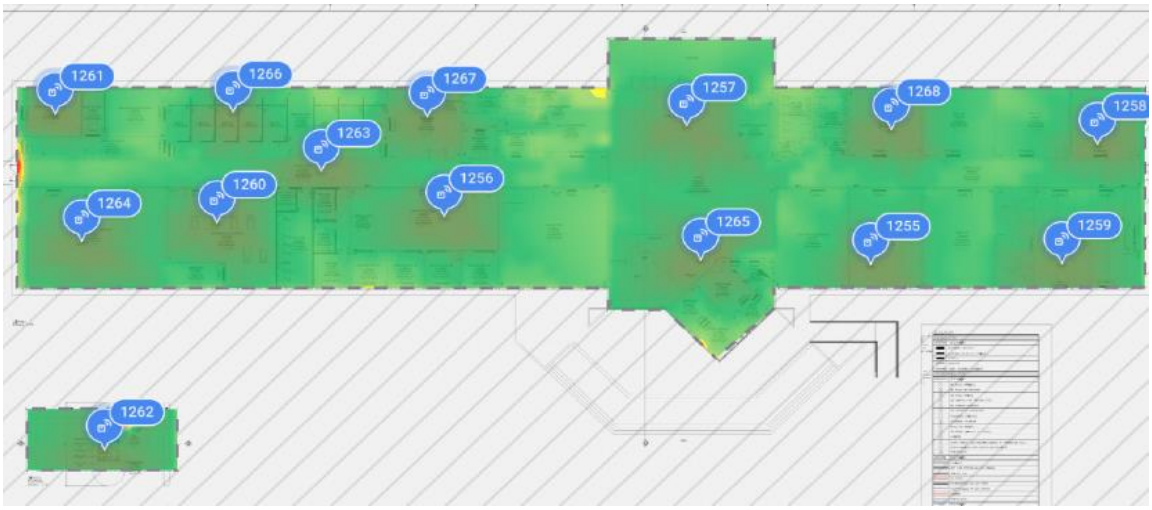
Campus Conceição – Térreo



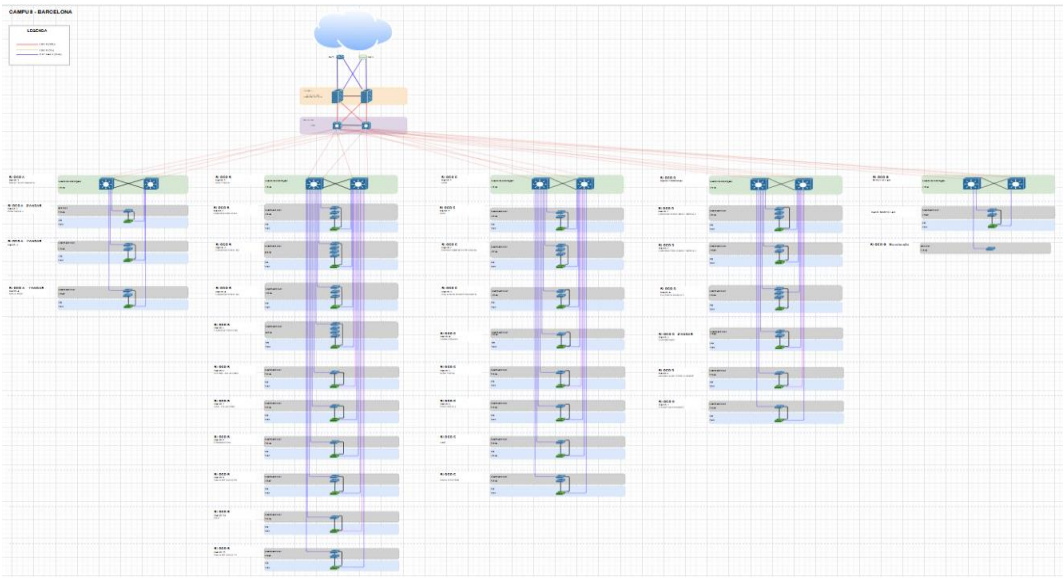
CAMPUS ITAPETININGA – Disposição dos equipamentos no projeto

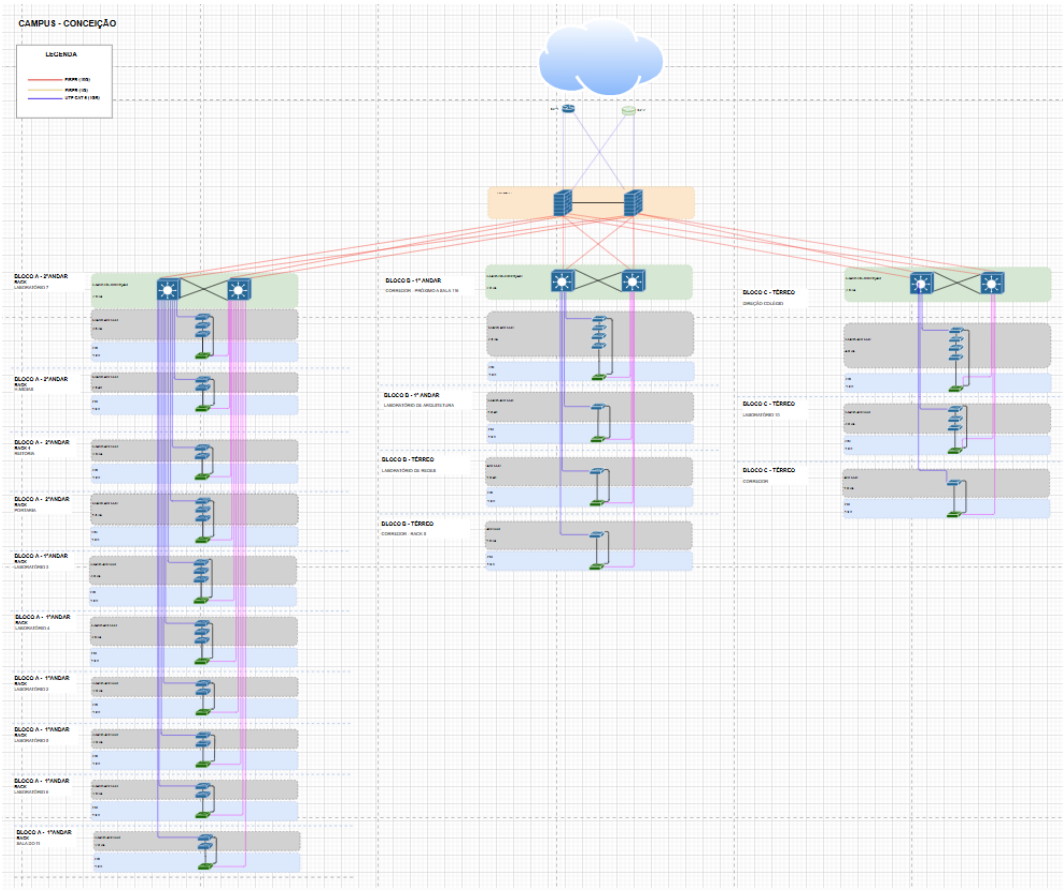
Campus Itapetininga

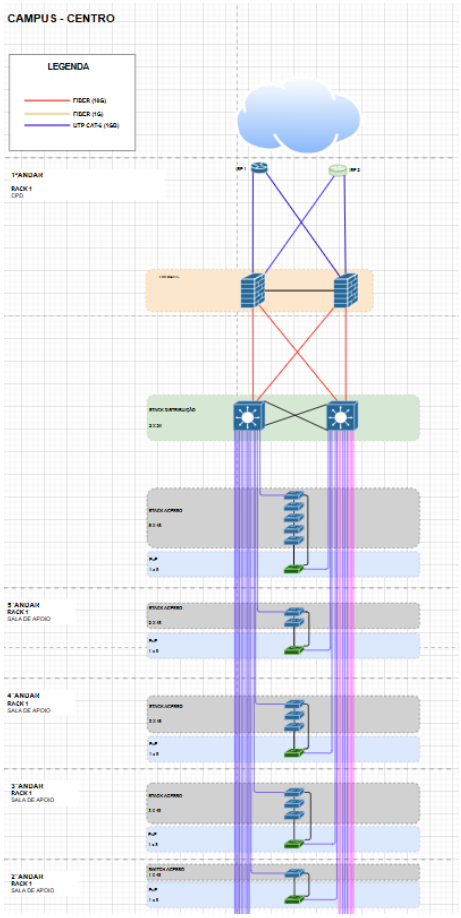
Campus Itapetininga - Atual

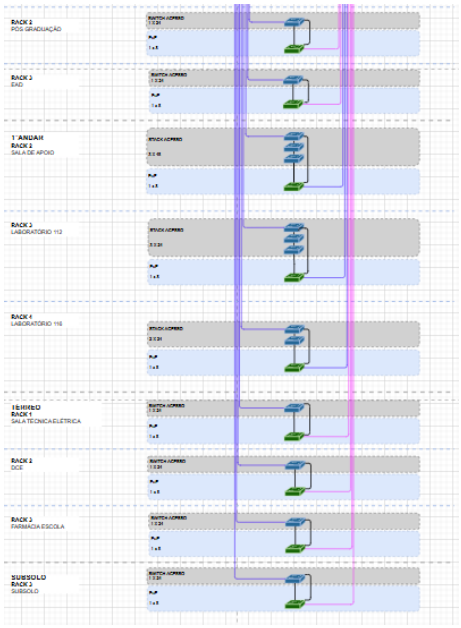


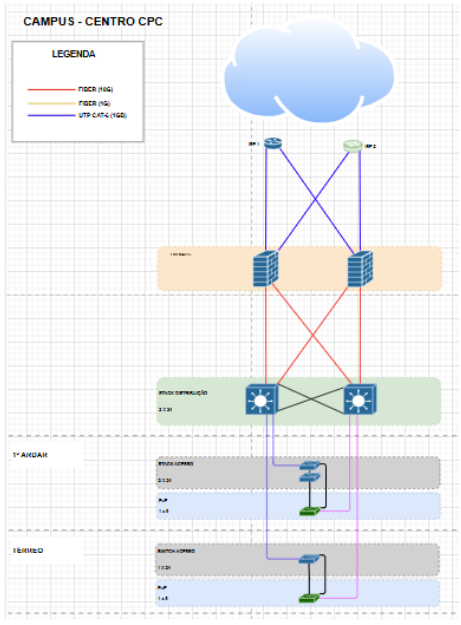
TOPOLOGIA E INTERCONEXÕES

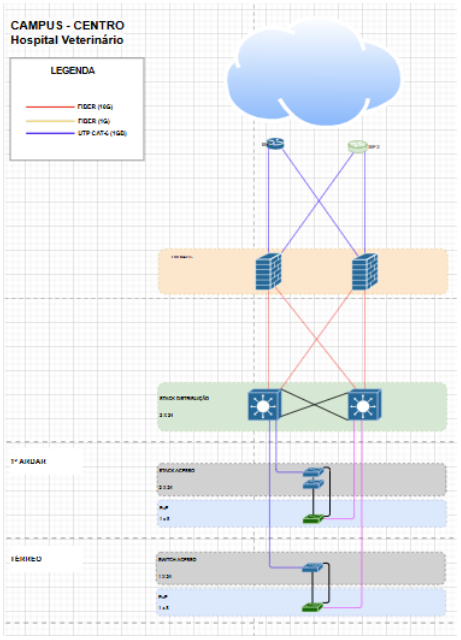


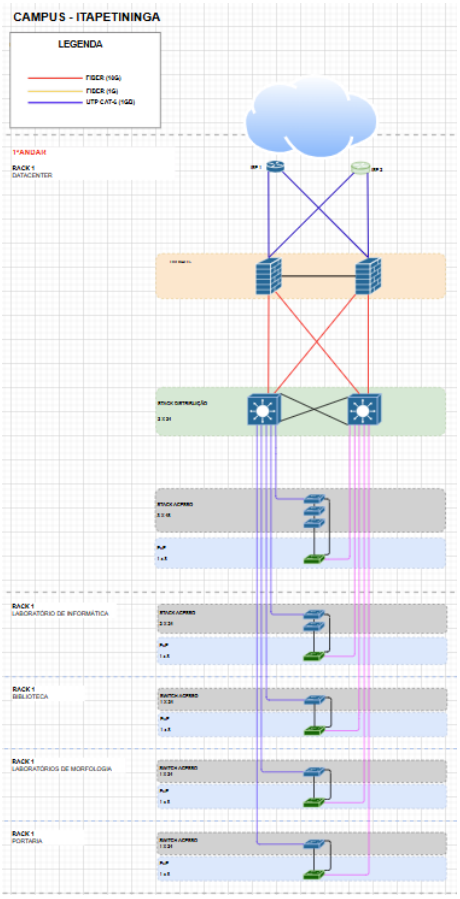


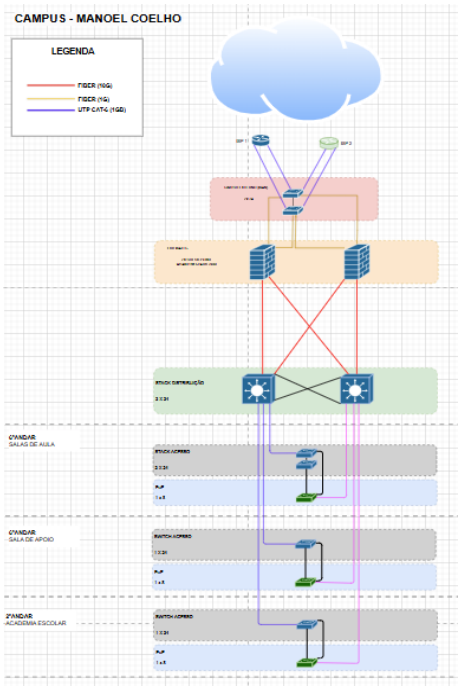

CAMPUS - CENTRO
LEGENDA
1º ANDAR
RACK 1
CPD
5º ANDAR
RACK 1
SALA DE APOIO
4º ANDAR
RACK 1
SALA DE APOIO
3º ANDAR
RACK 1
SALA DE APOIO
2º ANDAR
RACK 1
SALA DE APOIO


RACK 2
PÓS GRADUAÇÃO
RACK 3
EAD
1º ANDAR
RACK 2
SALA DE APOIO
RACK 3
LABORATÓRIO 112
RACK 4
LABORATÓRIO 116
TÉRREO
RACK 1
SALA TÉCNICA ELÉTRICA
RACK 2
DCE
RACK 3
FARMÁCIA ESCOLA
SUBSOLO
RACK 2
SUBSOLO


CAMPUS - CENTRO CPC
LEGENDA
1º ANDAR
TÉRREO


CAMPUS - CENTRO
Hospital Veterinário
LEGENDA
1º ANDAR
TÉRREO


CAMPUS - ITAPETININGA
LEGENDA
FIBER (10G)
FIBER (1G)
UTP CAT-6 (1GD)
1°ANDAR
RACK 1
DATACENTER
RACK 1
LABORATÓRIO DE INFORMÁTICA
RACK 1
BIBLIOTECA
RACK 1
LABORATÓRIOS DE MORFOLOGIA
RACK 1
PORTARIA


CAMPUS - MANOEL COELHO
LEGENDA
FIBER (10G)
FIBER (1G)
UTP CAT-6 (1GD)
0°ANDAR
SALAS DE AULA
0°ANDAR
SALA DE APOIO
2°ANDAR
ACADEMIA ESCOLAR

ANEXO XVI

MINUTA DE CONTRATO Nº ___/2026 E TERMO DE CONFIDENCIALIDADE E RESPONSABILIDADE DE PROTEÇÃO DE DADOS PESSOAIS QUE ENTRE SI CELEBRAM A "UNIVERSIDADE MUNICIPAL DE SÃO CAETANO DO SUL – USCS", E A EMPRESA " _____"

Aos _____ dias do mês de _____ do ano de 2026, a **Universidade Municipal de São Caetano do Sul - USCS**, por intermédio da Reitoria, inscrita no CNPJ sob nº 44.392.215/0001-70, sediada à Avenida Goiás, 3400, Bairro Barcelona - São Caetano do Sul - CEP 09550-051 – Estado de São Paulo, neste ato representada pelo Reitor o senhor _____, inscrito no Cadastro de Pessoa Física CPF, sob número 000.***.***-00, doravante denominada Contratante e, de outro lado, a empresa _____, inscrita no CNPJ sob nº _____, sediada à _____, nº _____ – Vila: _____ – _____ – CEP _____ – _____, neste ato representada na forma de seu contrato social, pelo _____, portador do Cadastro de Pessoa Física nº 000.***.***-00, doravante denominada Contratada, com fundamento na Lei Federal nº 14.133/2021, Lei Municipal nº 4660//2008, estando as partes vinculadas ao Processo de Compras 873/2025 Edital de Pregão Eletrônico nº 27/2025 e a proposta vencedora, assinam o presente contrato de fornecimento e serviços, obedecendo as seguintes disposições:

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. O presente instrumento contratual tem por objeto a contratação de empresa especializada para fornecer Solução de Serviço gerenciado para gestão de ativos de rede, monitoramento e segurança de rede WiFi, incluindo fornecimento de softwares, equipamentos e licenciamentos na modalidade *As a Service*, suporte técnico especializado, acessórios e garantia para atendimento da Universidade Municipal de São Caetano do Sul, conforme condições e especificações constantes no edital e seus anexos.

1.2. A solução gerenciada para gestão de ativos de rede WiFi deverá abranger o fornecimento da infraestrutura necessária, configuração, implantação, gerenciamento e monitoramento contínuo de switches, pontos de acesso WiFi e controladora com vistas a garantir alta disponibilidade, segurança e desempenho da infraestrutura de Tecnologia da Informação da Universidade USCS, levando-se em conta que o ambiente de WiFi deverá comportar o acesso simultâneo de 10.000 usuários

1.3. A Contratada ficará obrigada a aceitar, nas mesmas condições contratuais, acréscimos ou supressões que se fizerem necessários, até 25% (vinte e cinco) por cento do valor inicial atualizado do contrato.

CLÁUSULA SEGUNDA - DOS PRAZOS

2.1. A Contratada deverá cumprir os seguintes prazos para a perfeita execução do instrumento contratual:

2.1.1. A contratada deverá cumprir o prazo estipulado de até 45 dias para fornecimento dos equipamentos switch de acesso tipos 1, 2 e 3, bem como os equipamentos descritos como pontos de acesso tipos 1, 2, 3, 4 e 5, ambos *as a service*, contendo em todos os bens entregues na sede da Universidade USCS (Campus Barcelona ao gestor designado) a indicação de registro patrimonial da proponente Contratada, tomando-se por referência que o prazo de entrega será contado nos termos do subitem 12.2 do edital, cujo escopo remete às especificações contidas no termo de referência do edital;

2.1.2. Em relação a etapa de implementação que se ancora nas atividades de instalação, configuração e ativação física dos equipamentos, quantificados e especificados sob o crivo técnico no Termo de referência do edital, a Contratada terá prazo de até 45 dias para sua finalização, portanto, o proponente deverá considerar 90 dias como prazo máximo para a disponibilização completa da solução objeto do certame, incluindo-se nesse intervalo temporal os aspectos ligados à infraestrutura do projeto, contados nos termos do subitem 12.2. do instrumento convocatório;.

2.1.3. A empresa quando da entrega física dos equipamentos, deverá elaborar plano de implementação junto a Universidade USCS (cronograma), cujo documento deverá conter a distribuição dos equipamentos nas unidades que integrarão o projeto, obedecendo ao mapa que contém a localização de cada ponto de acesso e switch nas respectivas unidades (anexo III do contrato), topologia física e lógica, bem como o quadro de pessoal alocado na tarefa e os respectivos papeis assumidos por cda membro da equipe, aderente às exigências técnica/tecnológicas aportadas no Termo de Referência do Edital.

2.1.4. O cronograma de execução, deverá indicar de modo percentual a distribuição e execução dos serviços, considerando-se o dimensionamento e as respectivas unidades da Universidade USCS que integram o projeto, estabelecido no anexo I deste instrumento de contrato (item "**a**")

2.1.5. Caso a ordem de serviço seja enviada por correspondência eletrônica, o prazo para entrega dos equipamentos *as a service*, instalação e configuração da solução contratada, independente do recebimento, inicia-se 24 (vinte e quatro) horas após sua expedição, ressaltando-se que o prazo deve iniciar em dia útil.

2.1.6. **Quanto ao serviço mensal de solução de gerenciamento de ativos de rede, monitoramento e segurança que inclui o fornecimento de softwares, equipamentos de rede WiFi, licenciamentos, suporte técnico´especializado, acessórios e garantias.**

2.1.6.1. Concluído a fase de estruturação, que contempla a disponibilização física de equipamentos *as a service* e implementação da solução, com escopo definido a partir das especificações contidas no termo de referência do edital, o gestor do contrato designado pela USCS terá o prazo máximo de até 10(dez) dias para conferência, validação e emissão do **Termo de Aceitação**. A partir de então, terá início a prestação mensal dos serviços descritos acima, elencados sob a forma de solução integrada concernente ao objeto de contratação.

2.1.6.1.1. Em particular, no que concerne a entrega e implantação dos equipamentos *as a service*, bem como os serviços de instalação e configuração, dar-se-ão de modo parcial, de acordo com o cronograma a ser definido entre a Contratada e a Gestão do instrumento de contrato da Universidade USCS. Portanto, o **termo de aceitação** e consequentemente pagamento por essa etapa de infraestrutura será gradual, do mesmo modo, a ativação dos serviços decorrentes de tal implantação (suporte técnico, parametrização e monitoramento).

2.1.6.1.2. O cronograma de execução, deverá indicar de modo percentual a distribuição e execução dos serviços, considerando-se o dimensionamento e as respectivas unidades da Universidade USCS que integram o projeto, estabelecido no termo anexo I do instrumento de contrato (item "**a**").

2.1.6.2. Quanto ao início dos serviços de suporte técnico, serviços de monitoramento e segurança, serão computados para efeito de pagamento na data constante do termo de aceitação emitida pela gestão do instrumento de contrato da Universidade USCS, respeitando-se a condição (*pró-rata - no sentido de proporcionalidade*) disposta no subitem 12.3. e seguintes do instrumento convocatório, para o primeiro pagamento, caso não se inicie no primeiro dia do mês.

2.1.6.2.1. Para efeito de pagamento relativo aos serviços descritos no subitem imediatamente anterior, deverá ser considerado o escopo de fornecimento referente a soluçãode serviço proposta e contratada.

CLÁUSULA TERCEIRA – DA VIGÊNCIA DO CONTRATO

3.1. A Universidade Municipal de São Caetano do Sul firmará contrato para fornecer Solução de Serviço Gerenciado para Gestão de Ativos de rede WiFi, monitoramento e segurança, incluindo fornecimento de softwares, equipamentos, licenciamentos *as a Service*, bem como suporte técnico especializado e garantias, por prazo de 24 (vinte e quatro) meses consecutivos e ininterruptos, contados a partir do recebimento da ordem de serviços, conforme disposto no subitem 12.2. podendo ser prorrogado por igual período, de comum acordo, desde que devidamente justificado e manifestado com antecedência mínima de 60 (sessenta) dias antes do seu término, estendendo-se até o limite de 120 meses, nos termos do artigo 107, da Lei Federal 14.133/2021.

3.1.1. No caso de prorrogação será lavrado o Termo respectivo.

CLÁUSULA QUARTA – DAS RESPONSABILIDADES E OBRIGAÇÕES DA CONTRATADA

4.1. É de responsabilidade da Contratada executar o objeto do certame sob sua inteira responsabilidade, rigorosamente de acordo com as especificações contidas nos Anexos I, II e III do contrato. É salutar reafirmar que a Contratante não aceitará fornecimento de serviço ou equipamentos físicos ou ainda softwares e garantias, diferentes daqueles dispostos no Termo de Referência do edital 27/2025.

4.2. Manter durante a execução do contrato, em compatibilidade com as obrigações assumidas todas as condições de habilitação e qualificação exigidas no processo licitatório.

4.3. Responsabilizar pela pelo fornecimento dos bens e execução dos serviços objeto da licitação, cabendo ao seu representante na condição de preposto acompanhar o cumprimento rigoroso dos prazos, organização de reuniões, entrega de documentos, elaboração de relatórios de acompanhamento e quaisquer atividades pertinentes à execução dos serviços.

4.4. A Contratada deverá registrar as ocorrências havidas durante a execução do objeto dando ciência a Universidade Municipal de São Caetano do Sul, respondendo integralmente por sua omissão.

4.5. A Universidade USCS não assumirá nenhuma responsabilidade pelo pagamento de impostos e outros encargos que competirem à Contratada, nem se obrigará a fazer a essa qualquer restituição ou reembolso de quantias ou acessórios que a mesma despender com esses pagamentos.

4.6. A Contratada deverá prestar os serviços sempre por pessoal qualificado, respondendo perante a USCS e a terceiros por todos os ônus, encargos, perdas e/ou danos porventura resultantes da execução do objeto da prestação de serviços.

4.7. A contratada deverá providenciar e custear pessoal habilitado em quantidade necessária para a execução dos serviços até o cumprimento integral do contrato.

4.8. A contratada deverá providenciar e e custear os recursos computacionais (hardware, software e demais elementos de ordem computacional), quando couber, utilizados por sua equipe de suporte técnico, monitoramente e de segurança relacionado ao gerenciamento da solução de gestão de ativos de rede WIFi, no desempenho de suas funções exigidas via celebração deste contrato.

4.9. A Contratada deverá manter equipe de profissionais treinados nas melhores práticas e tecnologias existentes no mercado de cibersegurança.

4.10. Não reproduzir, divulgar ou utilizar em benefício próprio, ou de terceiros, quaisquer dados, imagens produzidas ou informação de que tenha tomado ciência em razão da execução dos serviços discriminados neste instrumento, sem o consentimento, prévio e formal da Contratante.

4.11. A contratada poderá realizar subcontratação parcial do objeto (atividades relacionadas tão somente a etapa de infraestrutura), desde que tal subcontratação não diga respeito à atividade fim do objeto do certame, conforme disposto no artigo 122 da Lei 14.133/2021, contudo, sua efetiva realização deverá ser devidamente justificada e precedida expressamente de autorização da Universidade Municipal de São Caetano do Sul.

4.11.1. A subcontratação dos serviços será de inteira responsabilidade da contratada e deverá seguir as condições e especificações delimitadas para o objeto no termo de referência deste edital. Para efeito da respectiva subcontratação, a licitante apresentará à administração documentação que comprove capacitação técnica do subcontratado, que deverá ser avaliada e acostada aos autos do processo.

CLÁUSULA QUINTA - DO VALOR E DOS RECURSOS

5.1. Tendo em vista o fornecimento da Solução de Serviço Gerenciado para Gestão de Ativos de rede WiFi, monitoramento e segurança, incluindo o aporte de softwares, equipamentos, licenciamentos *as a Service*, bem como suporte técnico especializado e garantias, por prazo de 24 (vinte e quatro) meses consecutivos e ininterruptos, e, de acordo com as especificações e condições contidas nos anexos I, II e III deste instrumento contratual a Universidade USCS pagará à Contratada o valor global de R$ _____ (_____).

5.2. As despesas onerarão a Classificação das despesas Orçamentárias, referenciada na dotação 12.364.1500.2.100.3.3.90.40.00, do orçamento da USCS, em conformidade com o disposto no parágrafo 1º do artigo 12 da Lei nº 10.320, de 16/12/1968.

CLÁUSULA SÉXTA – DO FATURAMENTO E DO PAGAMENTO

6.1. A Contratada quando do fornecimento dos equipamentos de switch de acesso e pontos de acesso *as a service* e controladora (*SaaS*), bem como execução dos serviços de instalação, configuração e ativação descritos no termo de referência do edital, deverá comunicar por escrito o evento e emitir a respectiva nota fiscal, encaminhando-a ao gestor/fiscalizador do contrato designado pela Universidade USCS para averiguação e emissão do respectivo termo de aceitação e liberação para posterior pagamento.

6.1.1. Os pagamentos serão efetuados à Contratada em parcela única, no prazo de até 10 (dez) dias úteis, contados do primeiro dia seguinte ao recebimento do Termo de Aceitação juntamente com a documentação fiscal completa (nota fiscal, fatura e demais documentos exigíveis), pelo setor de Contas a Pagar da Universidade USCS.

6.1.2. A emissão dos respectivos Termos de Aceitação, deverão ocorrer no prazo de até 05 dias, contados da comunicação formal da conclusão do fornecimento dos equipamentos e/ou dos serviços pela Contratada, devidamente atestados pelo gestor/fiscalizador do contrato.

6.2. Quanto ao Serviços de gerenciamento da solução para gestão de ativos de rede WiFi (mensal).

6.2.1. **Faturamento mensal**

6.2.1.1. A empresa Contratada emitirá nota fiscal mensal referente aos serviços de gerenciamento de solução para gestão de ativos de rede WiFi, monitoramento e segurança, incluindo fornecimento a*s a service* de software, licenciamentos, suporte técnico especializado, acessórioas e garantias para switchs e pontos de acesso, no último dia útil do mês de prestação desses serviços, encaminhando-a ao gestor/fiscalizador do contrato, que deverá, no máximo, no próximo dia útil efetuar a conferência, liberação e encaminhamento ao setor de contas a pagar da Universidade USCS.

6.2.1.2. O pagamento do serviço mensal será efetuado regularmente na 2ª(segunda) terça-feira do mês subsequente ao início dos serviços, desde que a nota fiscal e termo de liberação de pagamento emitido pelo gestor/fiscalizador do contrato seja encaminhado ao setor de contas a pagar da Contratante no prazo mencionado no subitem anterior.

6.2.1.2.1. Para efeito de pagamento no primeiro período (mês), considerando-se a aplicação do disposto no item 12.3 do instrumento convocatório, os serviços em referência, serão pagos de modo proporcional ao número de dias efetivos de sua prestação, coberta pelo contrato nesse interim.

6.2.1.3. A ordem de pagamento será emitida pela seção de contas a pagar da USCS, a favor da Contratada, em agência do Banco _____, número _____ e conta corrente _____, ficando terminantemente vedada a negociação da duplicata mercantil na rede bancária ou com terceiros.

Parágrafo Primeiro**:** Caso o término da contagem aconteça em dias sem expediente bancário, o pagamento ocorrerá no primeiro dia útil imediatamente subsequente.

Parágrafo Segundo**:** Havendo divergência ou erro na emissão da documentação fiscal, será interrompida a contagem do prazo para fins de pagamento, sendo iniciada nova contagem somente após a regularização da documentação fiscal.

Parágrafo Terceiro**:** A constatação de irregularidades na execução deste ajuste motivará o desconto da importância correspondente ao descumprimento, sem prejuízo da eventual rescisão e aplicação das penalidades fixadas na cláusula décima.

6.3. A Universidade Municipal de São Caetano do Sul, poderá exigir a comprovação de quitação das obrigações trabalhistas vencidas relativas ao contrato, de acordo com disposto no § 3º do artigo 121 da Lei 14.133/2021 como condição para liberação de pagamento.

6.4. Eventualmente, em caso de atraso pela USCS no pagamento pelos serviços executados, desde que a empresa contratada não tenha concorrido de alguma forma para tanto, o valor devido deverá ser acrescido de encargos moratórios proporcionais aos dias de atraso, apurados desde a data limite prevista para opagamento até a data do efetivo pagamento, à taxa de 6% (seis por cento) ao ano, aplicando-se a seguinte fórmula:

EM = I x N x VP

EM = Encargos Moratórios a serem acrescidos ao valor originalmente devido
I = Índice de atualização financeira, calculado segundo a fórmula:
I = (6 / 100) / 365

N = Número de dias entre a data limite prevista para o pagamento e a data do efetivo pagamento
VP = Valor atualizado da parcela em atraso de atraso

6.4.1. Em caso de atraso superior a 30 dias do vencimento, o valor principal será atualizado monetariamente pelo indicador de preços IPCA do último mês, anterior à data limite, divulgado pelo Instituto Brasileiro de Geografia e Estatística.

6.4.1.1. Para efeito de aplicação dos itens imediatamente acima, a empresa contratada deverá apresentar solicitação expressa e formal, ocasião em que se realizará a análise e negociação com a Universidade USCS.

CLÁUSULA SÉTIMA - DO REAJUSTE DE PREÇOS

7.1. Os valores constantes da proposta e expressos em reais para para fornecimento de solução de serviço gerenciado para gestão ativos de rede WiFi, monitoramento e segurança, incluindo fornecimento de softwares, equipamentos, licenciamentos *as a service*, bem como suporte técnico especializado, acessórios e garantias, descritos no anexo I deste instrumento de contrato, poderão sofrer reajustes somente após o interregno de 12 meses, contados a partir do prazo inscrito no subitem 2.1.6.2. deste documento.

7.2. Na hipótese de manutenção do contrato, transcorridos os primeiros 12 meses, conforme expresso no subitem 7.1., o valor mensal decorrente dos serviços descritos no anexo I deste contrato poderá ser reajustado a partir do 13º (décimo terceiro) mês, de acordo com a variação do Índice Nacional de Preços

ao Consumidor Amplo – IPCA/IBGE, em conformidade com a legislação em vigor ou por outro índice que venha substituí-lo.

7.3. O reajuste poderá ser concedido mediante expressa solicitação da Contratada, para análise e negociação com a USCS, e terá incidência de pagamento respeitando-se as condições e períodos estabelecidos no item 7.1.

CLÁUSULA OITAVA - DAS PENALIDADES

8.1. Comete infração administrativa, nos termos da Lei 14.133/2021, a proponente vencedora do certame e/ou contratada que der causa à inexecução parcial ou total do contrato; ensejar o retardamento da execução do instrumento; apresentar documentação ou praticar ato fraudulento durante a execução do contrato; comportar-se de modo inidôneo ou cometer fraude de qualquer natureza; praticar ato lesivo previsto no artigo 5º da Lei Federal 12.846/2013.

8.1.1. As empresas que cometerem as infrações dispostas no item 8.1, estarão sujeitas a aplicação de advertência, impedimento de licitar e contratar com a administração pública, ser declarada inidônea para licitar e contratar, além da aplicação de multas reparatórias e/ou moratórias, conforme o caso.

8.1.2. A aplicação das sanções previstas neste instrumento contratual não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Universidade USCS, bem como não impede essa administração de se utilizar cumulativamente da aplicação das sanções com as multas previstas.

8.2. A recusa injustificada da adjudicatária em aceitar ou retirar o termo de contrato, no prazo e nas condições estabelecidas caracterizará descumprimento total da obrigação assumida, sujeitando-o a juízo da Administração, nos termos da legislação, inclusive, municipal:

8.2.1. Ao pagamento de multa de 30% (trinta por cento) sobre o valor do contrato;

8.2.2. Ao pagamento correspondente à diferença de preço decorrente de nova licitação ou contratação, para o mesmo fim.

8.3. Pela inexecução total do contrato, será aplicada à Contratada a multa de 30% (trinta por cento) sobre o valor total do ajuste;

8.4. Pela inexecução parcial do contrato, será aplicada à Contratada a multa de 20% (vinte por cento) sobre o valor da obrigação não cumprida.

8.5. Pelo atraso injustificado a Contratada incorrerá em multa diária de 0,5% (cinco décimos por cento) sobre o valor do contrato, excluída, quando for o caso, a parcela correspondente aos impostos incidentes, quando destacados no documento fiscal, sendo que a aplicação da multa terá início no primeiro dia seguinte ao término do prazo contratual ou de execução do serviço.

8.5.1. Os atrasos injustificados superiores a 30 (trinta) dias corridos serão obrigatoriamente considerados inexecução total ou parcial, estando a Contratada sujeita as sanções previstas nos subitens 8.3 ou 8.4.

8.6. Além das multas e das penalidades aqui contidas, poderão ser aplicadas à Contratada, sanções decorrentes do não cumprimento das condições estabelecidas pelo ***Service Level Agreement*** que integra o Termo de Referência do edital, item 11 e seguintes, conforme verificação e enquadramento do Gestor do instrumento de contrato designado pela USCS.

8.7. As multas a que aludem os subitens anteriores não impedem que a Administração rescinda unilateralmente o contrato e aplique outras sanções previstas nas Leis Federais e Municipais, a saber:

8.7.1. Advertência, por escrito, no caso de pequenas irregularidades.

8.7.1.1. A sanção de advertência poderá ser aplicada nos seguintes casos:

I. Descumprimento das determinações necessárias à regularização das faltas ou defeitos observados na prestação dos serviços;

II. Outras ocorrências que possam acarretar transtornos no desenvolvimento dos serviços da Contratante, desde que não caiba a aplicação de sanção mais grave.

8.7.2. Suspensão temporária do direito de licitar e impedimento de contratar com a Administração, pelo prazo de até dois anos, quando da inexecução contratual sobrevier prejuízo para a Administração;

8.7.2.1. A penalidade de suspensão será cabível quando a Contratada participar do certame e for verificada a existência de fatos que o impeçam de contratar com a Administração Pública. Caberá ainda a suspensão quando a Contratada, por descumprimento de cláusula contratual tenha causado transtornos no desenvolvimento dos serviços da Contratante.

8.7.3. 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.

8.7.3.1. Se a Contratada deixar de entregar a documentação ou apresentá-la falsamente, ensejar 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 cinco anos, impedido de contratar com a Administração Pública, sem prejuízo das multas previstas neste contrato e das demais cominações legais.

8.7.4. Verificado que a obrigação foi cumprida com atraso injustificado caracterizando a inexecução parcial, a Universidade Municipal de São Caetano do Sul poderá reter preventivamente, o valor da multa dos eventuais créditos que a Contratada tenha direito, até a decisão definitiva, assegurada a ampla defesa.

8.7.4.1. Se a USCS decidir pela não aplicação da multa, o valor retido será devolvido à Contratada.

8.8. Os atos previstos como infrações administrativas na Lei Federal nº 14.133/2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei Federal 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei.

8.9. Independentemente das sanções retro, a Contratada ficará sujeita ainda, à composição das perdas e danos causados à Administração e decorrentes de sua inadimplência, bem como arcará com a correspondente diferença de preços verificada em nova contratação, na hipótese de os demais classificados não aceitarem a contratação pelos mesmos preços e prazos fixados pelo inadimplente.

8.10. A personalidade jurídica da empresa vencedora poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos no Edital ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com a empresa vencedora.

8.11. É assegurada nos termos legais, os prazos para exercício do direito da ampla defesa e do contraditório, na aplicação das sanções previstas no escopo dos artigos 155 a 162 da Lei 14.133/2021, conforme o caso.

CLÁUSULA NONA - DA RESCISÃO

9.1. A falta de cumprimento das obrigações assumidas no presente instrumento ou a incidência do comportamento descrito no artigo 137 da Lei nº 14.133/2021, dará direito à USCS de rescindir, unilateralmente este contrato, independentemente de interpelação judicial, sendo aplicáveis, ainda, as disposições contidas no artigo 139 da mesma legislação. A rescisão contratual dar-se-á ainda em decorrência da aplicação dos termos contidos no artigo 138 da NLLC.

CLÁUSULA DÉCIMA - DA GARANTIA CONTRATUAL

10.1. A contratada, em até 10(dez) dias úteis contados da assinatura do contrato, deverá fazer prova de recolhimento, a título de Garantia de Execução do Contrato, equivalente a 5% (cinco por cento) do valor total pactuado, com vencimento para 60 (sessenta) dias após a data da entrega final dos serviços, correspondente a data da última parcela a ser paga pela Universidade Municipal de São Caetano do Sul, cabendo à Contratada optar por quaisquer modalidades assecuratórias previstas no parágrafo 1º do artigo 96 da Lei Federal 14.133/2021.

10.2. A garantia quando prestada nas modalidades fiança bancária e seguro garantia, deverá prever a cobertura de indenizações decorrentes de responsabilização da **Tomadora** dos serviços por obrigações assumidas pela Contratada, inclusive às concernentes aos encargos trabalhistas, previdenciários, fiscais e comerciais, nos termos deste contrato.

10.3. Na hipótese de o contratado optar pela modalidade de garantia inscrita no inciso II do parágrafo 1º do artigo 96 (Lei 14.133/2021), o prazo para prestação de garantia será assegurado nos termos do § 3º do mesmo artigo da mesma Lei.

10.4. Na hipótese de evidenciar qualquer impropriedade ou incorporação, a Contratante exigirá sua regularização ou substituição no prazo de 5(cinco) dias úteis da data de intimação.

10.5. A falta de atendimento à convocação para regularização ou substituição da garantia na forma e prazo especificado no item 10.4 acima, sujeitará a Contratada às seguintes consequências:

10.5.1. Retenção dos pagamentos que lhe sejam devidos, para recomposição da garantia contratual, na modalidade caução em dinheiro; ou

10.5.2. Caracterização de inexecução contratual, ensejando a consequente aplicação de penalidade prevista na cláusula 8ª deste documento e, ainda, a rescisão do ajuste com fundamento nos incisos do artigo 155 da Lei Federal nº 14.133/2021.

10.6. Caberá a Contratante decidir motivadamente entre a retenção de pagamentos para recomposição da garantia contratual ou a caracterização da inexecução contratual.

10.7. A correção monetária da garantia prestada na forma de caução em dinheiro será calculada com base na variação do índice IPCA/IBGE e, no caso de utilização de cheque, a data inicial da correção será a do crédito bancário.

CLÁUSULA DÉCIMA PRIMEIRA - DA GESTÃO E FISCALIZAÇÃO DO CONTRATO

11.1. O agente público designado para assumir a função de Gestor do instrumento contratual resultante deste processo licitatório será o responsável pela Diretoria de Tecnologia da Informação e Inovação, cujas atribuições lhes permitirá ainda estabelecer o(s) fiscalizador(es) técnico(s). Os designados serão responsáveis pelo acompanhamento e execução do termo contratual objeto do presente certame, procedendo, de acordo com suas competências, ao registro das ocorrências e adotando as providências necessárias ao fiel cumprimento do ajuste, bem como, responsabilizar-se-ão pela vigência com o consequente controle dos prazos de início e término contratual, eventual prorrogação, aditamentos e instauração de novo processo de licitação quando couber.

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

11.3. O gestor do contrato deverá coordenar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da autorização de fornecimento/ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

11.4. O gestor deverá elaborar relatório final contendo informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades relativas à administração e execução contratual.

11.5. Os fiscais técnicos do contrato anotarão para efeito de histórico de gerenciamento, todas as ocorrências relacionadas à sua execução, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. Identificada quaisquer irregularidades, este emitirá notificação, indicando o prazo para correção em sua execução.

11.6. Os fiscais técnicos comunicarão ao gestor desse instrumento, em prazo não inferior a 60 (sessenta) dias do término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

11.7. O gestor tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido por comissão, ou, pelo departamento competente para tal, em conformidade ao disposto no artigo 158 da Lei 14.133/2021.

11.8. Não obstante ser a Contratada a única e exclusiva responsável, inclusive perante terceiros, pela execução do objeto do contrato, reserva-se à USCS o direito de, sem que de qualquer forma restrinja a plenitude da responsabilidade da Contratada, exercer a mais ampla fiscalização dos serviços.

CLÁUSULA DÉCIMA SEGUNDA – DO FORO

12.1. Fica eleito o Foro da Comarca de São Caetano do Sul, Estado de São Paulo, com expressa renúncia de qualquer outro, por mais privilegiado que seja, para toda e qualquer ação oriunda deste ajuste e que não possa ser resolvida de comum acordo entre as partes.

12.2. E, por estarem justas e contratadas, as partes assinam o presente contrato em 2(duas) vias de igual teor e forma, perante a presença de 2(duas) testemunhas.

São Caetano do Sul, ____ de _____ de 2026.

_____	_____
Universidade Municipal de São Caetano do Sul	Nome da empresa
Contratante	**Contratada**

Testemunhas

_____	_____
Nome	Nome
CPF 000.***.***-00	CPF 000.***.***-00

TERMO DE CONFIDENCIALIDADE E RESPONSABILIDADE DE PROTEÇÃO DE DADOS PESSOAIS

Pregão Eletrônico nº 27/2025
Processo de Compras nº 873/2025

_____(responsável ou representante legal da empresa), inscrito no CPF sob o nº _____, abaixo firmado, vinculado nestes termos ao Contrato nº _____/2026, no qual figura como Contratada a empresa _____, inscrita no CNPJ sob o nº _____, assumo o compromisso de manter confidencialidade e sigilo sobre todas as informações técnicas, bem como a responsabilidade e proteção dos dados pessoais na conformidade do disposto na Lei nº 13.709/2018 e suas alterações, como também a eventuais regulamentações relacionadas à Contratante, Universidade Municipal de São Caetano do Sul - USCS.

Comprometendo-me ainda, por este termo de confidencialidade e sigilo a não repassar o conhecimento das informações, responsabilizando-me pelos funcionários que vierem ter acesso às informações, obrigando a Contratada ao ressarcimento de quaisquer danos e/ou prejuízos oriundos de uma eventual quebra de sigilo ou confidencialidade das informações fornecidas.

Para os fins previstos neste termo e no Contrato, os termos a seguir serão interpretados conforme a legislação brasileira, notadamente Lei nº 13.709, de 14 de agosto de 2018 e alterações posteriores (a "Lei Geral de Proteção de Dados Pessoais" ou "LGPD"), com os seguintes significados:

- "**ANPD**" ou "**Autoridade Nacional de Proteção de Dados Pessoais**" é a autoridade regulatória máxima para dispor sobre assuntos de proteção de dados pessoais no Brasil.
- "Controladora" significa a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao Tratamento de Dados Pessoais, ou seja, nos moldes do presente Termo, a **USCS**.
- "**Dado Pessoal**" ou "**Dados Pessoais**" significa qualquer informação relacionada a pessoa natural identificada ou identificável, ou seja, que tenha o potencial de ser usada, de forma direta ou indireta, isoladamente ou em conjunto, para identificar uma pessoa natural.
- "**Dados Pessoais Sensíveis**" significa qualquer Dado Pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
- **"Legislação de Proteção de Dados"** significa qualquer legislação nacional, decretos, regulamentos, inclusive normas regulatórias emitidas pela ANPD, aplicável à proteção da privacidade e de Dados Pessoais no contexto do Tratamento de Dados Pessoais, incluindo, mas não se limitando à Lei Geral de Proteção de Dados Pessoais.
- **"Incidente de Segurança"** significa qualquer acesso não autorizado a Dados Pessoais e situações acidentais ou ilícitas de destruição, perda, alteração comunicação ou qualquer forma de Tratamento inadequado ou ilícito dos Dados Pessoais.
- **"Operadora"** significa a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de Dados Pessoais em nome da Contratante e em conformidade com suas instruções legais, ou seja, nos termos do Contrato.
- **"Titular de Dados Pessoais"** ou "**Titular"** significa a pessoa natural a quem se referem os Dados Pessoais que são objeto de Tratamento.
- **"Tratamento"** significa toda operação realizada com Dados Pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, transferência, difusão ou extração de dados.

1. Das Informações Tecnológicas e Confidenciais

Não disponibilizar as informações tecnológicas e confidenciais, que em razão do desempenho da prestação dos serviços objeto do Contrato nº ____/2026 tiver acesso, tais como códigos fontes dos softwares de propriedade da USCS, Sistema de Gestão Acadêmica, bem como informações de propriedade da USCS que eventualmente sejam acessadas pela Contratada na consecução do objeto,

inclusive informações de clientes internos e externos. As demais informações confidenciais, incluindo, dentre outras, todas e quaisquer informações orais e/ou escritas, transmitidas e/ou divulgadas pela Contratante serão confidenciais, restritas e de propriedade desta.

Informações confidenciais e tecnológicas devem significar, sem se limitar, toda e qualquer informação, de natureza técnica, operacional, comercial, jurídica, know-how, planos de negócios, métodos de contabilidade, técnicas e experiências acumuladas, documentos, contratos, papéis, estudos, pareceres, pesquisas, códigos fontes, transmitida pela Contratante à Contratada.

2. Do Uso

A Contratada concorda em usar as informações confidenciais e tecnológicas recebidas da empresa como propósito restrito de se fazer cumprir o estabelecido no Contrato.

3. Da não Divulgação

A Contratada ao receber a informação confidencial somente poderá usá-la para o propósito estabelecido no item 2 acima e zelará para que tais informações confidenciais e tecnológicas não sejam de qualquer forma divulgadas ou reveladas a terceiros, utilizando-se, no mínimo, do mesmo zelo e cuidado que dispensa às suas próprias informações confidenciais.

4. Das Cópias

A Contratada fica desde já proibida de produzir cópias ou back-up sem licença da empresa, por qualquer meio ou forma, de quaisquer documentos fornecidos ou que tenham chegado ao seu conhecimento em virtude do Contrato, além daquelas imprescindíveis ao desenvolvimento de seu trabalho, considerando que todas sejam informações confidenciais.

5. Da Propriedade

Toda informação confidencial e tecnológica permanecerá sendo de propriedade da parte que revelar a informação confidencial, somente podendo ser usada pela parte receptora para os fins de execução do Contrato. Tais informações confidenciais e tecnológicas, incluídas as cópias realizadas serão retomadas à parte reveladora ou então destruídas pela parte receptora, tão logo que tenha terminado o prazo do Contrato.

6. Da Proteção de Dados Pessoais

Cada Parte se compromete a cumprir com o disposto na Legislação de Proteção de Dados na execução do objeto do Contrato. A Contratada poderá realizar o Tratamento de todos os Dados Pessoais em nome da Contratante nos termos do contrato limitando o acesso aos Dados Pessoais que tratar em nome da Contratante a seus colaboradores que tenham necessidade de acesso a tais Dados Pessoais para executarem as suas funções, assegurando que tais colaboradores sejam treinados com relação às obrigações de confidencialidade previstas nesse Termo e no Contrato, e concordem em cumpri-las.

6.1. A Contratada tratará os Dados Pessoais com a finalidade exclusiva e estritamente necessária ao cumprimento do Contrato e de acordo com as instruções legais da Contratante. A Contratada não irá realizar o Tratamento de Dados Pessoais para qualquer outra finalidade não prevista no Contrato, a menos que seja autorizada previamente por escrito pelo(s) representante(s) legal(is) da Contratante.

6.2. A Contratada não poderá transferir quaisquer Dados Pessoais relacionados ao Contrato, inclusive no que concerne ao armazenamento de dados em nuvem, salvo se previamente autorizado, por escrito, pela Contratante.

6.3. Dentro do prazo de 15 (quinze) dias (a) após os Dados Pessoais não mais serem necessários para os propósitos do Contrato, ou (b) após o encerramento do prazo do Contrato, ou, ainda, (c) por qualquer razão, como a devolução ou migração dos Dados Pessoais a outra empresa, por decisão da Contratante, a Contratada deverá após, destruir todos os Dados Pessoais em sua posse ou controle em decorrência do Contrato. Não obstante o disposto acima, a Contratada poderá manter uma cópia dos Dados Pessoais necessários ao cumprimento do prazo previsto na legislação aplicável, devendo a Contratada, nesse caso, informar para a Contratante quais Dados Pessoais serão mantidos, o prazo de sua guarda e qual o fundamento legal que justifica essa retenção. Após o término do prazo legal, a Contratada deverá destruir imediatamente os referidos Dados Pessoais. Nessa hipótese, as obrigações relativas a Dados Pessoais previstas neste instrumento continuarão em vigor até que todos os referidos Dados Pessoais sejam destruídos.

6.4. Não obstante quaisquer obrigações previstas no Contrato estabelecendo padrões para sistemas, aplicações, arquivos de dados e outras ferramentas de tecnologia, a Contratada garante que adotou e implementou, e manterá durante o prazo do Contrato, as medidas organizacionais e técnicas de segurança para proteger os Dados Pessoais contra destruição indevida, compartilhamento irregular ou

não-autorizado, perda acidental, alteração, acesso ou divulgação irregulares e/ou qualquer forma de Tratamento inadequado ou ilícito dos Dados Pessoais. A adequabilidade dessas medidas será avaliada à luz das técnicas mais modernas, custo de implementação, natureza dos Dados Pessoais e risco aos quais os Dados Pessoais estejam expostos. Essas medidas serão pelo menos iguais ou superiores a, cumulativamente: (i) qualquer regulamentação definida pela ANPD ou outro órgão governamental competente; (ii) padrões do ramo da Contratante e (iii) medidas que a Contratada adotar para proteger outro Dado Pessoal em sua posse ou controle.

6.5. Imediatamente e nunca em prazo superior a 24 (vinte e quatro) horas após tomar ciência ou suspeitar razoavelmente de qualquer Incidente de Segurança que possa comprometer a integridade, confidencialidade e/ou disponibilidade de qualquer Dado Pessoal, a Contratada deverá notificar a Contratante, por escrito, sobre tal fato. Referida notificação deverá, no mínimo:

(a) descrever a natureza dos Dados Pessoais afetados, as categorias e o número de titulares dos Dados Pessoais em questão;

(b) fornecer informações sobre os titulares de Dados Pessoais envolvidos;

(c) informar as medidas técnicas e de segurança utilizadas para a proteção dos Dados Pessoais;

(d) comunicar o nome e os detalhes de contato do encarregado ou responsável por proteção de Dados Pessoais da Contratada;

(e) descrever as prováveis consequências e riscos relacionados ao Incidente de Segurança;

(f) descrever as medidas adotadas ou propostas a serem adotadas para solucionar o Incidente Segurança; e

(g) descrever as medidas que foram ou serão tomadas para reverter ou mitigar os efeitos das perdas relacionadas ao Incidente de Segurança.

6.6. A Contratada deverá cooperar com a Contratante e adotar as medidas razoáveis, conforme as instruções da Contratante para auxiliar na investigação, mitigação e correção de cada Incidente de Segurança, permitindo à Contratante (i) realizar uma investigação completa sobre o Incidente de Segurança, (ii) formular uma resposta correta e adotar medidas adicionais adequadas em relação ao Incidente de Segurança, a fim de atender a qualquer requisito da legislação aplicável.

6.7. As Partes concordam em coordenar e cooperar de boa-fé no desenvolvimento do conteúdo de quaisquer declarações públicas relacionadas ou de quaisquer avisos necessários para os Titulares afetados pelo Incidente de Segurança ou para a ANPD. A Contratada não deve informar terceiros sem antes obter o consentimento prévio, por escrito, da Contratante, a menos que seja exigida notificação pela legislação à qual a Contratada esteja sujeita. Nesse caso, a Contratada deverá, na máxima extensão permitida pela legislação aplicável, informar a Contratante sobre tal requisito legal, fornecer uma cópia da(s) notificação(ões) proposta(s) e considerar os comentários feitos pela Contratante, antes de notificar a quaisquer terceiros sobre o Incidente de Segurança.

> **6.7.1.** Se a Contratante incorrer em custos, diretos ou indiretos, em razão do Incidente de Segurança, incluindo investigar, remediar e mitigar o seu impacto, a Contratada concorda em reembolsar a Contratante dos respectivos custos. Mediante correção satisfatória do Incidente de Segurança, a Contratada concorda em tomar ações razoavelmente necessárias para evitar nova ocorrência e fornecerá declarações escritas para a Contratante sobre as medidas apropriadas que foram tomadas para proteger a Contratada contra a ameaça de uma ocorrência de fato similar.

6.8. A contratada notificará a contratante, imediatamente, sobre qualquer solicitação recebida de um titular cujos dados pessoais estejam sendo tratados pela contratada em razão do contrato. A contratada concorda em cumprir com todas as instruções razoáveis solicitadas pela contratante quanto à resposta a tal solicitação individual e a não responder a qualquer solicitação de titular de dados pessoais diretamente. Além disso, a contratada concorda em fornecer toda e qualquer assistência requerida pela contratante para responder, dentro do período exigido pela legislação de proteção de dados ou política da contratante, a qualquer solicitação individual recebida pela contratada ou pela contratante.

6.9. A Contratada concorda em responder total e em até 2 (dois) dias úteis a todos os questionamentos da Contratante relacionados ao Tratamento de Dados Pessoais relativos ao Contrato, e auxiliar a Contratante a responder total e prontamente aos questionamentos de qualquer autoridade competente relativos ao Tratamento de Dados Pessoais relacionado ao Contrato, incluindo a ANPD. A Contratada notificará a Contratante imediatamente de qualquer solicitação efetuada pela ANPD ou outra autoridade competente para divulgar Dados Pessoais que a Contratada trate em nome da Contratante, salvo se tal comunicação for proibida pela Legislação. Adicionalmente, a Contratada concorda em cooperar com a Contratante para responder ou objetar tal solicitação.

6.10. A Contratada concorda que, mediante requisição razoável da Contratante, disponibilizará suas instalações para auditoria de conformidade da Contratante em relação às obrigações deste Termo ou do Contrato, a ser realizada pela própria Contratante ou empresa designada pela Contratante. A Contratada deverá cooperar integral e satisfatoriamente com a referida auditoria. No caso dessa auditoria revelar falhas materiais ou fragilidades nos esforços de proteção de Dados Pessoais por parte da Contratada, a Contratante terá o direito de suspender ou terminar o Contrato, bem como a execução dos serviços que

acarretam o Tratamento de Dados Pessoais até que tais medidas sejam resolvidas adequadamente.

6.11. A Contratada defenderá, indenizará e manterá indene a Contratante de quaisquer demandas, exigências, despesas, danos, perdas, custos, taxas ou penalidades decorrentes do descumprimento da Contratada da Legislação de Proteção de Dados, bem como do Contrato. Não obstante qualquer previsão no Contrato em contrário, as obrigações de indenização estabelecidas neste item não estarão sujeitas a nenhuma limitação de responsabilidade da Contratada.

6.12. A Contratada declara e garante que:

(a) realizará Tratamento dos Dados Pessoais tão somente dentro dos limites e na medida em que for autorizado pela Contratada, conforme suas instruções explícitas;

(b) caso a Contratada perceba que será incapaz de cumprir com os requisitos exigidos pela Legislação de Proteção da Dados, comunicará tal fato imediatamente e por escrito à Contratante, que poderá, a seu único e exclusivo critério, suspender a transferência de Dados Pessoais ou rescindir o Contrato;

(c) irá realizar a criptografia de quaisquer Dados Pessoais Sensíveis armazenados em aparelhos portáteis, bem como de todo Dado Pessoal solicitado pela Contratante, dentro do que lhe for razoavelmente exigido;

(d) não tem conhecimento de nenhum Incidente de Segurança nos últimos 5 (cinco) anos que possa afetar o Contrato ou a outra Parte; e

(e) encontra-se plenamente capaz de cumprir com os termos e condições do presente Termo, do Contrato e da Legislação de Proteção de Dados e que, no evento de uma relevante alteração das normas aplicáveis às atividades de Tratamento de Dados Pessoais que tenha potencial de modificar sua conformidade legal e contratual, notificará a Contratante imediatamente; e

(f) implementou todas as medidas organizacionais e técnicas de segurança exigidas nos termos do Contrato da Legislação de Proteção de Dados.

7. Da Responsabilidade

A Contratada se obriga a não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações confidenciais para nenhuma pessoa, física ou jurídica e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objeto referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o seu uso indevido por qualquer pessoa que, por qualquer razão tenha tido acesso a elas.

Restituir imediatamente o documento ou outro suporte que contiver informações sigilosas à parte reveladora, sempre que esta as solicitar ou sempre que as informações deixarem de ser necessárias e, não guardar para si, em nenhuma hipótese, cópia, reprodução ou segunda via das mesmas.

8. Da violação

A Contratada que recebe e tem conhecimento de informação confidencial, reconhece e aceita que, na hipótese de violação de quaisquer das cláusulas deste Termo, estará sujeito as sanções e penalidades legais conforme as Leis 9.609/1998 e 14.133/2021, sem prejuízo das perdas e danos que der causa, inclusive as de ordem moral ou concorrencial, bem como as de responsabilidades civis e criminais respectivas.

9. Do Prazo

A vigência da obrigação de confidencialidade, sigilo, proteção e responsabilidade pelos Dados Pessoais assumida pela minha pessoa por meio deste Termo e, por conseguinte a empresa denominada Contratada terá validade pelo tempo que perdurar o Contrato e disponibilização de informações por parte da Contratante.

São Caetano do Sul, ____ de _____de 2026.

_____

Nome e assinatura do responsável pelo contrato

Testemunhas

_____

Nome

CPF 000.***.***-00

_____

Nome

CPF 000.***.***-00

ANEXO I do Instrumento Contratual nº ____/2026
Processo de Compras nº873/2025

OBJETIVO

O presente documento, transcrito a partir do termo de referência do edital, teve como objetivo a contratação de empresa especializada para fornecr solução de serviço gerenciado para gestão ativos de rede WiFi, monitoramento e segurança, incluindo fornecimento de softwares, equipamentos e licenciamentos na modalidade *As a Service*, suporte técnico especializado, acessórios e garantia para atendimento da Universidade Municipal de São Caetano do Sul da Universidade Municipal de São Caetano do Sul, considerando o acesso simultâneo de 10.000 usuários conectados à rede WiFi, conforme especificações e condições contidas no edital de número 27/2025.

A solução é destinada ao atendimento dos colaboradores, discentes e docentes, bem como toda comunidade que utiliza os serviços da USCS, e deverá ser implementada nas seguintes unidades:

a) Unidades da Universidade USCS que integram o projeto:

1. Unidade Campus Barcelona: Avenida Goiás, 3400, Barcelona, São Caetano do Sul/SP, CEP 09550-051
2. Unidade Campus Centro: Rua Santo Antônio, 50, Centro, São Caetano do Sul/SP, CEP 09521-160
3. Unidade Campus Centro II: Rua Samuel Klein, 83, Centro, São Caetano do Sul, CEP 09510-125
4. Unidade Campus Conceição: Rua Conceição, 321, Santo Antônio, São Caetano do Sul, CEP 09530-060
5. Unidade Campus Itapetininga: Avenida Doutor Ciro Albuquerque, 4750 - Taboãozinho, Itapetininga/SP, CEP 18200-021

PARÂMETROS GERAIS, DESCRIÇÃO DA SOLUÇÃO E REQUESITOS DA CONTRATAÇÃO

A contratação em tela tem objetivo de atualizar o parque tecnológico da USCS, tornando compatível com a atual necessidade da Instituição, notadamente em relação ao atendimento qualificado aos seus usuários. A Universidade USCS, encontra-se em plena expansão de acordo com seu Planejamento Estratégico, tendo em registrado expressivo crescimento em sua estrutura física e sua capacidade de atendimento a comunidade. Desta forma, essa contratação é primordial para que a Universidade possa gerir e sustentar seus serviços que demandem conectividade. Neste sentido, há a necessidade de manter e racionalizar a infraestrutura de rede adequada, com a devida capacidade e com serviços de garantia e suporte técnico vigentes, suportando a atual demanda e sua projeção de crescimento futuro.

A solução prevê a disponibilização de equipamentos e tecnologias de última geração, conforme requisitos e quantitativos a seguir apresentados, devendo todos serem licenciados de modo a garantir o seu funcionamento adequado, bem como a segurança das aplicações da USCS e o suporte contínuo.

A solução está composta em diferentes itens e subitens, agrupados em um lote único. A composição em lote único atende melhor aos interesses da Universidade, a medida em que assegura maior interoperabilidade entre os equipamentos e consequentemente uma melhor gestão dos ativos e do próprio contrato.

No escopo desse projeto, essa administração tem a pretensão de contratar no mercado empresa com expertise para fornecer solução de serviço gerenciado de ativos de rede WiFi, baseada em equipamentos licenciados de switch e ponto de acesso *as a service*, integrada a prestação de serviços de suporte técnico especializado no formato 24x7, segurança e monitoramento, por período de 24 meses.

Considerando-se as particularidades inerentes ao processo de contratação de serviços tecnológicos, será necessário estabelecer reunião inicial de projeto (*kickoff*) tão logo seja celebrado o instrumento de contrato resultante desse processo de compras. Após envio da ordem de serviços, essa administração agendará a reunião, onde será discutido os aspectos relativos ao cronograma de execução dos serviços contratados, em particular, questões relacionadas a etapa de implementação da solução.

Deverão ser apresentados durante a fase de julgamento da proposta, a documentação oficial (quickspec ou datasheet) contendo as especificações técnicas dos equipamentos *as a service*, licenciamento e serviços que compõem a solução ofertada, inclusive no que se refere as certificações e homologações necessárias à consecução do projeto e demais itens que compõe a solução, para permitir a consistente avaliação de todos os itens ofertados.

A solução deve contemplar o serviço técnico especializado e monitoramento da infraestrutura de tecnologia, para atender o seguinte escopo:

O serviço de suporte operacional especializado deverá ser disponibilizado para apoiar as necessidades oriundas dos objetos dos itens deste documento, podendo ser realizado de forma presencial e/ou remota e deverá ter as seguintes características:

- Trabalhar em estreita colaboração com Diretoria de Tecnologia da Informação e Inovação, como equipes de suporte técnico, analistas de rede e equipes de segurança cibernética, para resolver problemas complexos, implementar mudanças e melhorias na infraestrutura de rede da Universidade;
- Acompanhar o monitoramento de rede e da controladora, receber alertas e notificações de problemas de rede, como interrupções de serviço e quedas de conexão. Investigar e resolver esses alertas/notificações, garantindo o mínimo de tempo de inatividade e impacto nos serviços;
- Realizar verificações regulares de rotina, atualizações de firmware, instalação de patches de segurança e outras atividades para manter a rede em bom estado de funcionamento;
- Avaliar novas funcionalidades e sugerir ajustes que possam melhorar a eficiência e a segurança da rede;
- Realizar novas instalações, configurações, suporte técnico, manutenções preventivas e corretivas dos equipamentos e softwares (switches, ponto de acesso Wi-Fi e controladoras);
- Reportar e elaborar notas técnicas sobre problemas graves para a Diretoria de Tecnologia da Informação e Inovação quando solicitado;

- Criação e acompanhamento no preenchimento de Requisição de Mudança (RDM) na infraestrutura de rede, segundo os procedimentos de gerenciamento de mudanças estabelecidos pela USCS. Isso envolve a análise de impacto, planejamento, execução e documentação das alterações realizadas;
- Monitorar e garantir que os NMS (Níveis Mínimos de Serviços) sejam cumpridos;
- Colaborar com equipes de projeto para implementar novas soluções de rede, como expansões, migrações ou atualizações tecnológicas de acordo com as demandas da USCS.

Necessidades de Negócio

- Continuidade dos serviços de TIC: Prover o aporte tecnológico necessário, para a implantação e a sustentação dos sistemas Institucionais, em consonância com a arquitetura tecnológica computacional.
- Conformidade: Alinhamento às boas práticas e condições de mercado para assegurar um ambiente tecnológico compatível.
- Manutenção e sustentabilidade: Prover e atualizar continuamente os recursos e ferramentas de Tecnologia da Informação.
- Garantia e suporte: Manter o parque atualizado com garantia e suporte às aplicações
- Segurança e privacidade: Prover mecanismos de segurança, compatível com a camada em que esses equipamentos se enquadram, visando a conferir confidencialidade, integridade e disponibilidade dos dados trafegados nos equipamentos de tecnologia.
- A Contratada deverá declarar que possui certificados do fabricante, comprovando que os produtos possuem a garantia solicitada neste termo de referência.

Necessidades Tecnológicas - Governança

- Alta disponibilidade: Fornecimento de infraestrutura tecnológica com certa redundância de ativos computacionais, constituindo serviços/sistemas mais resilientes e tolerantes a determinadas falhas em equipamentos e componentes de tecnologia da informação.
- Mitigação de riscos relativos à mudança e migração: Capacidade de migração das cargas de processamento da infraestrutura atual para a nova com riscos mitigados quanto à continuidade das operações e disponibilidade.
- Gerenciamento e monitoração: Capacidade de acompanhar, metrificar e realizar atividades em ativos e componentes computacionais por meio de interfaces de gerenciamento, que permitam o monitoramento o uso e a capacidade disponível de tais equipamentos.
- Escalabilidade e flexibilidade: Capacidade da solução ser adaptável, fornecendo infraestrutura para que os sistemas/serviços abrigados consigam ser expandidos, visando a atender, da melhor forma, às necessidades organizacionais.
- Auditoria e controle: Fornecer maneiras de controle e auditoria, compatível com a camada em que esses equipamento0s de tecnologia da informação se enquadram, visando a propiciar registros de acessos, definir papéis e suas respectivos privilégios e demais funcionalidades empregadas para se permitir o rastreio e controle de usuários.
- Atualização tecnológica: Capacidade de oferecer o aporte tecnológico necessário para a implantação de novos serviços, em consonância com as novas tecnologias disponíveis no mercado.

NecessidadesTtecnológicas - Requisitos técnicos esperados

- As especificações técnicas mínimas apuradas para o atendimento às necessidades do projeto, encontram-se descritas no tópico “Especificações Técnicas Mínimas da Solução”.
- O proponente deve declarar que é parceiro oficial ou que é revendedor autorizado pelo fabricante do equipamento ofertado.

TIPOLOGIA ACERCA DAS ESPECIFICAÇÕES E EXIGÊNCIAS APLICADAS AO PROJETO

A empresa a ser contratada será responsável pela aquisição, entrega, implementação (instalação e configuração) e licenciamento de todos os equipamentos *as a service* necessários e descritos no quadro a seguir desse documento. Ressalte-se que a Universidade Municipal de São Caetano do Sul, no âmbito desta contratação, não aceitará a entrega de hardwares e/ou softwares que não contemplem plenamente as especificações elencadas neste termo de referência.

Todos os equipamentos deverão ser entregues ao gestor designado para acompanhamento do contrato de prestação de serviço resultante desse processo licitatório, na sede da Universidade USCS, Campus Barcelona.

Item	Descrição	Qtde de Equipamento	Métrica	Quantidade
1	**Serviço gerenciado de solução para gestão ativos de rede, monitoramento e segurança, incluindo fornecimento de softwares, equipamentos, licenciamentos, suporte técnico especializado, acessórios e garantia.**			
1.1	**Serviço gerenciado de Switch, incluindo fornecimento de equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.**			
1.1.1	Switch de acesso tipo 1, *As a Service*, incluindo equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.	28	Meses	24
1.1.2	Switch de acesso tipo 2, *As a Service*, incluindo equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.	2	Meses	24
1.1.3	Switch de acesso tipo 3, *As a Service*, incluindo equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.	2	Meses	24
1.1.4	Implementação – instalação e configuração física da solução de Switch.	32	Serviço	1
1.2	**Serviço gerenciado de Ponto de Acesso (AP), incluindo fornecimento de equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.**			

1.2.1	Ponto de acesso tipo 1, *As a Service*, incluindo fornecimento de equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.	185	Meses	24
1.2.2	Ponto de acesso tipo 2, *As a Service*, incluindo fornecimento de equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.	12	Meses	24
1.2.3	Ponto de acesso tipo 3, *As a Service*, incluindo fornecimento de equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.	12	Meses	24
1.2.4	Ponto de acesso tipo 4, *As a Service*, incluindo fornecimento de equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.	6	Meses	24
1.2.5	Ponto de acesso tipo 5, *As a Service*, incluindo fornecimento de equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.	4	Meses	24
1.2.6	Implementação – instalação e configuração física da solução de Ponto de Acesso.	219	Serviço	1
1.3	**Serviço gerenciado de solução para gestão de ativos de rede, monitoramento e segurança, incluindo fornecimento de softwares, controladora (SaaS), licenciamento e suporte técnico especializado, acessórios e garantia.**			
1.3.1	Solução para gestão de switches, monitoramento e segurança, incluindo fornecimento de softwares, licenciamento e suporte técnico especializado.	1	Meses	24
1.3.2	Solução para gestão de pontos de acesso, monitoramento e segurança, incluindo fornecimento de softwares, controladora (SaaS), licenciamento e suporte técnico especializado.	1	Meses	24
1.3.3	Instalação, configuração e parametrização da solução para gerenciamento e gestão do parque de ativos de switches e pontos de acessos (251 equipamentos).	251	Serviço	1

Quadroa 01

1. CARACTERISTICAS GERAIS

1.1. As licenças a serem fornecidas para a implementação da solução, deverão estar em nome da USCS, e deverá estar vigente durante todo o período contratual.

1.2. O equipamento deve ser novo, sem uso anterior e o modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação na data de entrega da proposta.

1.3. Deve ser fornecida a versão mais recente (última versão comercial disponível) dos softwares, plataformas, sistemas operacionais e firmwares instalados.

1.4. Os requisitos técnicos devem ser sempre de fornecimento obrigatório, o proponente deverá comprovar através de documentos oficiais do fabricante.

1.5. O licenciamento deve ser unitário, por ativo gerenciado, suportando switches e pontos de acesso WiFi.

1.6. A contratada deverá fornecer todos os acessórios necessários para implantação e funcionamento do serviço contratado.

1.7. Todas as funcionalidades requisitadas nas especificações da solução, incluindo relatórios e informações analíticas, devem estar contempladas nas licenças.

2. **SWITCHES COORPORATIVOS - REQUISITOS GERAIS PARA SWITCHES TIPOS 1, 2, e 3:**

2.1. Todos os Switches especificados no presente documento devem ser do mesmo fabricante, compondo uma solução única de rede, para assegurar a compatibilidade funcional de todos os recursos e permitir o gerenciamento unificado.

2.2. Todos os acessórios que serão utilizados na prestação do serviço, tais como cabos de força (padrão ABNT NBR 14136) e cabos de interconexões (DAC/AOC/FIBRAS e etc), assim como transceivers e conversores de mídia deverão estar inclusos na solução.

2.2.1. A contratada a seu critério poderá prover protetores elétricos tais como mecanismos, acessórios e/ou equipamentos de proteção contra quedas, interrupções e distúrbios elétricos, para provimento e continuidade dos serviços do objeto do Anexo I – Termo de Referência.

2.3. O modelo do equipamento ofertado deve possuir, na data da entrega da proposta, homologação junto à ANATEL com certificado disponível publicamente no endereço eletrônico desta agência reguladora, conforme a Resolução número 242 de 30 de novembro de 2000.

2.4. Esses switches deverão possuir a mesma gerência dos pontos de acesso wifi de maneira centralizada, em ambiente de nuvem como serviço (**SaaS**).

2.5. O equipamento deve possuir dimensão adequada para instalação em rack padrão EIA 19 polegadas e ter altura máxima de 1U (uma unidade de altura de rack).

2.6. SWITCH DE ACESSO - TIPO 1

2.7. FUNCIONALIDADES GERAIS DOS SWITCHES TIPOS 1:

2.7.1. ESPECIFICAÇÕES GERAIS

2.7.1.1. Deve possuir altura máxima 1 (um) rack unit (RU);

2.7.1.2. Deve possuir fonte de alimentação interna, do tipo auto-sense, para operar de 100 a 240 VAC;

2.7.1.3. Deve possuir 8 (oito) portas 10/100/1000 Mbps, usando conectores RJ-45;

2.7.1.4. As portas 10/100/1000 BASE-T devem ser do tipo MDI/MDIX automático;

2.7.1.5. Deve possuir, no mínimo, 2 (duas) portas 1 Gbps SFP, as quais não devem operar em modo “combo” com as portas 10/100/1000 BASE-T em par trançado;

2.7.1.6. Deve possuir capacidade de processamento igual ou superior a 42 (quarenta e dois) Mpps;

2.7.1.7. Deve possuir capacidade de switching igual ou superior a 56 (cinquenta e seis) Gbps;

2.7.1.8. Deve possuir, pelo menos, 4 MB de buffers de pacotes;

2.7.1.9. Deve possuir, pelo menos, 2 GB de memória DRAM;

2.7.1.10. Deve possuir, pelo menos, 8 GB de memória NVRAM;

2.7.1.11. Deve ser do tipo compacto e fanless;

2.7.1.12. Deve implementar os protocolos IEEE 802.3af Power over Ethernet (PoE) e IEEE 802.3at Power over Ethernet Plus (PoE+);

2.7.1.13. Deve possuir PoE power budget de pelo menos 124 (cento e vinte e quatro) watts;

2.7.1.14. Deve possuir porta de console para gerenciamento utilizando conector RJ-45 ou USB Tipo C;

2.7.1.15. Deve possuir LEDs indicativos de energização, atividade do link e velocidade das portas;

2.7.1.16. Deve permitir identificar através de sinalização visual onde o switch está localizado no rack através de comandos para ligar e desligar os LEDs do equipamento;

2.7.1.17. Deve possuir botão de reset para voltar para configuração default de fábrica;

2.7.1.18. Deve implementar o padrão IEE 802.3az (Energy-Efficient Ethernet);

2.7.1.19. Deve possuir certificado de homologação junto à ANATEL de acordo a resolução 242 com documentos disponíveis publicamente no sítio público dessa agência na Internet;

2.7.2. Funções de camada 2

2.7.2.1. Deve possuir capacidade de no mínimo 32.000 (trinta e dois mil) endereços MAC;

2.7.2.2. Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad. Deve permitir a configuração de pelo menos 128 grupos de LACP com pelo menos 8 (oito) portas dentro de um mesmo grupo;

2.7.2.3. Deve implementar o protocolo IEEE 802.1Q para criação de pelo menos 4000 (quatro mil) vlans ativas;

2.7.2.4. Deve implementar o protocolo IEEE 802.1s (Multiple Spanning Tree), IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1D (MAC Bridging, Spanning Tree);

2.7.2.5. Deve ser compatível com o protocolo PVST / PVST+ e PRST;

2.7.2.6. Deve permitir a configuração de pelo menos 250 (duzentas e cinquenta) instâncias de Spanning Tree;

2.7.2.7. Deve implementar BPDU Guard e Root Guard;

2.7.2.8. Deve permitir a configuração de VLANs “trunking” de acordo com o protocolo 802.1Q e VLANs nativas (sem tag) simultaneamente na mesma porta;

2.7.2.9. Deve permitir a criação VLANs privadas;

2.7.2.10. Deve permitir a configuração de VLAN Q-in-Q Tagging de acordo com o padrão IEEE802.1ad ou IEEE802.1QinQ;

2.7.2.11. Deve implementar selective QinQ;

2.7.2.12. Deve implementar para o protocolo UDLD (Uni-Directional Link Detection) ou DLDP (Device Link Detection Protocol) ou similar;

2.7.2.13. Deve implementar jumbo frames até 9000 bytes nas portas Gigabit Ethernet;

2.7.2.14. Deve implementar mecanismos para controle do tráfego broadcasts, multicast e unknown unicast;

2.7.2.15. Deve implementar mecanismo de detecção ativa de loops através do envio frames de detecção. Na detecção de um evento de loop, deve ser capaz de realizar o bloqueio da porta (port shutdown);

2.7.2.16. Deve permitir a configuração de endereços MAC unicast e multicast estáticos em múltiplas portas ethernet simultaneamente, para permitir a configuração de “clusters” de firewalls;

2.7.2.17. Deve implementar IGMP Snooping para IGMPv1, IGMPv2 e IGMPv3;

2.7.2.18. Deve implmenetar MLD snooping v1 e v2;

2.7.2.19. Deve implementar protocolo de proteção de topologia em anel;

2.7.2.20. Deve possuir DHCP Server para IPv4 e IPv6;

2.7.3. Qualidade de Serviço

2.7.3.1. Deve permitir priorização de tráfego usando 8 (oito) filas de priorização por porta;

2.7.3.2. Deve permitir priorização de tráfego baseado no padrão IEEE 802.1p e no campo DSCP do protocolo Diffserv;

2.7.3.3. Deve implementar pelos menos os seguintes métodos para configuração das filas de priorização: ponderada, prioridade estrita e ambas combinadas;

2.7.3.4. Implementar priorização de tráfego baseado em porta física, protocolo IEEE 802.1p, endereços IP de origem e destino e portas TCP/UDP de origem e destino;

2.7.3.5. Deve permitir a configuração de Rate Limiting de entrada;

2.7.3.6. Deve permitir a configuração de Rate Shaping de saída;

2.7.3.7. Deve implementar os seguintes algoritmos de fila: Strict Priority e Round Robin com distribuição de pesos WRR (Weighted Round Robin) e uma combinação entre os dois métodos SP e WRR;

2.7.4. Segurança

2.7.4.1. Deve permitir autenticação de usuários usando o padrão IEEE 802.1x, permitindo associação dinâmica de VLANs e ACLs usando profiles definidas por um servidor RADIUS externo;

2.7.4.2. Deve permitir a associação de VLANs restritas para usuários que falhem durante a autenticação 802.1X;

2.7.4.3. Implementar método de autenticação baseado em endereço MAC para os dispositivos que não possuírem suplicantes 802.1X;

2.7.4.4. Deve possuir capacidade de autenticação 802.1x com atribuição de VLAN, regras de acesso de segurança e QoS individuais para, no mínimo, 02 (dois) dispositivos (Ex.: Telefone IP e PC) conectados em uma única porta e usando VLANs distintas;

2.7.4.5. Deve permitir, no mínimo e em cada porta, os seguintes tipos de autenticação usando VLANs distintas:

2.7.4.5.1. 2 (dois) dispositivos que suportam o padrão IEEE 802.1x;

2.7.4.5.2. 2 (dois) dispositivos MAC que não suportam o padrão IEEE 802.1x;

2.7.4.5.3. 1 (um) dispositivo que suporta o padrão IEEE 802.1x e 1 (um) dispositivo MAC que não suporta o padrão IEEE 802.1x;

2.7.4.6. O equipamento deve permitir a configuração de reautenticação 802.1x periódica;

2.7.4.7. O equipamento ofertado deve permitir a autenticação via Web Authentication para usuários que não possuem 802.1x;

2.7.4.8. Deve implementar "Change of Authorization" de acordo com a RFC 5176;

2.7.4.9. Deve permitir a autenticação de usuários para acesso às funções de gerenciamento usando-se os protocolos RADIUS, TACACS ou TACACS+;

2.7.4.10. Deve permitir a criação de ACLs para a filtragem de tráfego IPv4 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, bits do protocolo 802.1p e campo DSCP do protocolo Diffserv;

2.7.4.11. Deve permitir a criação de ACLs para a filtragem de tráfego IPv6 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, campo PCP do protocolo 802.1p e campo DSCP do protocolo Diffserv;

2.7.4.12. Deve implementar ACLs de entrada e ACLs de saída para IPv4;

2.7.4.13. Deve implementar ACLs de entrada e ACLs de saída para IPv6;

2.7.4.14. Permitir a filtragem do tráfego através de pelo menos 500 (quinhentas) regras de ACL (Access Control List);

2.7.4.15. Deve implementar segurança de acesso baseada em endereços MAC de origem, com a possibilidade de bloqueio permanente ou temporário das portas onde for detectada uma violação de segurança;

2.7.4.16. Deve permitir a criação de filtros de endereço MAC de origem e destino;

2.7.4.17. Deve possuir protocolos para proteção de ataques de Denial of Service;

2.7.4.18. Deve possuir funcionalidade de proteção contra servidores DHCP não autorizados DHCPv4 snooping e DHCPv6 snooping;

2.7.4.19. Deve possuir funcionalidade de proteção contra-ataques do tipo "ARP Poisoning";

2.7.4.20. Deve implementar IP Source Guard em IPv4 e IPv6;

2.7.4.21. Deve implementar proteção contra-ataques do tipo TCP SYN e ataques do tipo Smurf;

2.7.4.22. Deve permitir o monitoramento da movimentação de um endereço MAC de uma porta para outra, facilitando a distinção entre um movimento legítimo com um movimento malicioso de um ataque de MAC spoofing;

2.7.4.23. Deve implementar RADsec conforme RFC6614;

2.7.5. Gerenciamento

2.7.5.1. Deve permitir monitoração e configuração usando SNMP v1, v2 e v3;

2.7.5.2. Deve permitir o gerenciamento via SNMPv3 com as seguintes opções: sem autenticação e sem privacidade, com autenticação e sem privacidade e com autenticação e com privacidade;

2.7.5.3. Deve ser possível enviar "traps" e realizar o gerenciamento via SNMP através das redes IPv4 e IPv6;

2.7.5.4. Deve permitir a configuração de porta para espelhamento de tráfego, para a coleta de pacotes em analisadores de protocolo ou detecção de intrusão;

2.7.5.5. Deve permitir espelhamento de tráfego baseado em Porta, VLAN, Filtro MAC e ACL;

2.7.5.6. Deve permitir a configuração de porta para espelhamento de tráfego para uma porta em um switch remoto;

2.7.5.7. Deve implementar gerenciamento usando SSH v2 utilizando os algoritmos de criptografia 3DES e AES. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

2.7.5.8. Deve implementar gerenciamento via Telnet. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

2.7.5.9. Deve implementar pelo menos 4 (quatro) grupos de RMON;

2.7.5.10. Deve permitir o monitoramento dos transceivers óticos, retornando informação de temperatura, potência de transmissão (dBm), potência de recepção (dBm) e status;

2.7.5.11. Deve implementar funcionalidade de diagnóstico do cabo de par trançado, retornando informação de comprimento do cabo, status do link;

2.7.5.12. Deve permitir a atualização de arquivos de configuração e imagens de firmware usando TFTP ou FTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

2.7.5.13. Deve permitir a atualização de imagens de firmware dos equipamentos de uma pilha sem a necessidade de reinicialização simultânea de todos os equipamentos da pilha, permitindo a continuidade do tráfego de dados durante o processo de atualização;

2.7.5.14. Deve permitir configuração automática do seu próprio endereço IP e a seguir carga automática de um arquivo de configuração pré-definido, usando um servidor DHCP e um servidor TFTP ou FTP;

2.7.5.15. Deve implementar o protocolo LLDP conforme o padrão IEEE 802.1AB, bem como LLDP-MED;

2.7.5.16. Deve permitir a configuração de seu relógio interno de forma automática através do protocolo NTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

2.7.5.17. Deve permitir armazenamento simultâneo de duas imagens de firmware em memória flash.

2.7.5.18. Deve permitir o envio de mensagens de syslog à pelo menos 2 servidores distintos. Deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

2.7.5.19. Deve permitir o envio de syslog com formato conforme RF5424 para prover mais informações no seu header;

2.7.5.20. Deve implementar funcionalidade de rollback automático de configuração, permitindo que o switch retorne automaticamente para uma configuração estável prévio caso o administrador não confirmar a alteração realizada dentro de um prazo de tempo configurável.

2.8. SWITCH DE ACESSO – TIPO 2

2.8.1. ESPECIFICAÇÕES GERAIS

2.8.1.1. Deve possuir altura máxima 1 (um) rack unit (RU);

2.8.1.2. Deve possuir fonte de alimentação interna, do tipo auto-sense, para operar de 100 a 240 VAC;

2.8.1.3. Deve possuir 24 (vinte e quatro) portas 10/100/1000 Mbps, usando conectores RJ-45;

2.8.1.4. As portas 10/100/1000 BASE-T devem ser do tipo MDI/MDIX automático;

2.8.1.5. Deve possuir, no mínimo, 4 (quatro) portas 1/10 Gbps SFP+, as quais não devem operar em modo “combo” com as portas 10/100/1000 BASE-T em par trançado;

2.8.1.6. Deve possuir capacidade de processamento igual ou superior a 96 (noventa e seis) Mpps;

2.8.1.7. Deve possuir capacidade de switching igual ou superior a 128 (cento e vinte e oito) Gbps;

2.8.1.8. Deve possuir, pelo menos, 4 MB de buffers de pacotes;

2.8.1.9. Deve possuir, pelo menos, 2 GB de memória DRAM;

2.8.1.10. Deve possuir, pelo menos, 8 GB de memória NVRAM;

2.8.1.11. Deve implementar os protocolos IEEE 802.3af Power over Ethernet (PoE) e IEEE 802.3at Power over Ethernet Plus (PoE+);

2.8.1.12. Deve implementar funcionalidade que garante o fornecimento contínuo de energia para dispositivos alimentados (PDs) conectados a um switch, mesmo durante o processo de reinicialização do switch, recurso conhecido como Perpetual PoE ou Persistent PoE;

2.8.1.13. Deve possuir PoE power budget de pelo menos 370 (trezentos e setenta) watts;

2.8.1.14. Deve possuir porta de console para gerenciamento utilizando conector RJ-45 ou USB Tipo C;

2.8.1.15. Deve possuir LEDs indicativos de energização, atividade do link e velocidade das portas;

2.8.1.16. Deve permitir identificar através de sinalização visual onde o switch está localizado no rack através de comandos para ligar e desligar os LEDs do equipamento;

2.8.1.17. Deve possuir botão de reset para voltar a para configuração default de fábrica;

2.8.1.18. Deve implementar o padrão IEE 802.3az (Energy-Efficient Ethernet);

2.8.1.19. Deve possuir certificado de homologação junto à ANATEL de acordo a resolução 242 com documentos disponíveis publicamente no sítio público dessa agência na Internet;

2.8.2. Funções de camada 2

2.8.2.1. Deve possuir capacidade de no mínimo 32.000 (trinta e dois mil) endereços MAC;

2.8.2.2. Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad. Deve permitir a configuração de pelo menos 128 (cento e vinte e oito) grupos de LACP com pelo menos 8 (oito) portas dentro de um mesmo grupo;

2.8.2.3. Deve implementar o protocolo IEEE 802.1Q para criação de pelo menos 4000 (quatro mil) vlans ativas;

2.8.2.4. Deve implementar o protocolo IEEE 802.1s (Multiple Spanning Tree), IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1D (MAC Bridging, Spanning Tree);

2.8.2.5. Deve ser compatível com o protocolo PVST / PVST+ e PRST;

2.8.2.6. Deve permitir a configuração de pelo menos 250 (duzentas e cinquenta) instâncias de Spanning Tree;

2.8.2.7. Deve implementar BPDU Guard e Root Guard;

2.8.2.8. Deve permitir a configuração de VLANs “trunking” de acordo com o protocolo 802.1Q e VLANs nativas (sem tag) simultaneamente na mesma porta;

2.8.2.9. Deve permitir a criação VLANs privadas;

2.8.2.10. Deve permitir a configuração de VLAN Q-in-Q Tagging de acordo com o padrão IEEE802.1ad ou IEEE802.1QinQ;

2.8.2.11. Deve implementar selective QinQ;

2.8.2.12. Deve implementar para o protocolo UDLD (Uni-Directional Link Detection) ou DLDP (Device Link Detection Protocol) ou similar;

2.8.2.13. Deve implementar jumbo frames até 9000 bytes nas portas Gigabit Ethernet;

2.8.2.14. Deve implementar mecanismos para controle do tráfego broadcasts, multicast e unknown unicast;

2.8.2.15. Deve implementar mecanismo de detecção ativa de loops através do envio frames de detecção. Na detecção de um evento de loop, deve ser capaz de realizar o bloqueio da porta (port shutdown);

2.8.2.16. Deve permitir a configuração de endereços MAC unicast e multicast estáticos em múltiplas portas ethernet simultaneamente, para permitir a configuração de “clusters” de firewalls;

2.8.2.17. Deve implementar IGMP Snooping para IGMPv1, IGMPv2 e IGMPv3;

2.8.2.18. Deve implmenetar MLD snooping v1 e v2;

2.8.2.19. Deve implementar protocolo de proteção de topologia em anel;

2.8.2.20. Deve possuir DHCP Server para IPv4 e IPv6;

2.8.3. Qualidade de Serviço

2.8.3.1. Deve permitir priorização de tráfego usando 8 (oito) filas de priorização por porta;

2.8.3.2. Deve permitir priorização de tráfego baseado no padrão IEEE 802.1p e no campo DSCP do protocolo Diffserv;

2.8.3.3. Deve implementar pelos menos os seguintes métodos para configuração das filas de priorização: ponderada, prioridade estrita e ambas combinadas;

2.8.3.4. Implementar priorização de tráfego baseado em porta física, protocolo IEEE 802.1p, endereços IP de origem e destino e portas TCP/UDP de origem e destino;

2.8.3.5. Deve permitir a configuração de Rate Limiting de entrada;

2.8.3.6. Deve permitir a configuração de Rate Shaping de saída;

2.8.3.7. Deve implementar os seguintes algoritmos de fila: Strict Priority e Round Robin com distribuição de pesos WRR (Weighted Round Robin) e uma combinação entre os dois métodos SP e WRR;

2.8.4. Segurança

2.8.4.1. Deve permitir autenticação de usuários usando o padrão IEEE 802.1x, permitindo associação dinâmica de VLANs e ACLs usando profiles definidas por um servidor RADIUS externo;

2.8.4.2. Deve permitir a associação de VLANs restritas para usuários que falhem durante a autenticação 802.1X;

2.8.4.3. Implementar método de autenticação baseado em endereço MAC para os dispositivos que não possuírem suplicantes 802.1X;

2.8.4.4. Deve possuir capacidade de autenticação 802.1x com atribuição de VLAN, regras de acesso de segurança e QoS individuais para, no mínimo, 02 (dois) dispositivos (Ex.: Telefone IP e PC) conectados em uma única porta e usando VLANs distintas;

2.8.4.5. Deve permitir, no mínimo e em cada porta, os seguintes tipos de autenticação usando VLANs distintas:

2.8.4.5.1. 2 (dois) dispositivos que suportam o padrão IEEE 802.1x;

2.8.4.5.2. 2 (dois) dispositivos MAC que não suportam o padrão IEEE 802.1x;

2.8.4.5.3. 1 (um) dispositivo que suporta o padrão IEEE 802.1x e 1 (um) dispositivo MAC que não suporta o padrão IEEE 802.1x;

2.8.4.6. O equipamento deve permitir a configuração de reautenticação 802.1x periódica;

2.8.4.7. O equipamento ofertado deve permitir a autenticação via Web Authentication para usuários que não possuem 802.1x;

2.8.4.8. Deve implementar “Change of Authorization” de acordo com a RFC 5176;

2.8.4.9. Deve permitir a autenticação de usuários para acesso às funções de gerenciamento usando-se os protocolos RADIUS, TACACS ou TACACS+;

2.8.4.10. Deve permitir a criação de ACLs para a filtragem de tráfego IPv4 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, bits do protocolo 802.1p e campo DSCP do protocolo Diffserv;

2.8.4.11. Deve permitir a criação de ACLs para a filtragem de tráfego IPv6 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, campo PCP do protocolo 802.1p e campo DSCP do protocolo Diffserv;

2.8.4.12. Deve implementar ACLs de entrada e ACLs de saída para IPv4;

2.8.4.13. Deve implementar ACLs de entrada e ACLs de saída para IPv6;

2.8.4.14. Permitir a filtragem do tráfego através de pelo menos 500 (quinhentas) regras de ACL (Access Control List);

2.8.4.15. Deve implementar segurança de acesso baseada em endereços MAC de origem, com a possibilidade de bloqueio permanente ou temporário das portas onde for detectada uma violação de segurança;

2.8.4.16. Deve permitir a criação de filtros de endereço MAC de origem e destino;

2.8.4.17. Deve possuir protocolos para proteção de ataques de Denial of Service;

2.8.4.18. Deve possuir funcionalidade de proteção contra servidores DHCP não autorizados DHCPv4 snooping e DHCPv6 snooping;

2.8.4.19. Deve possuir funcionalidade de proteção contra-ataques do tipo “ARP Poisoning”;

2.8.4.20. Deve implementar IP Source Guard em IPv4 e IPv6;

2.8.4.21. Deve implementar proteção contra-ataques do tipo TCP SYN e ataques do tipo Smurf;

2.8.4.22. Deve permitir o monitoramento da movimentação de um endereço MAC de uma porta para outra, facilitando a distinção entre um movimento legítmo com um movimento malicioso de um ataque de MAC spoofing;

2.8.4.23. Deve implementar RADsec conforme RFC6614;

2.8.5. Gerenciamento

2.8.5.1. Deve permitir monitoração e configuração usando SNMP v1, v2 e v3;

2.8.5.2. Deve permitir o gerenciamento via SNMPv3 com as seguintes opções: sem autenticação e sem privacidade, com autenticação e sem privacidade e com autenticação e com privacidade;

2.8.5.3. Deve ser possível enviar “traps” e realizar o gerenciamento via SNMP através das redes IPv4 e IPv6;

2.8.5.4. Deve permitir a configuração de porta para espelhamento de tráfego, para a coleta de pacotes em analisadores de protocolo ou detecção de intrusão;

2.8.5.5. Deve permitir espelhamento de tráfego baseado em Porta, VLAN, Filtro MAC e ACL;

2.8.5.6. Deve permitir a configuração de porta para espelhamento de tráfego para uma porta em um switch remoto;

2.8.5.7. Deve implementar gerenciamento usando SSH v2 utilizando os algoritmos de criptografia 3DES e AES. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

2.8.5.8. Deve implementar gerenciamento via Telnet. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

2.8.5.9. Deve implementar pelo menos 4 (quatro) grupos de RMON;

2.8.5.10. Deve permitir o monitoramento dos transceivers óticos, retornando informação de temperatura, potência de transmissão (dBm), potência de recepção (dBm) e status;

2.8.5.11. Deve implementar funcionalidade de diagnóstico do cabo de par trançado, retornando informação de comprimento do cabo, status do link;

2.8.5.12. Deve permitir a atualização de arquivos de configuração e imagens de firmware usando TFTP ou FTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

2.8.5.13. Deve permitir a atualização de imagens de firmware dos equipamentos de uma pilha sem a necessidade de reinicialização simultânea de todos os equipamentos da pilha, permitindo a continuidade do tráfego de dados durante o processo de atualização;

2.8.5.14. Deve permitir configuração automática do seu próprio endereço IP e a seguir carga automática de um arquivo de configuração pré-definido, usando um servidor DHCP e um servidor TFTP ou FTP;

2.8.5.15. Deve implementar o protocolo LLDP conforme o padrão IEEE 802.1AB, bem como LLDP-MED;

2.8.5.16. Deve permitir a configuração de seu relógio interno de forma automática através do protocolo NTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

2.8.5.17. Deve permitir armazenamento simultâneo de duas imagens de firmware em memória flash.

2.8.5.18. Deve permitir o envio de mensagens de syslog à pelo menos 2 servidores distintos. Deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

2.8.5.19. Deve permitir o envio de syslog com formato conforme RF5424 para prover mais informações no seu header;

2.8.5.20. Deve implementar funcionalidade de rollback automático de configuração, permitindo que o switch retorne automaticamente para uma configuração estável prévio caso o administrador não confirmar a alteração realizada dentro de um prazo de tempo configurável.

2.9. SWITCH DE ACESSO - TIPO 3

2.9.1. ESPECIFICAÇÕES GERAIS

2.9.1.1. Deve possuir altura máxima 1 (um) rack unit (RU);

2.9.1.2. Deve possuir fonte de alimentação interna, do tipo auto-sense, para operar de 100 a 240 VAC;

2.9.1.3. Deve possuir 48 (quarenta e oito) portas 10/100/1000 Mbps, usando conectores RJ-45;

2.9.1.4. As portas 10/100/1000 BASE-T devem ser do tipo MDI/MDIX automático;

2.9.1.5. Deve possuir, no mínimo, 4 (quatro) portas 1/10 Gbps SFP+, as quais não devem operar em modo “combo” com as portas 10/100/1000 BASE-T em par trançado;

2.9.1.6. Deve possuir capacidade de processamento igual ou superior a 132 (cento e trinta e dois) Mpps;

2.9.1.7. Deve possuir capacidade de switching igual ou superior a 176 (cento e setenta e seis) Gbps;

2.9.1.8. Deve possuir, pelo menos, 4 MB de buffers de pacotes;

2.9.1.9. Deve possuir, pelo menos, 2 GB de memória DRAM;

2.9.1.10. Deve possuir, pelo menos, 8 GB de memória NVRAM;

2.9.1.11. Deve implementar os protocolos IEEE 802.3af Power over Ethernet (PoE) e IEEE 802.3at Power over Ethernet Plus (PoE+);

2.9.1.12. Deve possuir PoE power budget de pelo menos 370 (trezentos e setenta) watts;

2.9.1.13. Deve possuir porta de console para gerenciamento utilizando conector RJ-45 ou USB Tipo C;

2.9.1.14. Deve possuir LEDs indicativos de energização, atividade do link e velocidade das portas;

2.9.1.15. Deve permitir identificar através de sinalização visual onde o switch está localizado no rack através de comandos para ligar e desligar os LEDs do equipamento;

2.9.1.16. Deve possuir botão de reset para voltar para configuração default de fábrica;

2.9.1.17. Deve implementar o padrão IEE 802.3az (Energy-Efficient Ethernet);

2.9.1.18. Deve possuir certificado de homologação junto à ANATEL de acordo a resolução 242 com documentos disponíveis publicamente no sítio público dessa agência na Internet;

2.9.2. Funções de Camada 2

2.9.2.1. Deve possuir capacidade de no mínimo 32.000 (trinta e dois mil) endereços MAC;

2.9.2.2. Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad. Deve permitir a configuração de pelo menos 128 (cento e vinte e oito) grupos de LACP com pelo menos 8 (oito) portas dentro de um mesmo grupo;

2.9.2.3. Deve implementar o protocolo IEEE 802.1Q para criação de pelo menos 4000 (quatro mil) vlans ativas;

2.9.2.4. Deve implementar o protocolo IEEE 802.1s (Multiple Spanning Tree), IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1D (MAC Bridging, Spanning Tree);

2.9.2.5. Deve ser compatível com o protocolo PVST / PVST+ e PRST;

2.9.2.6. Deve permitir a configuração de pelo menos 250 (duzentas e cinquenta) instâncias de Spanning Tree;

2.9.2.7. Deve implementar BPDU Guard e Root Guard;

2.9.2.8. Deve permitir a configuração de VLANs “trunking” de acordo com o protocolo 802.1Q e VLANs nativas (sem tag) simultaneamente na mesma porta;

2.9.2.9. Deve permitir a criação VLANs privadas;

2.9.2.10. Deve permitir a configuração de VLAN Q-in-Q Tagging de acordo com o padrão IEEE802.1ad ou IEEE802.1QinQ;

2.9.2.11. Deve implementar selective QinQ;

2.9.2.12. Deve implementar para o protocolo UDLD (Uni-Directional Link Detection) ou DLDP (Device Link Detection Protocol) ou similar;

2.9.2.13. Deve implementar jumbo frames até 9000 bytes nas portas Gigabit Ethernet;

2.9.2.14. Deve implementar mecanismos para controle do tráfego broadcasts, multicast e unknown unicast;

2.9.2.15. Deve implementar mecanismo de detecção ativa de loops através do envio frames de detecção. Na detecção de um evento de loop, deve ser capaz de realizar o bloqueio da porta (port shutdown);

2.9.2.16. Deve permitir a configuração de endereços MAC unicast e multicast estáticos em múltiplas portas ethernet simultaneamente, para permitir a configuração de “clusters” de firewalls;

2.9.2.17. Deve implementar IGMP Snooping para IGMPv1, IGMPv2 e IGMPv3;

2.9.2.18. Deve implmenetar MLD snooping v1 e v2;

2.9.2.19. Deve implementar protocolo de proteção de topologia em anel;

2.9.2.20. Deve possuir DHCP Server para IPv4 e IPv6;

2.9.3. Qualidade de Serviço

2.9.3.1. Deve permitir priorização de tráfego usando 8 (oito) filas de priorização por porta;

2.9.3.2. Deve permitir priorização de tráfego baseado no padrão IEEE 802.1p e no campo DSCP do protocolo Diffserv;

2.9.3.3. Deve implementar pelos menos os seguintes métodos para configuração das filas de priorização: ponderada, prioridade estrita e ambas combinadas;

2.9.3.4. Implementar priorização de tráfego baseado em porta física, protocolo IEEE 802.1p, endereços IP de origem e destino e portas TCP/UDP de origem e destino;

2.9.3.5. Deve permitir a configuração de Rate Limiting de entrada;

2.9.3.6. Deve permitir a configuração de Rate Shaping de saída;

2.9.3.7. Deve implementar os seguintes algoritmos de fila: Strict Priority e Round Robin com distribuição de pesos WRR (Weighted Round Robin) e uma combinação entre os dois métodos SP e WRR;

2.9.4. Segurança

2.9.4.1. Deve permitir autenticação de usuários usando o padrão IEEE 802.1x, permitindo associação dinâmica de VLANs e ACLs usando profiles definidas por um servidor RADIUS externo;

2.9.4.2. Deve permitir a associação de VLANs restritas para usuários que falhem durante a autenticação 802.1X;

2.9.4.3. Implementar método de autenticação baseado em endereço MAC para os dispositivos que não possuírem suplicantes 802.1X;

2.9.4.4. Deve possuir capacidade de autenticação 802.1x com atribuição de VLAN, regras de acesso de segurança e QoS individuais para, no mínimo, 02 (dois) dispositivos (Ex.: Telefone IP e PC) conectados em uma única porta e usando VLANs distintas;

2.9.4.5. Deve permitir, no mínimo e em cada porta, os seguintes tipos de autenticação usando VLANs distintas:

2.9.4.5.1. 2 (dois) dispositivos que suportam o padrão IEEE 802.1x;

2.9.4.5.2. 2 (dois) dispositivos MAC que não suportam o padrão IEEE 802.1x;

2.9.4.5.3. 1 (um) dispositivo que suporta o padrão IEEE 802.1x e 1 (um) dispositivo MAC que não suporta o padrão IEEE 802.1x;

2.9.4.6. O equipamento deve permitir a configuração de reautenticação 802.1x periódica;

2.9.4.7. O equipamento ofertado deve permitir a autenticação via Web Authentication para usuários que não possuem 802.1x;

2.9.4.8. Deve implementar “Change of Authorization” de acordo com a RFC 5176;

2.9.4.9. Deve permitir a autenticação de usuários para acesso às funções de gerenciamento usando-se os protocolos RADIUS, TACACS ou TACACS+;

2.9.4.10. Deve permitir a criação de ACLs para a filtragem de tráfego IPv4 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, bits do protocolo 802.1p e campo DSCP do protocolo Diffserv;

2.9.4.11. Deve permitir a criação de ACLs para a filtragem de tráfego IPv6 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, campo PCP do protocolo 802.1p e campo DSCP do protocolo Diffserv;

2.9.4.12. Deve implementar ACLs de entrada e ACLs de saída para IPv4;

2.9.4.13. Deve implementar ACLs de entrada e ACLs de saída para IPv6;

2.9.4.14. Permitir a filtragem do tráfego através de pelo menos 500 (quinhentas) regras de ACL (Access Control List);

2.9.4.15. Deve implementar segurança de acesso baseada em endereços MAC de origem, com a possibilidade de bloqueio permanente ou temporário das portas onde for detectada uma violação de segurança;

2.9.4.16. Deve permitir a criação de filtros de endereço MAC de origem e destino;

2.9.4.17. Deve possuir protocolos para proteção de ataques de Denial of Service;

2.9.4.18. Deve possuir funcionalidade de proteção contra servidores DHCP não autorizados DHCPv4 snooping e DHCPv6 snooping;

2.9.4.19. Deve possuir funcionalidade de proteção contra-ataques do tipo “ARP Poisoning”;

2.9.4.20. Deve implementar IP Source Guard em IPv4 e IPv6;

2.9.4.21. Deve implementar proteção contra-ataques do tipo TCP SYN e ataques do tipo Smurf;

2.9.4.22. Deve permitir o monitoramento da movimentação de um endereço MAC de uma porta para outra, facilitando a distinção entre um movimento legítmo com um movimento malicioso de um ataque de MAC spoofing;

2.9.4.23. Deve implementar RADsec conforme RFC6614;

2.9.5. **Gerenciamento**

2.9.5.1. Deve permitir monitoração e configuração usando SNMP v1, v2 e v3;

2.9.5.2. Deve permitir o gerenciamento via SNMPv3 com as seguintes opções: sem autenticação e sem privacidade, com autenticação e sem privacidade e com autenticação e com privacidade;

2.9.5.3. Deve ser possível enviar “traps” e realizar o gerenciamento via SNMP através das redes IPv4 e IPv6;

2.9.5.4. Deve permitir a configuração de porta para espelhamento de tráfego, para a coleta de pacotes em analisadores de protocolo ou detecção de intrusão;

2.9.5.5. Deve permitir espelhamento de tráfego baseado em Porta, VLAN, Filtro MAC e ACL;

2.9.5.6. Deve permitir a configuração de porta para espelhamento de tráfego para uma porta em um switch remoto;

2.9.5.7. Deve implementar gerenciamento usando SSH v2 utilizando os algoritmos de criptografia 3DES e AES. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

2.9.5.8. Deve implementar gerenciamento via Telnet. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

2.9.5.9. Deve implementar pelo menos 4 (quatro) grupos de RMON;

2.9.5.10. Deve permitir o monitoramento dos transceivers óticos, retornando informação de temperatura, potência de transmissão (dBm), potência de recepção (dBm) e status;

2.9.5.11. Deve implementar funcionalidade de diagnóstico do cabo de par trançado, retornando informação de comprimento do cabo, status do link;

2.9.5.12. Deve permitir a atualização de arquivos de configuração e imagens de firmware usando TFTP ou FTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

2.9.5.13. Deve permitir a atualização de imagens de firmware dos equipamentos de uma pilha sem a necessidade de reinicialização simultânea de todos os equipamentos da pilha, permitindo a continuidade do tráfego de dados durante o processo de atualização;

2.9.5.14. Deve permitir configuração automática do seu próprio endereço IP e a seguir carga automática de um arquivo de configuração pré-definido, usando um servidor DHCP e um servidor TFTP ou FTP;

2.9.5.15. Deve implementar o protocolo LLDP conforme o padrão IEEE 802.1AB, bem como LLDP-MED;

2.9.5.16. Deve permitir a configuração de seu relógio interno de forma automática através do protocolo NTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

2.9.5.17. Deve permitir armazenamento simultâneo de duas imagens de firmware em memória flash.

2.9.5.18. Deve permitir o envio de mensagens de syslog à pelo menos 2 servidores distintos. Deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

2.9.5.19. Deve permitir o envio de syslog com formato conforme RF5424 para prover mais informações no seu header;

2.9.5.20. Deve implementar funcionalidade de rollback automático de configuração, permitindo que o switch retorne automaticamente para uma configuração estável prévio caso o administrador não confirmar a alteração realizada dentro de um prazo de tempo configurável.

3. PONTOS DE ACESSO COORPORATIVO, INDOOR E OUTDOOR - REQUISITOS GERAIS PARA PONTOS DE ACESSO WIFI TIPOS 1, 2, 3, 4 e 5:

3.1. Todos os Pontos de Acesso Wi-fi do Lote 1 especificados no presente documento devem ser do mesmo fabricante, compondo uma solução única de rede, para assegurar a compatibilidade funcional de todos os recursos e permitir o gerenciamento unificado.

3.2. Todos os acessórios que serão utilizados na prestação do serviço, tais como cabos de força (padrão ABNT NBR 14136) e cabos de interconexões (DAC/AOC/FIBRAS e etc), assim como transceivers e conversores de mídia deverão estar inclusos na solução.

3.3. O fornecedor poderá utilizar injetores PoE (Power over Ethernet), limitando-se a até 10% (dez porcento) do volume total de Pontos de Acesso wi-fi, devendo atender todas as demais especificações técnicas descritas.

3.4. Caso o fornecedor opte pelo fornecimento na modalidade prevista no item 3.3, os injetores PoE deverão necessariamente serem do mesmo fabricante dos pontos de acesso wi-fi.

3.5. Esses pontos de acesso wi-fi deverão possuir a mesma console de gerência dos switches.

3.6. A controladora dos Pontos de Acesso Wi-fi deve ser centralizada e fornecida em ambiente de nuvem como serviço (**SaaS**).

3.7. Todos os modelos-tipo de pontos de acesso WiFi apresentados abaixo deverão atender aos seguintes requisitos:

3.7.1. Desenho de solução com alta disponibilidade e tolerância a falhas;

3.7.2. Gerenciamento dos recursos de rádio que permitem que os pontos de acesso automaticamente ajustem a cobertura em caso de fala em um dos pontos de acesso;

3.7.3. Os pontos de acesso deverão ser fornecidos com kit de fixação em parede ou teto (indoor e outdoor).

3.8. PONTO DE ACESSO - TIPO 1

3.8.1. ESPECIFICAÇÕES GERAIS

3.8.2. Deverá ser do mesmo fabricante do controlador WLAN.

3.8.3. Deverá ser apresentado certificado válido de interoperabilidade fornecido pela Wi-Fi Alliance na categoria de Enterprise Access Point.

3.8.4. Suportar, no mínimo, 256 (duzentos e cinquenta e seis) usuários wireless simultâneos, sem nenhum tipo de licença adicional.

3.8.5. Possuir suporte a pelo menos 16 (dezesseis) SSIDs por ponto de acesso.

3.8.6. Possibilitar alimentação elétrica local via fonte de alimentação com seleção automática de tensão (100-240V) e via padrão PoE (IEEE 802.3af ou 802.3at).

3.8.7. Deve suportar temperatura de operação entre 0°C a 40°C.

3.8.8. Deverá possuir estrutura que permita a utilização do equipamento em locais internos, com fixação em teto e parede.

3.8.9. Não serão aceitos equipamentos com antenas aparentes (externas ao ponto de acesso) rosqueáveis, permitindo sua remoção.

3.8.10. Deve possuir LEDs para a indicação do status das portas ethernet, rede wireless, gerenciamento via controladora, indicador de conexão sem fio Mesh e da atividade do equipamento.

3.8.11. Deverá ser fornecido com todas as funcionalidades de segurança habilitadas.

3.8.12. Deverá ser fornecido com a versão mais recente de software.

3.8.13. Características dos Rádios

3.8.14. O ponto de acesso deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax com operação nas frequências 2.4 GHz e 5 GHz de forma simultânea.

3.8.15. Implementar as seguintes taxas de transmissão com fallback automático:

3.8.15.1. IEEE 802.11b: 11, 5.5, 2 e 1 Mbps

3.8.15.2. IEEE 802.11a e IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps

3.8.15.3. IEEE 802.11n: 6.5 Mbps a 300 Mbps

3.8.15.4. IEEE 802.11ac: 6.5 Mbps a 867 Mbps

3.8.15.5. IEEE 802.11ax: 4 até 1200 Mbps

3.8.16. Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio em 2.4GHz e 5GHz e com ganhos máximos combinados de no mínimo, 3 dBi.

3.8.17. Deve suportar potência de saída agregada somando todas as cadeias de transmissão de, no mínimo, 17 dBm para 5 GHz e de, no mínimo, 20 dBm para 2.4 GHz.

3.8.18. Deverá suportar canalização de 20 MHz, 40 MHz e 80 MHz.

3.8.19. Deverá possuir mecanismo de rádio com suporte a MIMO 2x2 com 2 spatial streams.

3.8.20. Deverá possuir suporte a Multi User MIMO (MU-MIMO)

3.8.21. Deverá possuir suporte a MRC – Maximal Ratio Combining ou similar

3.8.22. Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2.4GHz livre para dispositivos que trabalhem somente nesta frequência.

3.8.23. Permitir ajustes dinâmicos de RF de modo a otimizar o tamanho da célula de abrangência de RF.

3.8.24. Deve ser capaz de operar no modo Mesh sem adição de novo hardware ou alteração do sistema operacional, sendo que a comunicação até o controlador pode ser feita via wireless ou pela rede local.

3.8.25. Deve suportar autocura por meio de Mesh em caso de falha da conexão cabeada de dados, bem como permitir que os pontos de acesso gerenciados estabeleçam automaticamente uma rede mesh sem fio.

3.8.26. Possuir capacidade de selecionar automaticamente o canal de transmissão.

3.8.27. Rede e Serviços

3.8.28. Deverá possuir 01 (uma) interface IEEE 802.3 10/100/1000 Mbps Base-T Ethernet, auto-sensing, com conector RJ-45, para conexão à rede local fixa.

3.8.29. Deverá possuir ao menos uma porta USB para inserção de dispositivos voltados à implementação de redes IoT com suporte aos padrões BLE ou ZigBee

3.8.30. Deve suportar, em conjunto com o controlador de rede sem fio, a identificação e controle de aplicações dos dispositivos clientes conectados ao ponto de acesso.

3.8.31. Deve suportar, em conjunto com o controlador de rede sem fio, a configuração de limite de banda (rate limit) por usuário e por SSID.

3.8.32. Deve suportar, em conjunto com o controlador, suporte ao mecanismo de localização e rastreamento de usuários (Location Based Service).

3.8.33. O ponto de acesso poderá estar conectado diretamente ou remotamente ao controlador WLAN, inclusive através de roteamento em Camada 3.

3.8.34. Implementar cliente DHCP, para configuração automática de seu endereço IP e implementar também suporte à endereçamento IP estático.

3.8.35. Deve suportar VLANs conforme o padrão IEEE 802.1Q.

3.8.36. Deverá permitir atribuir uma VLAN para cada SSID.

3.8.37. Deverá suportar o uso de VLANs dinâmicas em conjunto com o controlador de rede sem fio.

3.8.38. Deverá suportar as seguintes funcionalidades wireless:

3.8.38.1. IEEE 802.11r

3.8.38.2. IEEE 802.11v

3.8.38.3. IEEE 802.11k

3.8.38.4. WMM e Power Save

3.8.38.5. LPDC e STBC

3.8.39. Deve suportar limitação de banda por grupo de usuários ou por SSID.

3.8.40. Deve implementar balanceamento de usuários por ponto de acesso e por rádio (2.4GHz e 5 GHz).

3.8.41. Deve implementar mecanismo para otimização de roaming entre pontos de acesso.

3.9. Segurança e Gerenciamento

3.9.1. Deve suportar a utilização de sistema antifurto do tipo Kensington lock ou similar que permita a instalação de um cabo de segurança com a finalidade de evitar furto do equipamento.

3.9.2. Implementar, pelo menos, os seguintes padrões de segurança wireless:

3.9.2.1. (WPA) Wi-Fi Protected Access

3.9.2.2. (WPA2) Wi-Fi Protected Access 2

3.9.2.3. (WPA3) Wi-Fi Protected Access 3

3.9.2.4. (AES) Advanced Encryption Standard

3.9.2.5. (TKIP) Temporal Key Integrity Protocol

3.9.2.6. IEEE 802.1x

3.9.2.7. IEEE 802.11i

3.9.3. Deverá permitir a criação de filtros de MAC address de forma a restringir o acesso à rede wireless.

3.9.4. Permitir habilitar e desabilitar a divulgação do SSID.

3.9.5. Deve implementar autenticação de usuários usando portal de captura.

3.9.6. Deve implementar autenticação de usuários usando redes baseadas em portal captivo WISPr

3.9.7. Deve implementar autenticação de usuários usando redes baseadas em padrão Hotspot 2.0.

3.9.8. Permitir a configuração e gerenciamento direto através de browser padrão (HTTPS), SSH, SNMPv2c e SNMPv3, ou através do controlador, a fim de se garantir a segurança dos dados.

3.9.9. Permitir gerenciamento através de plataformas de software que sigam padrões SNMPv2c e SNMPv3.

3.9.10. Implementar funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, das políticas de segurança, QoS, autenticação e monitoramento de RF.

3.9.11. Permitir que sua configuração seja realizada automaticamente quando este for conectado ao controlador WLAN do mesmo fabricante.

3.9.12. Permitir que o processo de atualização de software seja realizado manualmente através de interface web, FTP ou TFTP e automaticamente através de controlador WLAN do mesmo fabricante.

3.9.13. Deverá ser fornecido com todas as funcionalidades de segurança, incluindo WIDS, e Wi-Fi Mesh habilitadas, incluindo autocura via Mesh.

3.10. PONTO DE ACESSO - TIPO 2

3.10.1. ESPECIFICAÇÕES GERAIS

3.10.1.1. Deverá ser do mesmo fabricante do controlador WLAN para fins de compatibilidade.

3.10.1.2. Deverá possuir estrutura que permita a utilização do equipamento em locais internos, com fixação em teto e parede.

3.10.1.3. Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto, com data anterior à publicação do edital, conforme a resolução 242. Não serão aceitos protocolos de entrada ou outros documentos diferentes do certificado, uma vez que os mesmos não garantem o fornecimento de equipamentos homologados e em conformidade com as leis brasileiras.

3.10.1.4. Visando a plena compatibilidade do ponto de acesso com o padrão WiFi 6 e suas respectivas funcionalidades, a citar, de forma não-exaustiva, DL OFDMA, UL OFDMA, DL MU-MIMO e se faz necessário que o equipamento ofertado esteja listado como Wi-Fi CERTIFIED 6 no programa da WiFi Alliance na data do pregão.

3.10.1.5. Deve possuir a certificação IEC 61373 para uso em ambientes sujeitos à vibração e impactos.

3.10.1.6. Deve ser compatível com o padrão UL 2043, que regula os componentes dos materiais com o intuito de proteger contra danos causados por fogo, bem como pela fumaça.

3.10.1.7. Suportar, no mínimo, 500 (quinhentos) usuários wireless simultâneos, sem nenhum tipo de licença adicional.

3.10.1.8. Possuir suporte a pelo menos 16 (dezesseis) SSIDs por ponto de acesso.

3.10.1.9. Possibilitar alimentação elétrica local via fonte de alimentação com seleção automática de tensão (100-240V) e via padrão PoE (IEEE 802.3at ou 802.3bt). Ademais, para PoE, a alimentação elétrica deve ocorrer através de uma única interface de rede, sem perda de funcionalidade e de desempenho.

3.10.1.10. Deve suportar temperatura de operação entre 0°C a 40°C.

3.10.1.11. O equipamento ofertado não deverá possuir antenas aparentes externas ao ponto de acesso, evitando desta forma que as mesmas sejam removidas, o que ocasionaria na degradação do desempenho da rede sem fio.

3.10.1.12. Deverá possuir 2 (duas) interfaces ethernet, sendo 1 (uma) 10/100/1000 Mbps e 1 (uma) 1/2.5 Gbps, utilizando conector RJ-45, para conexão à rede local.

3.10.1.13. Deve suportar LLDP na interface ethernet.

3.10.1.14. Deverá possuir, no mínimo, um rádio embarcado para IoT, o qual deve ser compatível com BLE ou ZigBee.

3.10.1.15. Deverá dispor de uma porta USB para inserção de módulo IoT compatível com BLE e ZigBee.

3.10.1.16. Deverá possuir múltiplos LEDs para a indicação do status da alimentação do ponto de acesso, rádios de 2.4 GHz e 5 GHz, operação em Mesh e gerenciamento via controladora.

3.10.1.17. Deverá ser fornecido com todas as funcionalidades de segurança, incluindo WIPS/WIDS, e Wi-Fi Mesh habilitadas, incluindo autocura via Mesh.

3.10.1.18. Deve ser compatível com IPv4, IPv6 e dual-stack.

3.10.2. Características dos Rádios

3.10.2.1. O ponto de acesso deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax, com operação nas frequências de 2.4 GHz e 5 GHz de forma simultânea.

3.10.2.2. Implementar as seguintes taxas de transmissão com fallback automático: IEEE 802.11b: 1 Mbps a 11 Mbps, IEEE 802.11a e IEEE 802.11g: 6 Mbps a 54 Mbps, IEEE 802.11n: 6.5 Mbps a 600 Mbps, IEEE 802.11ac: 6.5 Mbps a 1732 Mbps e IEEE 802.11ax: 4 Mbps a 2400 Mbps.

3.10.2.3. Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax, com ganhos de, no mínimo 3 dBi para 2.4GHz e 5GHz.

3.10.2.4. Deverá suportar potência agregada de saída, considerando todas as cadeias MIMO, de, no mínimo, 24 dBm na frequência de 5 GHz e 23 dBm na frequência de 2.4 GHz.

3.10.2.5. Deverá suportar canalização de 20 MHz, 40 MHz, 80 MHz e 160 MHz.

3.10.2.6. Deverá possuir mecanismo de rádio com suporte a 6 (seis) fluxos espaciais, sendo 4x4:4 em 5 GHz e 2x2:2 em 2.4 GHz para SU-MIMO e MU-MIMO.

3.10.2.7. Deve permitir ajustes dinâmicos do sinal de rádio frequência para otimizar o tamanho da célula de abrangência do ponto de acesso.

3.10.2.8. Deve possuir capacidade de selecionar automaticamente o canal de transmissão.

3.10.2.9. Deve suportar os padrões IEEE 802.11r, IEEE 802.11k e IEEE 802.11v.

3.10.3. **Serviços, Segurança e Gerenciamento**

3.10.3.1. Deve permitir controle e gerenciamento pelo controlador WLAN através de Camada 2 ou 3 do modelo OSI.

3.10.3.2. Deve ser capaz de operar no modo Mesh sem adição de novo hardware ou alteração do sistema operacional, sendo que a comunicação até o controlador pode ser feita via wireless ou pela rede local.

3.10.3.3. Deve suportar autocura por meio de Mesh em caso de falha da conexão cabeada de dados, bem como permitir que os pontos de acesso gerenciados estabeleçam automaticamente uma rede mesh sem fio.

3.10.3.4. Em caso de falha de comunicação entre os pontos de acesso e o controlador WLAN, os usuários associados à rede sem fio devem continuar conectados com acesso à rede. Além disso, deve ser possível que novos usuários se associem à rede sem fio utilizando autenticação do tipo IEEE 802.1x mesmo que os pontos de acesso estejam sem comunicação com a controladora.

3.10.3.5. Deve suportar, somente por meio do ponto de acesso em conjunto com o controlador de rede sem fio, a identificação e controle de aplicações dos dispositivos clientes conectados ao ponto de acesso, levando em consideração a camada 7 do modelo OSI.

3.10.3.6. Deve suportar a configuração de limite de banda por usuário ou por SSID.

3.10.3.7. Deve oferecer suporte a mecanismo de localização e rastreamento de usuários (Location Based Services).

3.10.3.8. Implementar cliente DHCP, para configuração automática de seu endereço IP e implementar também suporte a endereçamento IP estático.

3.10.3.9. Deve suportar VLANs conforme o padrão IEEE 802.1Q.

3.10.3.10. Deve suportar atribuição dinâmica de VLAN por usuário.

3.10.3.11. Deve implementar balanceamento de usuários por ponto de acesso.

3.10.3.12. Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2.4 GHz livre para dispositivos que trabalhem somente nesta frequência.

3.10.3.13. Deve implementar mecanismo para otimização de roaming entre pontos de acesso.

3.10.3.14. Deve suportar HotSpot 2.0, Captive Portal e WISPr.

3.10.3.15. Implementar, pelo menos, os seguintes padrões de segurança wireless: (WPA) Wi-Fi Protected Access, (WPA2) Wi-Fi Protected Access 2, (WPA3) Wi-Fi Protected Access 3, (AES) Advanced Encryption Standard, (TKIP) Temporal Key Integrity Protocol, PSK por dispositivo, IEEE 802.1X e IEEE 802.11i.

3.10.3.16. Deverá permitir a criação de filtros de endereços MAC de forma a restringir o acesso à rede sem fio.

3.10.3.17. Deverá permitir a criação de listas de controle de acesso de Camada 3 e 4 do modelo OSI.

3.10.3.18. Deverá ser possível criar políticas de controle com base no tipo ou sistema operacional do dispositivo.

3.10.3.19. Deve permitir habilitar e desabilitar a divulgação do SSID.

3.10.3.20. Deverá implementar autenticação de usuários usando portal de captura;

3.10.3.21. Deve implementar autenticação de usuários usando WISPr e Hotspot 2.0.

3.10.3.22. Deverá suportar funções para análise de espectro.

3.10.3.23. Deve disponibilizar uma página local acessível pelo cliente conectado ao ponto de acesso para visualização de estatísticas de conexão e informações do respectivo ponto de acesso.

3.10.3.24. Deve suportar conversão de tráfego multicast para unicast.

3.10.3.25. Permitir a configuração e gerenciamento direto através de navegador padrão (HTTPS), SSH, SNMPv2c, SNMPv3.

3.10.3.26. Permitir que sua configuração seja realizada automaticamente quando este for conectado ao controlador WLAN do mesmo fabricante.

3.10.3.27. Implementar funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, das políticas de segurança, QoS, autenticação e monitoramento de RF.

3.10.3.28. Permitir que o processo de atualização de software seja realizado manualmente através de interface Web, FTP ou TFTP e automaticamente através de controlador WLAN do mesmo fabricante.

3.11. PONTO DE ACESSO - TIPO 3

3.11.1. ESPECIFICAÇÕES GERAIS

3.11.1.1. Deverá ser do mesmo fabricante do controlador WLAN para fins de compatibilidade.

3.11.1.2. Deverá possuir estrutura que permita a utilização do equipamento em locais internos, com fixação em teto e parede, devendo ser fornecidos todos os acessórios necessários para estas montagens.

3.11.1.3. Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto, com data anterior à publicação do edital, conforme a resolução 242. Não serão aceitos protocolos de entrada ou outros documentos diferentes do certificado, uma vez que os mesmos não garantem o fornecimento de equipamentos homologados e em conformidade com as leis brasileiras.

3.11.1.4. Deve ser compatível com o padrão UL2043, que regula os componentes dos materiais com o intuito de proteger contra danos causados por fogo, bem como pela fumaça.

3.11.1.5. Suportar, no mínimo, 256 (duzentos e cinquenta e seis) usuários wireless simultâneos, sem nenhum tipo de licença adicional.

3.11.1.6. Possuir suporte a pelo menos 16 (dezesseis) SSIDs por ponto de acesso.

3.11.1.7. Possibilitar alimentação elétrica local via fonte de alimentação DC e via padrão PoE (IEEE 802.3at ou 802.3bt). Ademais, para PoE, a alimentação elétrica deve ocorrer através de uma única interface de rede, sem perda de funcionalidade e de desempenho.

3.11.1.8. Deve suportar temperatura de operação entre 0°C a 40°C.

3.11.1.9. O equipamento ofertado não deverá possuir antenas aparentes externas ao ponto de acesso, evitando desta forma que as mesmas sejam removidas, o que ocasionaria na degradação do desempenho da rede sem fio.

3.11.1.10. Deverá possuir 1 (uma) interface ethernet multi-gigabit 1/2.5Gbps utilizando conector RJ-45, para conexão à rede local.

3.11.1.11. Deverá possuir LED para a indicação do status de operação do ponto de acesso.

3.11.1.12. Deverá ser fornecido com todas as funcionalidades de segurança, incluindo WIDS, e Wi-Fi Mesh habilitadas.

3.11.1.13. Deverá ser fornecido com a versão mais recente de software.

3.11.1.14. Deve ser compatível com IPv4 e IPv6.

3.11.2. Características dos Rádios

3.11.2.1. O ponto de acesso deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11ax e IEEE 802.11be, com operação nas frequências de 2.4 GHz, 5 GHz de forma simultânea.

3.11.2.2. Implementar as seguintes taxas de transmissão com fallback automático: IEEE 802.11b: 1 Mbps à 11 Mbps, IEEE 802.11a e IEEE 802.11g: 6 Mbps à 54 Mbps, IEEE 802.11n: 6.5 Mbps à 300 Mbps, IEEE 802.11ac: 6.5 Mbps à 860 Mbps, IEEE 802.11ax: 4 Mbps à 1774 Mbps e IEEE 802.11be: 4Mbps à 3570 Mbps.

3.11.2.3. Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11ax e IEEE 802.11be, com ganhos de no mínimo 3dBi nas frequências de 2,4GHz e 5GHz.

3.11.2.4. Deverá suportar potência agregada de saída, considerando todas as cadeias MIMO, de, no mínimo, 23 dBm nas frequências de 2,4 GHz e 5 GHz.

3.11.2.5. Deverá suportar canalização de 20 MHz, 40 MHz, 80 MHz e 160 MHz.

3.11.2.6. Deverá possuir mecanismo de rádio com suporte a 4 (quatro) fluxos espaciais simultâneos, sendo 2x2:2 em 2.4 GHz e 2x2:2 em 5 GHz, para SU-MIMO e MU-MIMO.

3.11.2.7. Deve permitir ajustes dinâmicos do sinal de rádio frequência para otimizar o tamanho da célula de abrangência do ponto de acesso.

3.11.2.8. Deve possuir capacidade de selecionar automaticamente o canal de transmissão.

3.11.2.9. Deve suportar os padrões IEEE 802.11r, IEEE 802.11k e IEEE 802.11v.

3.11.3. Serviços, Segurança e Gerenciamento

3.11.3.1. Deve permitir controle e gerenciamento pelo controlador WLAN através de Camada 2 ou 3 do modelo OSI.

3.11.3.2. Deve ser capaz de operar no modo Mesh sem adição de novo hardware ou alteração do sistema operacional, sendo que a comunicação até o controlador pode ser feita via wireless ou pela rede local.

3.11.3.3. Deve suportar auto cura por meio de Mesh em caso de falha da conexão cabeada de dados, bem como permitir que os pontos de acesso gerenciados estabeleçam automaticamente uma rede mesh sem fio.

3.11.3.4. Em caso de falha de comunicação entre os pontos de acesso e o controlador WLAN, os usuários associados à rede sem fio devem continuar conectados com acesso à rede. Além disso, deve ser possível que novos usuários se associem à rede sem fio utilizando autenticação do tipo IEEE 802.1X mesmo que os pontos de acesso estejam sem comunicação com a controladora.

3.11.3.5. Deve suportar, somente por meio do ponto de acesso em conjunto com o controlador de rede sem fio, a identificação e controle de aplicações dos dispositivos clientes conectados ao ponto de acesso, levando em consideração a camada 7 do modelo OSI.

3.11.3.6. Deve suportar a configuração de limite de banda por usuário ou por SSID.

3.11.3.7. Implementar cliente DHCP, para configuração automática de seu endereço IP e implementar também suporte a endereçamento IP estático.

3.11.3.8. Deve suportar VLANs conforme o padrão IEEE 802.1Q.

3.11.3.9. Deve suportar atribuição dinâmica de VLAN por usuário.

3.11.3.10. Deve implementar balanceamento de usuários por ponto de acesso.

3.11.3.11. Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2.4 GHz livre para dispositivos que trabalhem somente nesta frequência.

3.11.3.12. Deve implementar mecanismo para otimização de roaming entre pontos de acesso.

3.11.3.13. Implementar, pelo menos, os seguintes padrões de segurança wireless: (WPA) Wi-Fi Protected Access, (WPA2) Wi-Fi Protected Access 2, (WPA3) Wi-Fi Protected Access 3, (AES) Advanced Encryption Standard, (TKIP) Temporal Key Integrity Protocol, PSK privada (por usuário), IEEE 802.1X, IEEE 802.11i.

3.11.3.14. Deverá suportar MLO (Multi-Link Operation) e Preamble Puncturing.

3.11.3.15. Deverá permitir a criação de listas de controle de acesso de Camada 3 e 4 do modelo OSI.

3.11.3.16. Deverá ser possível criar políticas de controle com base no tipo ou sistema operacional do dispositivo.

3.11.3.17. Deve permitir habilitar e desabilitar a divulgação do SSID.

3.11.3.18. Deverá implementar autenticação de usuários usando portal de captura.

3.11.3.19. Deve implementar autenticação de usuários usando WISPr e Hotspot 2.0.

3.11.3.20. Deve suportar conversão de tráfego multicast para unicast.

3.11.3.21. Permitir a configuração e gerenciamento direto através de navegador padrão (HTTPS), SSH, SNMPv2c, SNMPv3 ou através do controlador, a fim de se garantir a segurança dos dados.

3.11.3.22. Deve suportar o protocolo LLDP.

3.11.3.23. Permitir que sua configuração seja realizada automaticamente quando este for conectado ao controlador WLAN do mesmo fabricante.

3.11.3.24. Implementar funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, das políticas de segurança, QoS, autenticação e monitoramento de RF.

3.11.3.25. Permitir que o processo de atualização de software seja realizado manualmente através de interface Web, FTP ou TFTP e automaticamente através de controlador WLAN do mesmo fabricante.

3.11.3.26. Deve permitir a formação de grupo de Pontos de Acesso gerenciados em modo cluster, sem necessidade de controlador WLAN dedicado, onde o próprio Ponto de Acesso atua como controlador e gerenciador dos outros APs do grupo. Nesse modo, deve permitir o gerenciamento de grupo de no mínimo 100 (cem) pontos de acesso que se comuniquem e compartilhem das mesmas configurações.

3.12. PONTO DE ACESSO - TIPO 4

3.12.1. ESPECIFICAÇÕES GERAIS

3.12.1.1. Deverá ser do mesmo fabricante do controlador WLAN para fins de compatibilidade.

3.12.1.2. Deverá possuir estrutura que permita a utilização do equipamento em locais internos, com fixação em teto e parede, devendo ser fornecidos todos os acessórios necessários para estas montagens.

3.12.1.3. Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto, com data anterior à publicação do edital, conforme a resolução 242. Não serão aceitos protocolos de entrada ou outros documentos diferentes do certificado, uma vez que os mesmos não garantem o fornecimento de equipamentos homologados e em conformidade com as leis brasileiras.

3.12.1.4. Deve ser compatível com o padrão UL2043, que regula os componentes dos materiais com o intuito de proteger contra danos causados por fogo, bem como pela fumaça.

3.12.1.5. Suportar, no mínimo, 700 (setecentos) usuários wireless simultâneos, sem nenhum tipo de licença adicional.

3.12.1.6. Possuir suporte a pelo menos 32 (trinta e dois) SSIDs por ponto de acesso.

3.12.1.7. Possibilitar alimentação elétrica local via fonte de alimentação DC e via padrão PoE (IEEE 802.3at ou 802.3bt). Ademais, para PoE, a alimentação elétrica deve ocorrer através de uma única interface de rede, sem perda de funcionalidade e de desempenho.

3.12.1.8. Deve suportar temperatura de operação entre 0°C a 50°C.

3.12.1.9. O equipamento ofertado não deverá possuir antenas aparentes externas ao ponto de acesso, evitando desta forma que as mesmas sejam removidas, o que ocasionaria na degradação do desempenho da rede sem fio.

3.12.1.10. Deverá possuir 2 (duas) interfaces ethernet, sendo 1 (uma) multi-gigabit 1/2.5/5 Gbps e 1 (uma) 10/100/1000 Mbps, utilizando conector RJ-45, para conexão à rede local.

3.12.1.11. Deverá possuir um rádio embarcado para IoT, o qual deve ser compatível com BLE e ZigBee, e deverá ter capacidade para Matter & Thread.

3.12.1.12. Deverá dispor de uma porta USB para inserção de módulo IoT compatível com BLE e ZigBee.

3.12.1.13. Deverá possuir LEDs para a indicação do status de operação do ponto de acesso.

3.12.1.14. Deverá ser fornecido com todas as funcionalidades de segurança, incluindo WIDS, e Wi-Fi Mesh habilitadas.

3.12.1.15. Deverá ser fornecido com a versão mais recente de software.

3.12.1.16. Deve ser compatível com IPv4 e IPv6.

3.12.2. Características dos rádios

3.12.2.1. O ponto de acesso deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11ax e IEEE 802.11be, com operação nas frequências de 2.4 GHz, 5 GHz e 6 GHz de forma simultânea.

3.12.2.2. Implementar as seguintes taxas de transmissão com fallback automático: IEEE 802.11b: 1 Mbps à 11 Mbps, IEEE 802.11a e IEEE 802.11g: 6 Mbps à 54 Mbps, IEEE 802.11n: 6.5 Mbps à 300 Mbps, IEEE 802.11ac: 6.5 Mbps à 860 Mbps, IEEE 802.11ax: 4 Mbps à 4800 Mbps e IEEE 802.11be: 4Mbps à 5760 Mbps.

3.12.2.3. Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11ax e IEEE 802.11be, com ganhos de no mínimo 3dBi nas frequências de 2,4GHz, 5GHz e 6GHz.

3.12.2.4. Deverá suportar potência agregada de saída, considerando todas as cadeias MIMO, de, no mínimo, 24 dBm nas frequências de 2,4 GHz, 5 GHz e 6 GHz.

3.12.2.5. Deverá suportar canalização de 20 MHz, 40 MHz, 80 MHz, 160 MHz e 320 MHz.

3.12.2.6. Deverá possuir mecanismo de rádio com suporte a 6 (seis) fluxos espaciais simultâneos, sendo 2x2:2 em 2.4 GHz, 2x2:2 em 5 GHz e 2x2:2 em 6 GHz, para SU-MIMO e MU-MIMO.

3.12.2.7. Deve permitir que o AP opere em MIMO 4x4:4 em 5GHz, mesmo que para isso o AP deva ser configurado em modo dual-band (2.4GHz e 5GHz).

3.12.2.8. Deve permitir ajustes dinâmicos do sinal de rádio frequência para otimizar o tamanho da célula de abrangência do ponto de acesso.

3.12.2.9. Deve possuir capacidade de selecionar automaticamente o canal de transmissão.

3.12.2.10. Deve suportar os padrões IEEE 802.11r, IEEE 802.11k e IEEE 802.11v.

3.12.3. Serviços, segurança e gerenciamento

3.12.3.1. Deve permitir controle e gerenciamento pelo controlador WLAN através de Camada 2 ou 3 do modelo OSI.

3.12.3.2. Deve ser capaz de operar no modo Mesh sem adição de novo hardware ou alteração do sistema operacional, sendo que a comunicação até o controlador pode ser feita via wireless ou pela rede local.

3.12.3.3. Deve suportar auto cura por meio de Mesh em caso de falha da conexão cabeada de dados, bem como permitir que os pontos de acesso gerenciados estabeleçam automaticamente uma rede mesh sem fio.

3.12.3.4. Em caso de falha de comunicação entre os pontos de acesso e o controlador WLAN, os usuários associados à rede sem fio devem continuar conectados com acesso à rede. Além disso, deve ser possível que novos usuários se associem à rede sem fio utilizando autenticação do tipo IEEE 802.1X mesmo que os pontos de acesso estejam sem comunicação com a controladora.

3.12.3.5. Deve suportar, somente por meio do ponto de acesso em conjunto com o controlador de rede sem fio, a identificação e controle de aplicações dos dispositivos clientes conectados ao ponto de acesso, levando em consideração a camada 7 do modelo OSI.

3.12.3.6. Deve suportar a configuração de limite de banda por usuário ou por SSID.

3.12.3.7. Implementar cliente DHCP, para configuração automática de seu endereço IP e implementar também suporte a endereçamento IP estático.

3.12.3.8. Deve suportar VLANs conforme o padrão IEEE 802.1Q.

3.12.3.9. Deve suportar atribuição dinâmica de VLAN por usuário.

3.12.3.10. Deve implementar balanceamento de usuários por ponto de acesso.

3.12.3.11. Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2.4 GHz livre para dispositivos que trabalhem somente nesta frequência.

3.12.3.12. Deve implementar mecanismo para otimização de roaming entre pontos de acesso.

3.12.3.13. Implementar, pelo menos, os seguintes padrões de segurança wireless: (WPA) Wi-Fi Protected Access, (WPA2) Wi-Fi Protected Access 2, (WPA3) Wi-Fi Protected Access 3, (AES) Advanced Encryption Standard, (TKIP) Temporal Key Integrity Protocol, PSK privada (por usuário), IEEE 802.1X, IEEE 802.11i e OWE.

3.12.3.14. Deverá suportar TPM 2.0.

3.12.3.15. Deverá suportar MLO (Multi-Link Operation) e Preamble Puncturing.

3.12.3.16. Deverá permitir a criação de filtros de endereços MAC de forma a restringir o acesso à rede sem fio.

3.12.3.17. Deverá permitir a criação de listas de controle de acesso de Camada 3 e 4 do modelo OSI.

3.12.3.18. Deverá ser possível criar políticas de controle com base no tipo ou sistema operacional do dispositivo.

3.12.3.19. Deve permitir habilitar e desabilitar a divulgação do SSID.

3.12.3.20. Deverá implementar autenticação de usuários usando portal de captura.

3.12.3.21. Deve implementar autenticação de usuários usando WISPr e Hotspot 2.0.

3.12.3.22. Deve suportar conversão de tráfego multicast para unicast.

3.12.3.23. Permitir a configuração e gerenciamento direto através de navegador padrão (HTTPS), SSH, SNMPv2c, SNMPv3 ou através do controlador, a fim de se garantir a segurança dos dados.

3.12.3.24. Deve suportar o protocolo LLDP.

3.12.3.25. Permitir que sua configuração seja realizada automaticamente quando este for conectado ao controlador WLAN do mesmo fabricante.

3.12.3.26. Implementar funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, das políticas de segurança, QoS, autenticação e monitoramento de RF.

3.12.3.27. Permitir que o processo de atualização de software seja realizado manualmente através de interface Web, FTP ou TFTP e automaticamente através de controlador WLAN do mesmo fabricante.

3.12.3.28. Deve permitir a formação de grupo de Pontos de Acesso gerenciados em modo cluster, sem necessidade de controlador WLAN dedicado, onde o próprio Ponto de Acesso atua como controlador e gerenciador dos outros APs do grupo. Nesse modo, deve permitir o gerenciamento de grupo de no mínimo 100 (cem) pontos de acesso que se comuniquem e compartilhem das mesmas configurações.

3.13. PONTO DE ACESSO - TIPO 5

3.13.1. ESPECIFICAÇÕES GERAIS

3.13.1.1. Equipamento de ponto de acesso para rede local sem fio deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax com operação nas frequências de 2.4 GHz e 5 GHz de forma simultânea

3.13.1.2. Deverá ser do mesmo fabricante do Controlador WLAN

3.13.1.3. Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto, com data anterior à publicação do edital, conforme a resolução 242. Não serão aceitos protocolos de entrada ou outros documentos diferentes do certificado, uma vez que os mesmos não garantem o fornecimento de equipamentos homologados e em conformidade com as leis brasileira

3.13.1.4. Possuir antenas internas e integradas com padrão de irradiação omnidirecional, compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax.

3.13.1.5. Não serão aceitos equipamentos com antenas aparentes (externas ao ponto de acesso) que sejam rosqueáveis, permitindo a remoção das antenas

3.13.1.6. Deve suportar potência de saída de no mínimo 22 dBm com operação na frequência 5GHz e de no mínimo 22 dBm com operação na frequência 2.4GHz

3.13.1.7. Deve suportar ganho de antena de no mínimo 2 dBi para 2.4GHz e 3dBi para 5GHz

3.13.1.8. Deverá atender aos padrões IEEE 802.11d e IEEE 802.11h

3.13.1.9. Deverá suportar canalização de 20 MHz, 40 MHz e 80MHz

3.13.1.10. Deverá possuir mecanismo de rádio com suporte à MIMO 2x2 com 2 Spatial Streams

3.13.1.11. Deverá suportar Multi User MIMO (MU-MIMO)

3.13.1.12. Deverá, em conjunto com o controlador de rede sem fio, permitir a análise de espectro do ambiente em modo dedicado ou simultâneo ao fornecimento de serviço aos dispositivos clientes.

3.13.1.13. Deverá suportar meio de direcionamento de sinal para ganho de desempenho

3.13.1.14. Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2,4 GHz livre para dispositivos que trabalhem somente nesta frequência.

3.13.1.15. Deve suportar, em conjunto com o controlador de rede sem fio, a identificação e controle de aplicações dos dispositivos clientes conectados ao ponto de acesso.

3.13.1.16. Deve suportar, em conjunto com o controlador de rede sem fio, a configuração de limite de banda (rate limit) por usuário e por SSID.

3.13.1.17. Deve oferecer suporte ao mecanismo de localização e rastreamento de usuários (Location Based Service)

3.13.1.18. Deverá possuir, no mínimo, 01 (uma) interface IEEE 802.3 10/100/1000 Mbps Base-T Ethernet, auto-sensing, com conector RJ-45, para conexão à rede local fixa.

3.13.1.19. É desejável possuir LEDs para a indicação do status: portas ethernets, rede wireless, gerenciamento via controladora e atividades do equipamento

3.13.1.20. Deverá possuir o padrão de alimentação IEEE 802.3af (PoE) ou IEEE 802.3at (PoE).

3.13.1.21. Deve suportar temperatura de operação entre -20°C a 65°C com PoE ativado

3.13.1.22. Deverá possuir certificação IP67

3.13.1.23. Deverá possuir estrutura que permita a utilização do equipamento em locais internos e externos, com fixação em teto, parede e também em poste e fornecer acessórios para que possa ser feita a fixação

3.13.1.24. Deverá ser fornecido com todas as funcionalidades de segurança instaladas. Não deve haver licença restringindo itens de segurança do equipamento e nem a quantidade de usuários conectados

3.13.1.25. Funcionar via configuração do controlador no modo de MESH (WiFi Mesh) sem adição de novo hardware ou alteração do sistema operacional, sendo a comunicação até o controlador efetuada via wireless ou por pelo menos 02 pontos ethernet conectados ao controlador ou a uma rede local

3.13.1.26. Deverá ser fornecido com todas as licenças para funcionamento em MESH (WiFi Mesh)

3.13.2. GERENCIAMENTO

3.13.2.1. Permitir a configuração e gerenciamento direto através de browser padrão (HTTPS), SSH, SNMPv2c e SNMPv3, ou através do controlador, a fim de garantir a segurança dos dados

3.13.2.2. Permitir gerenciamento através de plataformas de software que sigam padrões SNMPv2c e SNMPv3

3.13.2.3. Implementar funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, das políticas de segurança, QoS, autenticação e monitoramento de RF

3.13.2.4. Permitir que sua configuração seja automaticamente realizada quando este for conectado no ambiente de rede do Controlador WLAN.

3.13.2.5. O ponto de acesso poderá estar diretamente ou remotamente conectado ao controlador WLAN, inclusive via roteamento da camada 3 de rede OSI

3.13.2.6. O ponto de acesso deverá conectar-se ao controlador WLAN através de túnel seguro padrão ou através de protocolo de comunicação seguro que ofereça controle total do equipamento

3.13.2.7. Permitir ajustes dinâmicos de RF modo a otimizar o tamanho da célula de abrangência de RF

3.13.2.8. Permitir que o processo de atualização de versão seja realizado manualmente através da WEB ou FTP ou TFTP e automaticamente através do Controlador WLAN descrito neste documento.

3.13.3. REDE

3.13.3.1. Implementar cliente DHCP, para configuração automática do seu endereço IP e implementar também endereçamento IP estático

3.13.3.2. Deve suportar VLAN seguindo a norma IEEE 802.1q

3.13.3.3. Possuir suporte a pelo menos 30 SSIDs por ponto de acesso

3.13.3.4. Permitir habilitar e desabilitar a divulgação do SSID

3.13.3.5. Possuir capacidade de selecionar automaticamente o canal de transmissão

3.13.3.6. Suportar, no mínimo, 500 (quinhentos) usuários wireless simultâneos

3.13.3.7. Deve suportar limitação de banda por grupo de usuário ou SSID

3.13.3.8. Implementar, pelo menos, os seguintes padrões de segurança wireless:

3.13.3.8.1. (WPA) Wi-Fi Protected Access

3.13.3.8.2. (WPA2) Wi-Fi Protected Access 2

3.13.3.8.3. (WPA3) Wi-Fi Protected Access 3

3.13.3.8.4. (AES) Advanced Encryption Standard

3.13.3.8.5. (TKIP) Temporal Key Integrity Protocol

3.13.3.8.6. IEEE 802.1x

3.13.3.8.7. IEEE 802.11i

3.13.3.9. Implementar as seguintes taxas de transmissão e com fallback automático:

3.13.3.9.1. IEEE 802.11b: 11 Mbps

3.13.3.9.2. IEEE 802.11a e IEEE 802.11g: 54 Mbps

3.13.3.9.3. IEEE 802.11n: 300Mbps

3.13.3.9.4. IEEE 802.11ac: 867Mbps

3.13.3.9.5. IEEE 802.11ax: 1200Mbps

3.13.3.10. Deverá permitir a criação de filtros de MAC address de forma a restringir o acesso à rede wireless

4. GESTÃO DE ATIVOS DE REDE, MONITORAMENTO E SEGURANÇA - REQUISITOS GERAIS:

4.1. Especificações Gerais

4.1.1. A solução deve vir acompanhada de todos os acessórios necessários para sua operacionalização, tais como softwares, licenças, documentações técnicas e manuais que contenham informações suficientes, que possibilite a instalação, configuração e operacionalização da solução.

4.1.2. O controlador WLAN deverá ser do tipo virtual e compatível com os ambientes VMWare 6.7 e superiores, Hyper-V Windows 2016 e 2019, KVM CentOS 7.4 e superiores, AWS, MS Azure ou GCE. O ambiente virtualizado deverá ser disponibilizado em servidor ou servidores da Contratante com as especificações recomendadas pelo fabricante da solução;

4.1.3. Não serão aceitas soluções baseadas nas premissas de pontos de acesso autônomos ou controladores agregados a outros equipamentos, tais como Switches, Firewalls, Roteadores ou até mesmo controlador virtual dentro do próprio ponto de acesso;

4.1.4. Não serão aceitos sistemas implementados em virtualizadores de desktop, tais como Oracle VM VirtualBox ou VMware Workspace;

4.1.5. Deverá ser do mesmo fabricante dos pontos de acesso e switches fornecidos pela Contratada, para fins de compatibilidade e gerenciamento.

4.1.6. Deverá suportar a operação como um cluster (N+1) para prover resiliência e desempenho, podendo o mesmo ser composto por, no mínimo, 2 (dois) controladores e expansível até 4 (quatro) controladores.

4.1.7. Deve ser acompanhado de todos os acessórios necessários para operacionalização da solução, tais como softwares, documentações técnicas e manuais que contenham informações suficientes, que possibilitem a instalação, configuração e operacionalização da solução.

4.1.8. Deve possuir uma arquitetura modular do tipo multi-tenant, permitindo gestão centralizada, mas com acesso independente e isolado para cada domínio.

4.1.9. Deverá suportar pontos de acesso internos e externos nos padrões 802.11a/b/g/n/ac/ax/be.

4.1.10. Deverá suportar switches de camada 2 e camada 3 com densidade de portas de 1GbE até 100GbE.

4.1.11. Deverá possuir suporte a RESTful API compatível com JSON e disponibilizar suporte às funções GET, POST, DELETE, PUT e PATCH.

4.2. Gerenciamento dos Pontos de Acesso

4.2.1. Suportar o gerenciamento de pelo menos 5.000 (cinco mil) Pontos de Acesso na sua capacidade máxima. Caso a solução trabalhe com licenciamento para esse fim, estas deverão ser fornecidas juntamente com cada Ponto de acesso;

4.2.2. Suportar, no mínimo 100.000 (cem mil) dispositivos clientes simultâneos por controlador.

4.2.3. Prover o gerenciamento centralizado dos Pontos de Acesso, suportando versões de firmware diferentes.

4.2.4. Deverá permitir gerenciamento através de Endereço IP, Range de IPs e Sub-Redes pré-configuradas

4.2.5. Permitir a configuração total dos pontos de acesso, assim como os aspectos de segurança da rede wireless (WLAN) e Rádio Frequência (RF)

4.2.6. O controlador WLAN poderá estar diretamente e/ou remotamente conectado aos Pontos de Acesso por ele gerenciados, inclusive via roteamento em camada 3 do modelo OSI

4.2.7. Possibilitar a configuração de envio dos eventos do Controlador WLAN para um servidor de Syslog remoto

4.2.8. Implementar, pelo menos, os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps SNMP

4.2.9. Permitir a visualização de alertas da rede em tempo real

4.2.10. Implementar, no mínimo, dois níveis de acesso administrativo ao equipamento (apenas leitura e leitura/escrita) protegidos por senhas independentes

4.2.11. Permitir a customização do acesso administrativo através de atribuição de grupo de função do usuário administrador

4.2.12. Permitir a configuração e gerenciamento através de navegador padrão (HTTPS).

4.2.13. Gerenciar de forma centralizada a autenticação de usuários

4.2.14. Permitir o envio de alertas ou alarmes através do protocolo SMTP, sendo que a comunicação com o servidor deverá ser autenticada e cifrada (SMTP/TLS)

4.2.15. Permitir que o processo de atualização de versão seja realizado através de navegador padrão (HTTPS) ou SSH.

4.2.16. Deverá possuir a capacidade de importação de certificados digitais emitidos por uma autoridade certificadora externa;

4.2.17. A disponibilidade da rede sem fio deve ser passível de agendamento para, no mínimo, as opções a seguir:

4.2.17.1. 24 horas por dia, 7 dias na semana

4.2.17.2. Agendamento customizado permitindo escolher os dias da semana e horários

4.2.17.3. Os horários definidos não precisam ser sequenciais, ou seja, a solução deve suportar que o administrador defina o horário de funcionamento das 08:00 às 12:00 e 14:00 às 18:00.

4.2.18. Possuir ferramentas de diagnóstico e log de eventos para depuração e gerenciamento em primeiro nível.

4.2.19. Possuir ferramenta que permite o monitoramento em tempo real de informações de utilização de CPU, memória e estatísticas de rede

4.2.20. Possibilitar cópia “backup” da configuração, bem como a funcionalidade de restauração da configuração através de navegador padrão (HTTPS) ou FTP ou TFTP.

4.2.21. Possuir a capacidade de armazenar múltiplos arquivos de configuração do controlador pertencente à rede sem fio

4.2.22. Monitorar o desempenho da rede sem fio, permitindo a visualização de informações de cada ponto de acesso.

4.2.23. Deve suportar a possiblidade de trabalhar com cluster de controladores WLAN no modo ativo/ativo, com sincronismo automático das configurações entre controladores para suporte a redundância em alta disponibilidade (HA - high availability). Não há necessidade de ofertar a solução de cluster redundantes nesse certame. O cluster deve ter suporte as seguintes funcionalidades:

4.2.24. Deverá suportar o compartilhamento de recursos e licenças de pontos de acesso entre os controladores participantes do cluster.

4.2.25. Deverá, em caso de falha, suportar a redundância de forma automática e sem nenhuma necessidade de intervenção do administrador de rede

4.2.26. Deverá possuir a capacidade de geração de informações ou relatórios de, no mínimo, os seguintes tipos: Listagem de clientes Wireless, Listagem de Pontos de Acesso, utilização da rede.

4.2.27. Deverá suportar, somente por meio do controlador e do ponto de acesso, a identificação de aplicações dos clientes conectados com base na camada 7 do modelo OSI, permitindo o controle de acesso, de banda (uplink e/ou downlink) e definição de regra de QoS para estas aplicações.

4.2.28. Permitir visualizar a localização dos pontos de acesso e através desta obter o status de funcionamento dos mesmos.

4.2.29. Deverá possibilitar a importação de plantas baixas nos formatos DWG ou JPG ou PNG, devendo permitir a visualização dos Pontos de Acesso instalados com seu estado de funcionamento, bem como disponibilizar uma visualização da cobertura do sinal em 2.4GHz, 5GHz ou 6GHz.

4.2.30. Deve ser capaz de localizar clientes wireless na planta baixa adicionada no sistema;

4.2.31. Implementar funcionalidade de análise espectral, permitindo a detecção de interferências no ambiente de rede sem fio.

4.2.32. Implementar análise de tráfego por WLAN, Ponto de acesso e dispositivos cliente, apresentando os 10 itens mais usados.

4.2.33. Deve ser possível definir o nível de segurança administrativo da solução suportando, no mínimo:

4.2.33.1. Habilitar Captcha para Acesso

4.2.33.2. Período em dias para alteração obrigatória da senha

4.2.33.3. Política para reutilização de senha

4.2.33.4. Comprimento mínimo da senha e complexidade

4.2.33.5. Segundo Fator de Autenticação via SMS

4.2.34. A solução deve suportar a adição de um serviço de SMS externo, tal como Twilio.

4.2.35. Implementar funcionalidade de análise espectral em tempo real e por frequência, 2.4GHz ou 5GHz permitindo a detecção de interferências e geração de gráficos de uso do ambiente de rede sem fio;

4.2.36. Deve suportar integração com tags da Ekahau e AeroScout/Stanley para Real-Time Location Service (RTLS);

4.3. REDE

4.3.1. Deverá implementar suporte aos protocolos IPv4 e IPv6

4.3.2. Deverá suportar tagging de VLANs

4.3.3. Implementar associação dinâmica de usuário a VLAN com base nos parâmetros da etapa de autenticação via IEEE 802.1x.

4.3.4. Suportar associação dinâmica de ACL e de QoS por usuário, com base nos parâmetros da etapa de autenticação.

4.3.5. Deverá suportar, no mínimo, 1030 (mil e trinta) SSIDs simultâneos

4.3.6. Deverá possuir funcionalidade de balanceamento de carga entre VLANs e permitir que clientes sejam designados para diferentes VLANs dentro de um mesmo SSID, com suporte a até 50 VLANs por pool.

4.3.7. Em caso de falha de comunicação entre os pontos de acesso e a controladora, os usuários associados à rede sem fio devem continuar conectados com acesso à rede. Também deve permitir que novos usuários se associem à rede sem fio utilizando autenticação do tipo 802.1X mesmo que os pontos de acesso estejam sem comunicação com a controladora

4.3.8. Deve ser possível evitar que dispositivos 802.11b se conectem a rede, visando melhorar o desempenho da rede sem fio.

4.3.9. Deve suportar 802.11d e 802.11k.

4.3.10. Deve suportar captura de pacotes por ponto de acesso para resolução de problemas, sendo possível definir a captura nos rádios de 2.4 GHz, 5 GHz e 6GHz, bem como na interface LAN. Ainda, a operação deve ser realizada via interface Web e deve ser possível exportar o arquivo de captura para análise local em software de análise de pacote, tal como Wireshark.

4.3.11. Deve ser possível rastrear a conexão de um cliente wireless em tempo real para analisar problemas de conectividade e identificar em qual estágio o problema aconteceu.

4.3.12. Deve ser possível estabelecer um limite para o nível de sinal visando permitir que o cliente se junte à rede sem fio, o qual deve ser estabelecido em dBm e variar entre -60dBm e -90dBm.

4.3.13. Deverá suportar de forma centralizada a configuração de agregação de portas (LACP) ethernet dos pontos de acesso que possuírem suporte a essa funcionalidade.

4.3.14. Deve suportar autoconfiguração e autocorreção para rede Mesh.

4.4. SEGURANÇA WLAN

4.4.1. Os itens a seguir devem estar integrados a solução ofertada, não serão aceitos equipamentos externos à solução. Caso sejam necessárias licenças ou softwares de controle os mesmos devem ser fornecidos de forma que a solução esteja operacional e sem nenhuma restrição no ato de sua implementação (hardware e softwares necessários para implementação)

4.4.2. Implementar, pelo menos, os seguintes padrões e funcionalidades de segurança wireless:

4.4.2.1. (WPA) Wi-Fi Protected Access;

4.4.2.2. (WPA2) Wi-Fi Protected Access 2;

4.4.2.3. (WPA3) Wi-Fi Protected Access 3;

4.4.2.4. (TKIP) Temporal Key Integrity Protocol;

4.4.2.5. (AES) Advanced Encryption Standard;

4.4.2.6. PSK (pre-shared key) único por dispositivo cliente em um mesmo SSID;

4.4.2.7. IEEE 802.1X;

4.4.2.8. IEEE 802.11i;

4.4.2.9. IEEE 802.11w.

4.4.3. Implementar, pelo menos, os seguintes controles/filtros:

4.4.3.1. Baseado em endereço MAC e isolamento de cliente na camada 2 do modelo OSI;

4.4.3.2. Baseado em endereço IP;

4.4.3.3. Baseado em protocolo, tais como TCP, UDP, ICMP e IGMP;

4.4.3.4. Baseado em porta de origem e/ou destino;

4.4.3.5. Baseado em tipo ou sistema operacional do dispositivo.

4.4.4. Permitir a autenticação para acesso dos usuários conectados nas redes WLAN (Wireless) através:

4.4.4.1. MAC Address;

4.4.4.2. Autenticação Local;

4.4.4.3. Captive Portal;

4.4.4.4. Active Directory;

4.4.4.5. RADIUS;

4.4.4.6. IEEE 802.1x;

4.4.4.7. LDAP.

4.4.5. Deverá permitir a seleção/uso de servidor RADIUS específico com base no SSID.

4.4.6. Deverá suportar servidor de autenticação RADIUS redundante. Isto é na falha de comunicação com o servidor RADIUS principal, o sistema deverá buscar um servidor RADIUS secundário.

4.4.7. A solução deverá suportar a criação de uma zona de visitantes, que terá seu acesso controlado através de senha cadastrada internamente, sendo que esta deverá possuir configuração de tempo pré-determinado de acesso a rede s/ fio.

4.4.8. O controlador deverá permitir a criação de múltiplos usuários visitantes (guests) de uma única vez (em lote).

4.4.9. Deve ser possível definir o período de validade da senha de visitantes em quantidade de horas, dias e semanas.

4.4.10. Deve permitir que após o processo de autenticação de usuários visitantes (guests) os mesmos sejam redirecionados para uma página de navegação específica e configurável.

4.4.11. Deve permitir que múltiplos usuários visitantes (guests) compartilhem a mesma senha de acesso à rede.

4.4.12. Deverá dispor de opção para enviar a senha de usuários visitantes (guests) por e-mail ou por SMS.

4.4.13. Deverá permitir que um usuário visitante se cadastre automaticamente através de funcionalidade do tipo “self registration”.

4.4.14. Deverá permitir o encaminhamento do tráfego de saída de usuários visitantes (guests) diretamente para a Internet, de forma totalmente separada do tráfego da rede corporativa.

4.4.15. Deve implementar login social com no mínimo, Linkedin, Google, Microsoft e Facebook.

4.4.16. Deverá permitir o isolamento do tráfego unicast, multicast ou ambos entre usuários visitantes (guests) em uma mesma VLAN/Subnet, sendo possível adicionar exceções com base em endereços MAC e IP.

4.4.17. Deverá ser possível permitir que o ponto de acesso filtre todo o tráfego IPv4 e IPv6 dos tipos multicast e broadcast dos clientes sem fio associados, com exceção de alguns tráfegos pertencentes a uma lista de exclusões, tais como ARP, DHCPv4 e DHCPv6, MLD, IGMP, IPv6 NS, IPv6 NA, IPv6 RS e todos pacotes do tipo unicast.

4.4.18. Deverá ser possível especificar o tipo de serviço Bonjour que será permitido entre VLANs.

4.4.19. Deve suportar mecanismo de acesso de acordo com o padrão Hotspot 2.0

4.4.20. Deve implementar mecanismos de segurança e proteção da rede sem fio contemplando, no mínimo, os recursos abaixo:

4.4.20.1. SSID Spoofing – Detectar APs não pertencentes ao controlador propagando o mesmo SSID;

4.4.20.2. MAC Spoofing – Detectar APs não pertencentes ao controlador propagando o mesmo MAC de um AP válido;

4.4.20.3. Rogue APs – Detectar APs não pertencentes ao controlador;

4.4.20.4. Same Network – Detectar APs não pertencentes ao controlador exibindo qualquer SSID pertencentes ao mesmo segmento de rede LAN;

4.4.20.5. Ad Hoc – Possibilidade de detectar rede Ad Hoc como Rogue;

4.4.20.6. Flood de Deauthentication – Detectar quando há um número excessivo de frames de desautenticação oriundos de um mesmo transmissor;

4.4.20.7. Flood de Disassociation – Detectar quando há um número excessivo de frames de desassociação oriundos de um mesmo transmissor;

4.4.20.8. Excesso de Clear to Send (CTS) – Detectar quando há um número excessivo de frames de CTS para um endereço MAC específico;

4.4.20.9. Excesso de Request to Send (RTS) – Detectar quando há um número excessivo de frames de RTS para um endereço MAC específico;

4.4.20.10. Excesso de Energia – Possibilidade de detectar tráfego com nível de potência de transmissão excessivo;

4.4.20.11. Deve implementar varredura de rádio frequência para identificação de ataques e Pontos de Acesso intrusos não autorizados (rogues);

4.4.20.12. Deve fazer a varredura no canal de operação do Ponto de Acesso sem impacto na performance da rede WLAN;

4.4.20.13. Deve utilizar os Pontos de Acesso para fazer a monitoração do ambiente Wireless procurando por pontos de acesso do tipo rogue de forma automática;

4.4.20.14. Deve ser possível especificar um ponto de acesso ou grupo de pontos de acesso para atuarem somente com a função de monitoramento visando detectar ataques e analisar o ambiente de rádio frequência;

4.4.20.15. Deverá ser capaz de localizar Pontos de Acesso do tipo rogue na planta baixa adicionada ao sistema com informações de, no mínimo:

4.4.20.15.1. Pontos de Acesso que detectam;

4.4.20.15.2. Tipo de Rogue;

4.4.20.15.3. Nome da Rede;

4.4.20.15.4. Nível de sinal de detecção.

4.5. RECURSOS DE GERENCIAMENTO AUTOMÁTICO DE RÁDIO FREQUÊNCIA (RF)

4.5.1.1. Na ocorrência de inoperância de um Ponto de Acesso, o controlador WLAN deverá ajustar automaticamente a potência dos Pontos de Acesso adjacentes, de modo a prover a cobertura da área não assistida.

4.5.1.2. Ajustar automaticamente a utilização de canais de modo a otimizar a cobertura de rede e mudar as condições de RF baseado em desempenho.

4.5.1.3. Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura de RF de forma automática.

4.5.1.4. Implementar sistema automático de balanceamento de carga para associação de clientes entre Pontos de Acesso próximos para otimizar o desempenho.

4.5.1.5. Implementar funcionalidade de balanceamento de carga entre os rádios de um mesmo Ponto de Acesso.

4.5.1.6. Permitir que o serviço wireless seja desabilitado de determinado ponto de acesso. Também deve ser possível selecionar o serviço de qual rádio (banda) de determinado ponto de acesso deve ser desabilitado.

4.6. RECURSOS DE CONVERGÊNCIA E MULTIMÍDIA

4.6.1.1. Suportar 802.11e

4.6.1.2. Deverá possuir funcionalidade de configuração do limite de banda disponível por usuário ou através de SSID/BSSID.

4.6.1.3. Deverá permitir a configuração de prioridade de um determinado SSID sobre outros SSIDs existentes na controladora.

4.6.1.4. Deve suportar WiFi Calling.

4.7. GERENCIAMENTO DOS SWITCHES

4.7.1.1. Deverá ser do mesmo fabricante dos Switches fornecidos neste certame, para fins de compatibilidade;

4.7.1.2. Suportar e gerenciar pelo menos 1000 (mil) switches na sua capacidade máxima. Caso a solução trabalhe com licenciamento para esse fim, estas deverão ser fornecidas juntamente com cada Switch;

4.7.1.3. Deve ser possível gerenciar Switches com perfis de Camada 2 e Camada 3.

4.7.1.4. Deve ser capaz de gerenciar todos os switches fornecidos neste certame.

4.7.1.5. Deve ser possível criar grupos lógicos de switches para facilitar a gestão.

4.7.1.6. Deve ser possível associar um switch automaticamente com um respectivo grupo de switches por meio de regras de registro, as quais devem ser definidas por, pelo menos, um dos meios a seguir: faixa de endereço IP, sub-rede ou modelo do switch.

4.7.1.7. Deve realizar backup da configuração dos switches diariamente, mantendo, no mínimo, um histórico das últimas 7 (sete) versões de arquivos de configurações.

4.7.1.7.1. A configuração só deve ser armazenada se houver alguma alteração entre o último backup e o backup atual.

4.7.1.8. Deve ser possível executar um backup manual.

4.7.1.9. Deve suportar a restauração de um determinado backup.

4.7.1.10. Deve dispor de uma opção para visualizar um determinado arquivo de configuração, bem como permitir analisar as diferenças entre arquivos de configurações distintos realçando-as para fácil identificação.

4.7.1.11. Deve permitir a atualização de firmware dos switches de modo individual e em grupos, bem como manter o histórico das atualizações de cada switch.

4.7.1.12. Deve permitir o agendamento de atualização de firmware dos switches de modo individual e em grupos.

4.7.1.13. Deve ser possível definir configurações comuns a um grupo de switches, tais como configurações de DNS e AAA (Authentication, Authorization e Accounting).

4.7.1.13.1. As configurações de AAA devem permitir habilitar ou desabilitar a autenticação, autorização e accounting para SSH ou Telnet, incluindo a seleção da ordem de preferência dos servidores AAA.

4.7.1.13.2. Para autenticação, deve ser possível definir servidor Radius, TACACS+ e usuário local.

4.7.1.13.3. Para autorização e accounting, deve ser possível definir servidor Radius e TACACS+.

4.7.1.14. Deverá possibilitar a criação de Listas de Controle de Acesso (ACL) do tipo padrão ou estendida e permitir a definição de quando a configuração deve ser aplicada no switch, se imediatamente ou por meio de agendamento.

4.7.1.15. Deverá permitir a criação de VLANs, permitindo atribuir um nome a esta VLAN, bem como definir quais portas devem ser untagged ou tagged.

4.7.1.16. Deve ser possível configurar DHCP Snooping, ARP Inspection e IP Source Guard.

4.7.1.17. Deve ser possível configurar IGMP Snooping Ativo ou Passivo.

4.7.1.18. Deve suportar configurações de Spanning Tree, tais como permitir definir entre STP (802.1d) ou RSTP (802.1w) e sua respectiva prioridade.

4.7.1.19. Deverá ser possível criar rotas estáticas e permitir a definição de quando a configuração deve ser aplicada no switch, se imediatamente ou por meio de agendamento.

4.7.1.20. Deve disponibilizar um histórico das configurações criadas, demonstrando o tipo de configuração, a data e o período em que foram criadas, bem como se a mesma foi implementada com sucesso ou se houve alguma falha.

4.7.1.21. Deve ser possível definir um hostname para cada switch.

4.7.1.22. Deve ser possível habilitar Jumbo Frame.

4.7.1.23. Deve suportar DHCP Server e DHCP Relay.

4.7.1.24. Deve dispor de funcionalidade para copiar configurações de um determinado switch para um ou mais switches.

4.7.1.25. Deve ser possível criar LAGs (Link Aggregation Group) do tipo estático ou dinâmico.

4.7.1.26. Deve ser possível criar empilhamento de switches.

4.7.1.27. Deve ser possível habilitar ou desabilitar uma porta, bem como definir um nome para cada porta.

4.7.1.28. Deve ser possível habilitar ou desabilitar PoE, bem como definir a classe ou prioridade PoE.

4.7.1.29. Deve ser possível definir configurações de camada 3 para uma porta como, por exemplo, área OSPF e endereço IP.

4.7.1.30. Deve permitir a visualização de alarmes relacionados ao switch, incluindo, mas não se limitando a: falha de uma fonte de alimentação, falha de um membro do empilhamento ou falha na alocação de PoE.

4.7.1.31. Deve permitir a detecção e visualização de eventos relacionados ao switch com base em certas condições, bem como permitir o envio de notificações por E-mail e Traps SNMP.

4.7.1.32. Deve ser possível criar eventos customizados, podendo definir o texto que um evento deve conter, condição em quantidade de vezes, janela de tempo em horas e severidade.

4.7.1.33. Deve dispor de painel gráfico com o estado das portas dos switches.

4.7.1.34. Deve disponibilizar um detalhamento das portas de um switch demonstrando, no mínimo, o nome da porta, o estado da porta (UP/DOWN), o estado administrativo da porta (UP/DOWN), a velocidade, a utilização de PoE para portas PoE, a utilização de banda (in/out), total de pacotes multicast (in/out), total de pacotes broadcast (in/out), número de pacotes com erro (in/out), erros de CRC e número de pacotes inbound descartados.

4.7.1.35. Deve disponibilizar graficamente a visão do painel frontal de um determinado switch permitindo visualizar, no mínimo, as seguintes informações de uma determinada porta: nome da porta, estado da porta (UP/DOWN), VLANs Untagged e Tagged, e, para portas PoE, a utilização de PoE.

4.7.1.36. Deve disponibilizar uma visão da topologia dos dispositivos gerenciados.

4.7.1.37. Deve possuir painéis demonstrando o volume de tráfego total para todos os switches ou para os switches de um grupo, bem como listar os principais switches do sistema por volume de tráfego, por erro de porta e por utilização de PoE.

4.7.1.38. Deve monitorar a utilização da CPU, da memória e estado da fonte de alimentação dos switches.

4.7.1.39. Deve permitir o monitoramento da temperatura de operação dos switches.

4.7.1.40. Deve ser possível visualizar os equipamentos vizinhos conectados ao switch, incluindo nome do dispositivo, endereço MAC, tipo do dispositivo e a partir de qual porta física do switch esse dispositivo vizinho pode ser encontrado.

4.7.1.41. Deve dispor de operações remotas para auxílio na resolução de problemas suportando, pelo menos, Ping e Traceroute.

4.7.1.42. Deve dispor de uma ferramenta para análise da conectividade do cliente por meio da inserção do endereço MAC do dispositivo final.

4.8. Monitoramento

4.8.1. Requisitos e Manutenção

4.8.2. Coleta de dados, detecção de eventos e geração de alertas.

4.8.3. Monitorar os ativos de rede por meio de SNMP (v2/v3), ICMP e outros protocolos relevantes.

4.8.4. Capacidade de monitoramento de no mínimo a quantidade total de ativos simultâneos informados no *Quadro 01* do Anexo I – Termo de Referência.

4.8.5. Implementação de triggers e actions para geração de alertas personalizados.

4.8.6. Gerar relatórios minimamente em PDF, CSV e Excel.

4.8.7. Monitorar os logs dos dispositivos, e gerar alertas com base nas informações dos logs.

4.8.8. Criar dashboards com gráficos e tabelas para facilitar a análise do desempenho da rede.

4.8.9. Implementação de dashboards específicos para cada tipo de ativo (pontos de acesso wifi e switches).

4.8.10. Coleta de métricas como latência, perda de pacotes, utilização de CPU, memória, temperatura e consumo de energia (quando disponível nos dispositivos).

4.8.11. Alertas configuráveis baseados em thresholds de desempenho.

4.8.12. Suporte a MIBs específicas dos fabricantes dos switches e pontos de acesso Wi-Fi.

4.8.13. A solução de monitoramento deve ser escalável para suportar o crescimento da rede.

4.8.14. A solução de monitoramento deve ser segura, com controle de acesso e criptografia de dados.

4.8.14.1. Monitoramento contínuo da disponibilidade e desempenho dos ativos de rede.

4.8.14.2. Acompanhamento do consumo de largura de banda, taxa de erro, tempo de resposta e utilização de CPU/memória dos dispositivos monitorados.

4.8.14.3. Identificação e registro de incidentes de conectividade e desempenho.

4.8.14.4. Atualização periódica de templates e ajustes em configurações conforme necessário.

4.8.14.5. Geração de dashboards dinâmicos e relatórios.

4.8.14.6. Configuração de agentes SNMP e ICMP para coleta de dados de switches e pontos de acesso WiFi.

4.8.14.7. Definição de templates e criação de triggers para alertas automáticos baseados em métricas predefinidas.

4.8.14.8. Configuração de notificações via e-mail, Telegran ou outras plataformas para alertas de falhas.

4.8.15. Geração de Relatórios e Dashboards

4.8.15.1. Criação de dashboards customizados para visualização em tempo real do estado dos ativos.

4.8.15.2. Emissão de relatórios gerenciais com estatísticas de disponibilidade, desempenho e incidentes.

4.8.15.3. Histórico de alertas e eventos.

4.8.16. Ativos a Serem Monitorados

4.8.16.1. Pontos de Acesso Wi-Fi

4.8.16.1.1. Disponibilidade (online/offline)

4.8.16.1.2. Número de clientes conectados

4.8.16.1.3. Tráfego de dados (upload/download)

4.8.16.1.4. Taxa de erros

4.8.16.1.5. Utilização de CPU e memória

4.8.16.2. Switches

4.8.16.2.1. Disponibilidade (online/offline)

4.8.16.2.2. Tráfego de dados em cada porta

4.8.16.2.3. Taxa de erros em cada porta

4.8.16.2.4. Utilização de CPU e memória

4.8.16.2.5. Status de VLANs

4.8.16.2.6. Status de Spanning Tree

4.9. Segurança

4.9.1. Deve realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance) em todos os componentes da infraestrutura de rede sem fio.

4.9.2. Deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede, incluindo pontos de acesso, switches e dispositivos conectados.

4.9.3. Deve suportar varreduras de vulnerabilidades de dispositivos de IoT conectados à infraestrutura sem fio.

4.9.4. Poderá fornecer um modelo de armazenamento integrado que não dependa de um banco de dados externos ou de terceiros. Caso o armazenamento dependa de banco de dados de terceiros, todas as licenças deverão ser fornecidas pela Contratada.

4.9.5. Deverá suportar API (Application Programming Interface) baseada em REST (Representatonal State Transfer) para automação de processos e integração com aplicações terceiras.

4.9.6. Deve possuir integração via API no mínimo com as seguintes linguagens: Python, PowerShell, Ruby, Javascript, Java, Swift e PHP.

4.9.7. Deve possuir métodos de consulta via API e envio, tais como: HTTP METHOD (POST, GET, PUT e DELETE).

4.9.8. Deve permitir o agrupamento de scanners para facilitar o gerenciamento e aplicação de políticas em diferentes localidades da rede sem fio.

4.9.9. O acesso à console de gerenciamento deve ser fornecido para pelo menos 10 usuários simultâneos.

4.9.10. Deve ser capaz de se integrar e disponibilizar insumos para soluções de correlação de eventos externa (SIEM).

4.9.11. Deve apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para correção.

4.9.12. Deve apresentar, para cada vulnerabilidade encontrada, evidências da vulnerabilidade através de saídas das verificações (outputs).

4.9.13. Deve fornecer controle de acesso baseado em função (RBAC - Role Based Access Control) para controlar o acesso do usuário a conjuntos de dados e funcionalidades.

4.9.14. Deve ser capaz de definir e gerenciar grupos de usuários, incluindo limitação de funções de varreduras e acesso a relatórios e dashboards.

4.9.15. Deve ter a capacidade de excluir determinados endereços IP ou dispositivos sem fio do escopo de qualquer varredura ou scan.

4.9.16. Deve criptografar todos resultados de varreduras obtidos e informações inseridas tanto em descanso quanto em trânsito.

4.9.17. Deve suportar métodos de autenticação usando bases de autenticação local, e SAML (Security Assertion Markup Language) para uso de SSO (Single Sign-On).

4.9.18. Deve ser capaz de orquestrar scanners ilimitados dentro da infraestrutura de rede sem fio.

4.9.19. Não deve impor nenhum limite de quantidade de scanners implementados dentro da infraestrutura.

4.9.20. Deverá possuir sistema de alertas para informar a disponibilidade de resultados dos escaneamentos através de e-mail.

4.9.21. Deve oferecer capacidade de configuração dinâmica de grupos de ativos através de no mínimo as seguintes características:

4.9.21.1. Endereço IP, DNS, NetBIOS Host e MAC

4.9.22. Deverá possuir painéis gerenciais (dashboards) pré-definidos para rápida visualização dos resultados, permitindo ainda a criação de painéis personalizados.

4.9.23. Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento.

4.9.24. Os relatórios devem ser disponibilizados sob demanda no console de gerência da solução.

4.9.25. Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um exploit disponível e informações do ativo na infraestrutura sem fio.

4.9.26. Deve permitir a customização de dashboards/relatórios específicos para a infraestrutura de rede sem fio.

4.9.27. Deve concentrar todos os relatórios na plataforma central de gerenciamento, não sendo aceitas soluções fragmentadas.

4.9.28. Deve ser capaz de produzir relatórios, pelo menos, nos seguintes formatos: HTML, PDF e CSV.

4.9.29. Deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e alvos específicos da rede sem fio.

4.9.30. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável).

4.9.31. Deve suportar o envio automático de relatórios para destinatários específicos.

4.9.32. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual.

4.9.33. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos.

4.9.34. Deve suportar varredura com ou sem agente, de maneira ativa e passiva, distribuídas em diferentes localidades e regiões da rede sem fio e gerenciar todos por uma console central.

4.9.35. Deve ser configurável para permitir a otimização das configurações de varredura, minimizando o impacto na performance da rede sem fio.

4.9.36. Deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux.

4.9.37. Deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo.

4.9.38. Deve suportar o agendamento de scans personalizados, incluindo a capacidade de executar varreduras em tempos designados, com frequência pré-determinada.

4.9.39. Deve ser capaz de identificar novos hosts no ambiente sem fio sem a necessidade de scan.

4.9.40. Deve possuir recurso de monitoria passiva do tráfego de rede sem fio para identificação de anomalias, novos dispositivos e desvios de padrões observados.

4.9.41. Ser capaz de identificar a comunicação de malwares na rede sem fio de forma passiva.

4.9.42. Deve em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede através da infraestrutura sem fio.

4.9.43. Deve ser capaz de exibir ambos severidade e pontuação, com base em CVSS (Common Vulnerability Scoring System) e inteligência de ameaças.

4.9.44. Deve utilizar sistema de pontuação e priorização das vulnerabilidades que utilize no mínimo:

4.9.44.1. CVSS Impact Score

4.9.44.2. Idade da Vulnerabilidade

4.9.44.3. Maturidade de códigos de exploração da vulnerabilidade encontrada

4.9.44.4. Frequência de uso da vulnerabilidade em ataques e campanhas atuais

4.9.44.5. Disponibilidade do código de exploração da vulnerabilidade

4.9.44.6. Presença de módulos de exploração de vulnerabilidade em frameworks automatizados de exploração de vulnerabilidades como CANVAS, Metasploit e Core Impact

4.9.44.7. Popularidade da vulnerabilidade em fóruns e comunicações na Darkweb

4.9.45. O mecanismo de priorização deve ser sujeito a modificações e atualizações diárias com base em inteligência de ameaças e observação de tendências na Internet.

4.9.46. Deve identificar e priorizar vulnerabilidades específicas dos equipamentos e protocolos de redes sem fio, incluindo vulnerabilidades em protocolos como WPA2, WPA3 e WEP.

4.9.47. Deve detectar configurações inseguras específicas de redes sem fio, como criptografia inadequada, exposição de SSIDs, canais inseguros e outros riscos próprios de ambientes wireless.

5. Acessórios – Transceivers, Cabos e Conectores Injetores PoE

5.1. TRANSCEIVER MULTIMODO

5.2. GERAL

5.2.1. Taxa de Transferência:

5.2.2. Suportar taxas de transferência de até 10 Gigabits por segundo.

5.2.3. Tipo de Fibra: Multimodo:

5.2.4. Alcance:

5.2.5. 300 metros: Em fibras multimodo OM3.

5.2.6. 400 metros: Em fibras multimodo OM4.

5.2.7. Formato: SFP+

5.2.8. LC Duplex: Utiliza conectores LC com uma interface full duplex para a transmissão e recepção de dados.

5.2.9. Hot-pluggable:

5.2.10. Deve ser do mesmo fabricante dos demais equipamentos

5.2.11. Temperatura de Operação: 0°C a 70°C: Operação típica em ambientes controlados.

5.2.12. Normas e Conformidades: IEEE 802.3ae: Conformidade com o padrão 10GBaseSR.

5.2.13. RoHS: Conformidade com a diretiva de restrição de substâncias perigosas.

5.2.14. DDM (Digital Diagnostics Monitoring): Capacidade de monitoramento em tempo real dos parâmetros do transceiver, como temperatura, tensão de alimentação, corrente de polarização do laser, potência óptica transmitida e recebida.

5.3. TRANSCEIVER MONOMODO

5.4. GERAL

5.4.1. Taxa de Transferência:

5.4.2. Suportar taxas de transferência de até 10 Gigabits por segundo.

5.4.3. Tipo de Fibra: Monomodo:

5.4.4. Alcance: 10KM

5.4.5. Formato: SFP+

5.4.6. LC Duplex: Utiliza conectores LC com uma interface full duplex para a transmissão e recepção de dados.

5.4.7. Hot-pluggable:

5.4.8. Deve ser do mesmo fabricante dos demais equipamentos

5.4.9. Temperatura de Operação: 0°C a 70°C: Operação típica em ambientes controlados.

5.4.10. Normas e Conformidades: IEEE 802.3ae: Conformidade com o padrão 10GBaseSR.

5.4.11. RoHS: Conformidade com a diretiva de restrição de substâncias perigosas.

5.4.12. 0DDM (Digital Diagnostics Monitoring): Capacidade de monitoramento em tempo real dos parâmetros do transceiver, como temperatura, tensão de alimentação, corrente de polarização do laser, potência óptica transmitida e recebida.

5.5. CABO DAC

5.6. GERAL

5.6.1. Cabo tipo DAC (Direct Attach Copper) 10Gbps, padrão SFPP para SFPP, com comprimento mínimo de 1m.

5.6.2. Deve ser do mesmo fabricante dos switches.

5.6.3. Transceivers SFP+ no padrão SFP+10G-BASE-T, suportando até 100 (cem) metros, com conectores RJ45 para cabos de rede par metálico CAT5e e/ou 6.

5.6.4. Os transceivers deverão ser plenamente compatíveis com os equipamentos do objeto disposto neste Termo de Referência".

5.7. Características Injetor PoE

5.7.1. Adaptador Power-over-Ethernet (PoE) para produtos com entradas PoE 1,0/2,5/5,0/10,0-BaseT. Classificado para uso em ambientes interiores.

5.7.2. Suporte a até 60W.

5.7.3. (1) Cabo de específico do país, IEC, 6 pés
5.7.4. (1) Módulo PoE (10/ 100/ 1000/ 2500/ 5000/ 10000Mbps)
5.7.5. Entrada: 100-24VCA ~ 50/60Hz 1,2A
5.7.6. Saída: 54VCC 1,12A (60W)
5.7.7. Porta de dados: Entrada RJ-45
5.7.8. Porta PoE/dados: Entrada RJ-45

6. Implementação - Instalação e Configuração

6.1.1. Todos os equipamentos e solução de gestão deverão ser entregues, instalados, configurados e postos em operação em consonância com o projeto aprovado;

6.1.2. Os equipamentos entregues deverão passar por testes de hardware do fabricante para assegurar a conformidade com os requisitos técnicos especificados. Estes testes deverão ser conduzidos e validados pela Contratada nas instalações da USCS, garantindo que o equipamento funcione conforme esperado antes de ser colocado em operação;

6.1.3. Os procedimentos envolvidos nos processos de instalação e configuração deverão ser previamente aprovados pela USCS, de forma a garantir intervalos de paralisação localizados que impactem o mínimo possível as atividades da USCS;

6.1.4. Sempre que a equipe técnica da USCS julgar necessário, ela poderá determinar que os procedimentos de instalação, totalmente ou em partes, sejam realizados em feriados, sábados ou domingos.

6.2. Suporte e Garantia

6.2.1. O suporte técnico da Contratada será iniciado a partir da emissão do Termo de Recebimento Provisório. A Contratada deverá prestar suporte aos elementos da solução por intermédio de sua sede, filiais ou escritórios, estando obrigada a:

6.2.2. Corrigir defeitos de fabricação ou projeto;

6.2.3. A Contratada será obrigada a substituir os equipamentos que apresentarem defeito de fabricação, dentro dos prazos estabelecidos nos demais subitens deste Termo de Referência;

6.2.4. Acondicionar adequadamente os equipamentos cujo reparo não possa ser realizado nas dependências da USCS de forma a permitir sua completa segurança e identificação durante o transporte, responsabilizando-se pela sua remoção e devolução ao local em que deve ser instalado e pelas despesas operacionais decorrentes;

6.2.5. Os custos relativos ao deslocamento de técnicos, transporte de componentes e equipamentos, dentre outros, são de responsabilidade da Contratada;

6.2.6. Detectar problemas e limitações de desempenho da solução relacionados a Software e/ou firmware instalados nos elementos que fazem parte do objeto deste Termo de Referência, substituindo-os por nova versão que implemente suas correções; quando esta implementar correções a possíveis problemas ou limitações de desempenho da solução.

6.2.7. O suporte técnico da Contratada deve estar disponível para abertura de chamados 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, mediante e-mail ou outro sistema de abertura que permita o registro com histórico;

6.2.8. Os chamados deverão ser atendidos por técnico(s) certificado(s)/capacitado(s) pelo fabricante. A comprovação da certificação/capacitação do(s)técnico(s) poderá ser exigida pela USCS a qualquer momento durante prestação do suporte.

6.2.9. O prazo de atendimento inicial inicia-se com a primeira intervenção pelo representante da Contratada, local ou remotamente;

6.2.10. A solução de contorno, se adotada, requererá a aplicação da solução definitiva no prazo a ser estabelecido pela USCS, a depender de cada caso;

6.2.11. O prazo de solução será contabilizado de acordo com o Termo de Referência;

6.2.12. Encaminhar aa USCS relatório contendo descrição do chamado aberto após solucionado, incluindo procedimento de resolução adotado e eventuais informações adicionais que poderão ser executadas para que o problema não se repita;

6.2.13. Excepcionalmente, a critério exclusivo da USCS, mediante justificativa tecnicamente fundamentada que demonstre a impossibilidade de atendimento dos prazos acima, poderá ser concedido prazo adicional à Contratada para resolução de problemas;

6.2.14. O suporte será utilizado para desempenhar as seguintes tarefas:

6.2.15. Prestar todo e qualquer tipo de suporte a todos os elementos integrantes da solução adquirida;

6.2.16. Subsidiar a equipe técnica da USCS na abertura de chamados, através da identificação de imperfeições, vícios, defeitos, incorreções ou excesso de defeitos e diagnóstico de problemas;

6.2.17. Auxiliar a equipe técnica da Contratada na resolução de problemas, fornecendo informações do ambiente e suas particularidades assim como ações adotadas e diagnósticos realizados;

6.2.18. Abrir chamados com o fabricante, caso o problema não seja da alçada de solução da Contratada, interagir, provendo as informações necessárias, até a sua conclusão;

6.2.19. Prestar todo e qualquer tipo de esclarecimento técnico à equipe da USCS, inclusive documentar e repassar os procedimentos de instalação, atualização, administração e configuração da solução, quando solicitados;

6.2.20. Manter sempre atualizado e completo o conjunto de procedimentos operacionais entregues pela Contratada à USCS;

6.2.21. Manter sempre atualizado as rotinas de automação para integração da solução com a gestão de configuração da USCS entregues pela Contratada;

6.2.22. Subsidiar a equipe técnica com dados referentes à solução instalada para que sejam mantidas atualizadas as bases de dados relativas à solução Contratada;

6.2.23. A garantia deverá abranger os elementos da solução pelo período mínimo de vigência do contrato, contados a partir da implementação de todos os equipamentos ou a partir da aprovação do plano de inserção pela USCS, o que ocorrer por último, com todos os custos inclusos;

6.2.24. A garantia deverá abranger todos os equipamentos, softwares, cabos, conectores e demais elementos da solução, conforme especificações do Termo de Referência;

6.2.25. No caso de substituição de peças ou de todo o equipamento, o RMA deverá ocorrer em até 1 dia útil após o diagnóstico de falha em chamado aberto;

6.2.26. A Contratada deverá providenciar permissão de acesso ao sítio do fabricante para acompanhamento pela USCS de chamados, download e acesso a documentações, patches, fixes, firmwares, arquivos de qualquer tipo e/ou qualquer outro material referente à solução.

6.3. Serviço técnico especializado, gestão, monitoramento e segurança da solução

6.3.1. O serviço de suporte operacional especializada deverá garantir a disponibilidade, desempenho e segurança dos switches e pontos de acessos WiFi da instituição, através do monitoramento contínuo de ativos de rede. O serviço deverá contemplar a instalação, configuração, manutenção e suporte técnico da solução, garantindo a disponibilidade e desempenho dos ativos de rede, conforme requisitos especificados no Projeto Básico.

6.3.2. Deverá ser disponibilizado pela Contratada para apoiar as necessidades oriundas dos objetos dos itens deste documento, podendo ser realizado de forma presencial e/ou remota.

6.3.3. Trabalhar em estreita colaboração com a Diretoria de Tecnologia da Informação e Inovação, como equipes de suporte técnico, analistas de rede e equipes de segurança cibernética, para resolver problemas complexos, implementar mudanças e melhorias na infraestrutura de rede da universidade;

6.3.4. Acompanhar o monitoramento e segurança dos ativos de rede, receber alertas e notificações de problemas de rede, como interrupções de serviço e quedas de conexão. Investigar e resolver esses alertas/notificações, garantindo o mínimo de tempo de inatividade e impacto nos serviços;

6.3.5. Realizar verificações regulares de rotina, atualizações de firmware, instalação de patches de segurança e outras atividades para manter a rede em bom estado de funcionamento;

6.3.6. Avaliar novas funcionalidades e sugerir ajustes que possam melhorar a eficiência e a segurança da rede;

6.3.7. Realizar novas instalações, configurações, suporte técnico, manutenções preventivas e corretivas dos softwares e equipamentos (soluções, plataformas, switches e pontos de acessos WiFi);

6.3.8. Reportar e elaborar notas técnicas sobre problemas graves para a DTI;

6.3.9. Criação e acompanhamento no preenchimento de Requisição de Mudança (RDM) na infraestrutura de rede, seguindo os procedimentos de gerenciamento de mudanças estabelecidos pela USCS. Isso envolve a análise de impacto, planejamento, execução e documentação das alterações realizadas;

6.3.10. Monitorar e garantir a segurança e que os Níveis Mínimos de Serviços (NMS) sejam cumpridos;

6.3.11. Colaborar com equipes de projeto para implementar novas soluções de rede, como expansões, migrações ou atualizações tecnológicas.

7. **ATENDIMENTO E SUPORTE DA SOLUÇÃO**

7.1. A Contratada deverá disponibilizar telefone com atendimento mínimo dentro do horário comercial (8:00h às 18:00h) de segunda a sexta-feira para prover a necessidade da Universidade USCS.

7.2. O suporte técnico deverá ser prestado em caso de falhas, dúvidas e/ou esclarecimentos de qualquer um dos produtos, módulos e programas referentes aos componentes da solução.

7.3. Para garantia da qualidade de atendimento a central de atendimento deverá permitir acesso 24 horas através dos canais: portal web, e-mail, telefone e Whatsapp, onde a Contratante possa:

7.3.1. Abrir chamados de atendimento;

7.3.2. Receber numeração do chamado de forma automática;

7.3.3. Acompanhar o andamento do chamado.

8. ETAPAS DO SERVIÇO

8.1. ETAPA 1 – IMPLEMENTAÇÃO

8.1.1. A implementação definida para os itens (1.1.4; 1.2.6 e 1.3.3) se dará respeitando os seguintes aspectos:

8.1.1.1. Os equipamentos que compõe a solução ofertada pela licitante vencedora, devem ser todos entregues em até 45 (quarenta e cinco) dias corridos após a emissão da Ordem de Serviço, na sede da USCS (Campus Barcelona), aos cuidados do gestor do contrato, com respectiva indicação de patrimônio da contratada, bem como com planilha indicativa dos quantitativos dos itens entregues e respectivas características (marca/modelo).

8.1.1.2. No ato do recebimento o gestor irá verificar se os equipamentos recebidos correspondem aos indicados na proposta vencedora, e no mesmo ato atestará o recebimento provisório dos itens.

8.1.1.3. Os equipamentos entregues poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações ou critérios de aceitação, devendo ser substituídos às suas custas, sem prejuízo da aplicação das penalidades cabíveis.

8.1.2. No prazo descrito no item 8.1.1.1. a contratada deverá encaminhar, também, à Diretoria de Tecnologia da Informação e Inovação da USCS, plano de execução (cronograma) contendo informações a respeito do planejamento para implementação da solução.

8.1.3. O plano de execução deverá contemplar obrigatoriamente, os seguintes aspectos:

8.1.3.1. Prazo para implementação dos equipamentos entregues na sede da USCS, que compõe a solução, será de até 45 (quarenta e cinco) dias corridos, a ser iniciado quando da aprovação do plano de inserção até o aceite provisório da etapa de implementação;

8.1.3.2. Prazo para implementação por Campus e/ou prédios/salas/áreas, desde que respeitado o prazo do item anterior;

8.1.3.3. Topologia sugerida para atendimento às necessidades da USCS;

8.1.3.4. Indicar o prazo para validação definitiva de 10 (quinze) dias corridos pela equipe de DTI da Universidade USCS, após o aceite provisório da etapa de implementação.

8.1.4. A implementação da solução será recebida/concluída provisoriamente, conforme plano de inserção, momento em que passará por validação e testes pela Diretoria de Tecnologia da Informação e Inovação da USCS. Após validação, sendo concluído satisfatoriamente será expedido termo de recebimento definitivo da implementação, no prazo de 10 (dez) dias corridos, podendo ser prorrogado por igual período, desde que, por motivo justificado.

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

8.1.4.2. Entregáveis desta etapa:

8.1.4.2.1. Plano de execução;

8.1.4.2.2. Relatório de entrega provisório e definitivo;

8.2. **ETAPA 2 - SUSTENTAÇÃO - SERVIÇO CONTINUADO POR 24 MESES**

8.2.1. Após expedição do termo de recebimento definitivo da etapa de implementação, dará início automaticamente a etapa 2 que terá vigência de 24 (vinte e quatro) meses conforme previsto neste instrumento.

8.2.2. Entregáveis nessa etapa se limita ao relatório mensal.

9. **FORMA DE MEDIÇÃO E PAGAMENTO**

9.1. **ETAPA 1 - IMPLEMENTAÇÃO – Prazo de até 90 dias corridos**

9.1.1. Os valores relativos a etapa de implantação representados pela instalação, configuração e ativação física dos itens descritos como 1.1.1; 1.1.2; 1.1.3; 1.2.1; 1.2.2; 1.2.3; 1.2.4; 1.2.5; 1.3.1 e 1.3.2, após recebimento provisório e emissão do termo de aceite pelo gestor do instrumento de contrato, a contratada deverá emitir nota fiscal que corresponderá aos serviços descritos nos itens 1.1.4, 1.2.6 e 1.3.3 do quadro 01 deste termo de referência, respeitando-se a definição percentual estabelecida no cronograma apresentado pela contratada no ato de entrega física dos equipamentos na sede

da Universidade USCS. O pagamento será efetuado em parcela única, ressalvadas eventuais glosas ou penalidades contratuais.

9.2. **ETAPA 2 - SUSTENTAÇÃO – Serviço Continuado por 24 meses.**

9.2.1. Os valores relativos a esta etapa serão pagos mensalmente, e terão seu início definido após a ativação dos equipamentos, o que corresponde ao momento de emissão do termo de aceite, respeitando-se o cronograma de execução definido entre a Ccontratada e a Universidade Municipal de São caetano do Sul.

10. **CRITÉRIOS DE ACEITAÇÃO**

10.1. A avaliação da qualidade dos produtos entregues, para fins de aceitação, consiste na verificação dos critérios relacionados a seguir:

10.1.1. Todos os equipamentos fornecidos deverão ser novos (incluindo todas as peças e componentes presentes nos produtos), de primeiro uso (sem sinais de utilização anterior), não recondicionados e em fase de comercialização normal através dos canais de venda do fabricante no Brasil (não serão aceitos produtos *end-of-sale e/ou end-of-life).*

10.1.2. Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si, sem a utilização de adaptadores, frisagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos não previstos nas especificações técnicas ou, ainda, com emprego de materiais inadequados ou que visem adaptar forçadamente o produto ou suas partes que sejam fisicamente ou logicamente incompatíveis.

10.1.3. Todos os componentes internos do(s) equipamento(s) deverá(ão) estar instalado(s) de forma organizada e livres de pressões ocasionados por outros componentes ou cabos, que possam causar desconexões, instabilidade, ou funcionamento inadequado.

10.1.4. Serão recusados os equipamentos que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos, sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado como novos pelo fornecedor dos produtos.

10.1.5. Os equipamentos, considerando a marca e modelo apresentados na licitação, não poderão estar fora de linha comercial, considerando a data de implementação e ativação. Os equipamentos devem ser fornecidos completos e prontos para a utilização, com todos os acessórios, componentes, cabos etc.

10.1.6. Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização da contratante, legalizado, não sendo admitidas versões "*shareware*" ou "*trial*". O modelo do produto ofertado pelo licitante deverá estar em fase de produção (no Brasil ou no exterior), com *datasheet* oficial disponibilizado em site oficial do fabricante e sem previsão de encerramento de produção, até a data de entrega da proposta.

11. **NÍVEIS MÍNIMOS DE SERVIÇOS EXIGIDOS - Service Level Agreement SLA**

11.1. Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pela Universidade USCS para aferir objetivamente os resultados pretendidos com a contratação.

11.2. Para a medição dos índices de nível de serviços, serão considerados os seguintes conceitos:

11.2.1. **Incidente:** É uma interrupção não planejada de um serviço de Tecnologia da Informação ou uma redução de qualidade de um serviço de TI;

11.2.2. **Problema:** é a causa desconhecida de um ou mais incidentes ou os problemas são a causa de um ou mais incidentes;

11.2.3. **Severidade:** Solicitações de alteração do nível de severidade poderá ser submetida à Contratada e, quando julgadas pertinentes, serão prontamente atendidas, conforme quadro a seguir.

Severidade	Descrição
Crítica	Indisponibilidade total dos serviços.
Alto	Degradação dos serviços.
Normal	Falha parcial dos serviços.

Quadro 02

11.3. **IMPLEMENTAÇÃO - Serviços de Entrega, Instalação e Configuração da Solução**

11.3.1. Todos os produtos deverão ser entregues nos quantitativos e localidades indicadas, instalados e configurados em conformidade com a especificação, dentro dos prazos máximos estipulados neste Termo, assim como previsto no termo de inserção (cronograma).

11.3.2. Será verificada a conformidade com as especificações técnicas, assim como mensurado o prazo de entrega da solução, conforme detalhamento dos indicadores de nível de serviço indicados a seguir.

11.3.3. Em caso de eventual falta de instalação ou configuração, decorrentes de falha de infraestrutura que deva ser provida pela USCS, por exemplo, mas não limitado a falha no cabeamento estruturado, de energia, ou *links* de internet, não caberá nenhum tipo glosa ou penalidade a contratada.

11.3.4. Em caso de eventual vício ou defeito no cabeamento estruturado, exclusivamente, seja para *uplink* (interconexão entre switches) ou para conexão de pontos de acesso de rede sem fio (equipamento WiFi), deverá a contratada prover a solução técnica às suas expensas.

11.3.5. A manutenção/substituição prevista no item imediatamente anterior se limita a substituição de cabeamento, em pontos de até 100 metros ou múltiplos de 100 m.

11.3.6. Para fins de atendimento ao item 11.3.4, deverá a contratada, caso necessário, realizar a infraestrutura e/ou fornecer cabos, minimamente CAT6 ou fibra óptica (multimodo/monomodo) compatíveis com a necessidade do projeto.

11.3.7. A contratada a seu critério poderá prover protetores elétricos tais como mecanismos, acessórios e/ou equipamentos de proteção contra quedas, interrupções e distúrbios elétricos, para provimento e continuidade dos serviços do objeto.

11.4. **SERVIÇOS DE GARANTIA, MANUTENÇÃO E SUPORTE TÉCNICO**

11.4.1. **Severidade 1 - Crítica**: Serviço indisponível para grande número de usuários e/ou com alta degradação de performance. Serviço indisponível para o público interno/externo (docentes, discentes, colaboradores, terceirizados, e público externo), deverá ser iniciado em até 2 (duas) horas e o chamado solucionado em até 4 (quatro) horas corridas;

11.4.2. **Severidade 2 - Alta:** Serviço degradado, com risco iminente de indisponibilidade ou indisponível. Incidentes relacionados a usuários de alta prioridade (limitado a 3% dos usuários), deverá ser iniciado em até 4 (quatro) horas e o chamado solucionado em até 8 (oito) horas úteis;

11.4.3. **Severidade 3- Normal:** Serviço apresentando problemas sem indisponibilidade ou degradação de performance para os usuários, eventos de alertas proativos sem impacto de negócios, deverá ser iniciado em até 12 (doze) horas e o chamado solucionado em até 24 horas úteis;

11.4.4. **Rotineiro:** Operações das ferramentas e equipamentos em geral tais como configuração em geral, parametrização de ferramentais, criação e/ou configurações de usuários e novas redes, deverá ser iniciado em até 24 horas e o chamado solucionado em até 48 horas úteis;

11.4.5. Para atendimento a chamados em que não haja necessidade de troca de peças ou intervenção local, será admitido o atendimento remoto, ao invés de presença no local de instalação da solução;

11.4.6. Horas comerciais, para fins de cálculo do NMS, são as compreendidas entre 8h e 18h, horário de Brasília, em dias úteis;

11.4.7. Por início de atendimento entende-se o registro do chamado em ferramenta própria para início da tratativa, a fim de efetuar a correção do incidente, requisição ou o *troubleshooting* preciso, com interlocução direta com a equipe da USCS;

11.4.8. Um chamado técnico somente poderá ser fechado após o aceite da USCS e o término de atendimento se dará com a disponibilidade do recurso para uso em perfeitas condições de funcionamento;

11.4.9. Um chamado fechado, sem anuência da USCS ou sem que o problema tenha sido de fato resolvido, será reaberto e os prazos serão contados a partir da data de abertura original do chamado, inclusive para efeito de aplicação das multas e sanções previstas;

11.4.10. No final do atendimento, o técnico da Contratada deverá elaborar um relatório de ocorrência onde conste o problema causador do chamado, a solução encontrada, as pendências, a data e hora do chamado, do início e do fim do atendimento. Esse relatório deve ter a concordância e assinatura de um técnico da Universidade USCS.

11.5. **DETALHAMENTO DOS INDICADORES DE NÍVEL DE SERVIÇO**

11.5.1. Caso a Contratada não atinja os níveis mínimos de serviço fixados neste Termo de Referência, não venha a produzir os resultados esperados, deixe de executar as atividades contratadas, deixe de utilizar os materiais e recursos humanos exigidos qualitativamente e/ou quantitativamente para fornecimento da solução ou, utilize-os com qualidade aquém da expectativa demandada, estará, conforme cada caso, sujeita a aplicação de glosas nos valores estabelecidos para multas e/ou penalidades ou retenção do pagamento até que as pendências sejam sanadas.

11.5.2. Indicador de Verificação de Atraso na Entrega do Objeto:

Indicador 01 – Indicador de Atraso na Entrega do Objeto (IAEO)		
Tópico	**Descrição**	
Finalidade	Medir eventual tempo de atraso de implementação da solução constante na Ordem de Serviço.	
Meta a cumprir	**IAEO <= 0**	A meta definida visa garantir a entrega da implementação da solução constante nas Ordens de Serviço dentro do prazo previsto.
Instrumento de medição	Registro de assinatura da Ordem de Serviço - OS e seus respectivos Termos de Recebimento Provisório e Definitivo emitidos.	
Forma de acompanhamento	A avaliação será feita considerando o cronograma de execução e os prazos previstos neste Termo. Será subtraída a data de entrega definitiva da implementação da solução da OS ou a data do início da prestação dos serviços (desde que o fiscal reconheça aquela data, com registro em Termo de Recebimento Provisório ou Definitivo), pela data da assinatura da OS.	
Periodicidade	Execução única ao início do contrato, para cada Ordem de Serviço.	
Mecanismo de Cálculo (métrica)	IAOE = (TEX – TEST) / TEST Onde: **IAEO** – Indicador de Atraso de Entrega do Objeto; **TEX** – Tempo de Execução – corresponde ao período de execução da OS, da sua data de início até a data de entrega dos produtos da OS. **TEST** – Tempo Estimado para a execução da OS – constante na OS, conforme estipulado no Termo de Referência. A data de início será aquela constante na Ordem de Serviço; caso não esteja explícita, será o primeiro dia útil após a sua emissão. A data de entrega da OS deverá ser aquela reconhecida pelo fiscal, conforme critérios constantes no TR. Para os casos em que o fiscal rejeita a entrega, o prazo de execução da OS continua a correr, findando-se apenas quando a contratada entregar os equipamentos da OS e haja aceitação por parte do fiscal.	
Observações	Obs1.: Serão utilizados dias corridos na medição. Obs2.: Os dias com expediente parcial na Universidade USCS serão considerados no cômputo do indicador. Obs3.: Não se aplicará este indicador para as OS de Manutenções Corretivas do tipo Garantia e aquelas com execução interrompida ou cancelada por solicitação da USCS. Obs4.: Esse indicador será aplicado para aferição dos seguintes níveis mínimos de serviços: • Recebimento Provisório (Entrega dos equipamentos) – Itens 1 e 2 • Recebimento Definitivo (Término da Instalação, Configuração e Entrega de documentação) – Itens 1 e 2	

Início de Vigência	Data da assinatura da Ordem de Serviço – OS
Faixas de ajuste no pagamento e Sanções	De 0 a 0,10 – Pagamento integral da OS; De 0,11 a 0,20 – Glosa de 0,5% sobre o valor da OS; De 0,21 a 0,30 – Glosa de 1,0% sobre o valor da OS; De 0,31 a 0,50 – Glosa de 5,0% sobre o valor da OS; De 0,51 a 1,00 – Glosa de 10,0% sobre o valor da OS; Acima de 1 – Será aplicada Glosa de 12,5% sobre o valor da OS e Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento deste Termo de Referência.

Quadroa 03

11.5.3. Indicador de Verificação de Suporte Atendido dentro do Prazo (SADPN)

Indicador 02 – Suporte Atendido dentro do Prazo – Severidade 3 - Normal (SADPN)	
Tópico	**Descrição**
Finalidade	Assegurar que os chamados estejam dentro do nível mínimo de serviço exigido neste Termo.
Meta a cumprir	90% dos chamados atendidos dentro do prazo.
Instrumento de medição	Através das ferramentas disponíveis para a gestão de demandas, por controle próprio da USCS ou registros de abertura e encerramento de chamados, desde que aceitos pelo fiscal como meio formal de comunicação com a contratada.
Forma de acompanhamento	Cálculo de prazo de cada chamado ao Nível Mínimo de Serviço exigido, conforme previsto neste Termo.
Periodicidade	Sob demanda.
Mecanismo de Cálculo (métrica)	$SADP = \frac{(TEX - TEST)}{TEST}$ Onde: **SADP** – Suporte Atendido dentro do Prazo; **TEX** – Tempo de Execução – corresponde ao período de execução do chamado, da sua data de início até a data de sua conclusão definitiva. **TEST** – Tempo Estimado para a execução do chamado. A data de início será aquela em que foi registrado o chamado junto à contratada em ferramenta própria para início da tratativa. A data de início será aquela em que foi registrado o chamado junto à contratada em ferramenta própria. A data de conclusão do chamado deverá ser aquela reconhecida pelo fiscal, conforme critérios constantes no Termo de Referência. Para os casos em que o fiscal rejeita o encerramento do chamado, o prazo de execução continua a correr, findando-se apenas quando a contratada solucionar definitivamente o chamado e haja aceitação por parte do fiscal.
Observações	Obs1: Serão utilizados dias úteis na medição. Obs2: Os dias com expediente parcial na USCS serão considerados como dias úteis no cômputo do indicador. Obs3: Não se aplicará este indicador para as OS ou chamados com execução interrompida ou cancelada por solicitação da USCS. Obs4: Este indicador será aplicado a chamados de Garantia e/ou de Suporte Técnico, considerando os prazos indicados no TR para correção de falhas de hardware ou software. Obs5.: Esse indicador será aplicado para aferição dos níveis mínimos de serviços de garantia e assistência técnica dos Itens 1 e 2
Início de Vigência	A partir do primeiro dia útil da emissão do Termo de Recebimento Definitivo - TRD.
Faixas de ajuste no pagamento e Sanções	De <=0 a 0,10 – Glosa de 0,0%; De 0,11 a 0,20 – Glosa de 0,5%; De 0,21 a 0,30 – Glosa de 1,0%; De 0,31 a 0,50 – Glosa de 3,0%; De 0,51 a 1,00 – Glosa de 5,0%; Acima de 1 – Será aplicada Glosa de 10% e aplicadas Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento previstas neste Termo de Referência. Obs1.: As glosas incidirão sobre o valor da obrigação não cumprida no item faturado;

Quadroa 04

11.5.4. Indicador de Verificação de Suporte Atendido dentro do Prazo (SADPN)

Indicador 03 – Suporte Atendido dentro do Prazo – Severidade 2 - Alta (SADPA)	
Tópico	**Descrição**
Finalidade	Assegurar que os chamados estejam dentro do nível mínimo de serviço exigido neste Termo.
Meta a cumprir	95% dos chamados atendidos dentro do prazo.

Instrumento de medição	Através das ferramentas disponíveis para a gestão de demandas, por controle próprio da USCS ou registros de abertura e encerramento de chamados, desde que aceitos pelo fiscal como meio formal de comunicação com a contratada.
Forma de acompanhamento	Cálculo de prazo de cada chamado ao Nível Mínimo de Serviço exigido, conforme previsto neste Termo.
Periodicidade	Sob demanda.
Mecanismo de Cálculo (métrica)	SADP = (TEX – TEST) / TEST Onde: **SADP** – Suporte Atendido dentro do Prazo; **TEX** – Tempo de Execução – corresponde ao período de execução do chamado, da sua data de início até a data de sua conclusão definitiva. **TEST** – Tempo Estimado para a execução do chamado. A data de início será aquela em que foi registrado o chamado junto à contratada em ferramenta própria. A data de conclusão do chamado deverá ser aquela reconhecida pelo fiscal, conforme critérios constantes no Termo de Referência. Para os casos em que o fiscal rejeita o encerramento do chamado, o prazo de execução continua a correr, findando-se apenas quando a contratada solucionar definitivamente o chamado e haja aceitação por parte do fiscal.
Observações	Obs1: Serão utilizados dias úteis na medição. Obs2: Os dias com expediente parcial na Universidade USCS serão considerados como dias úteis no cômputo do indicador. Obs3: Não se aplicará este indicador para as OS ou chamados com execução interrompida ou cancelada por solicitação da USCS. Obs4: Este indicador será aplicado a chamados de Garantia e/ou de Suporte Técnico, considerando os prazos indicados no TR para correção de falhas de hardware ou software. Obs5.: Esse indicador será aplicado para aferição dos níveis mínimos de serviços de garantia e assistência técnica dos Itens 1 e 2
Início de Vigência	A partir do primeiro dia útil da emissão do Termo de Recebimento Definitivo - TRD.
Faixas de ajuste no pagamento e Sanções	De <=0 a 0,10 – Glosa de 0,0%; De 0,11 a 0,20 – Glosa de 5%; De 0,21 a 0,30 – Glosa de 6,0%; De 0,31 a 0,50 – Glosa de 8,0%; De 0,51 a 1,00 – Glosa de 11,0%; Acima de 1 – Será aplicada Glosa de 15% e aplicadas Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento previstas neste Termo de Referência. Obs1.: As glosas incidirão sobre o valor da obrigação não cumprida no item faturado;

Quadroa 05

11.5.5. Indicador de Verificação de Suporte Atendido dentro do Prazo (SADPN)

Indicador 04 – Suporte Atendido dentro do Prazo – Severidade 1 - Crítica (SADPC)	
Tópico	**Descrição**
Finalidade	Assegurar que os chamados estejam dentro do nível mínimo de serviço exigido neste Termo.
Meta a cumprir	98% dos chamados atendidos dentro do prazo.
Instrumento de medição	Através das ferramentas disponíveis para a gestão de demandas, por controle próprio da USCS ou registros de abertura e encerramento de chamados, desde que aceitos pelo fiscal como meio formal de comunicação com a USCS.
Forma de acompanhamento	Cálculo de prazo de cada chamado ao Nível Mínimo de Serviço exigido, conforme previsto neste Termo.
Periodicidade	Sob demanda.
Mecanismo de Cálculo (métrica)	SADP = (TEX – TEST) / TEST Onde: **SADP** – Suporte Atendido dentro do Prazo; **TEX** – Tempo de Execução – corresponde ao período de execução do chamado, da sua data de início até a data de sua conclusão definitiva. **TEST** – Tempo Estimado para a execução do chamado. A data de início será aquela em que foi registrado o chamado junto à contratada em ferramenta própria. A data de conclusão do chamado deverá ser aquela reconhecida pelo fiscal, conforme critérios constantes no Termo de Referência. Para os casos em que o fiscal rejeita o encerramento do chamado, o prazo de execução continua a correr, findando-se apenas quando a contratada solucionar definitivamente o chamado e haja aceitação por parte do fiscal.
Observações	Obs1: Serão utilizados dias úteis na medição. Obs2: Os dias com expediente parcial na Universidade USCS serão considerados como dias úteis no cômputo do indicador.

	Obs3: Não se aplicará este indicador para as OS ou chamados com execução interrompida ou cancelada por solicitação da USCS. Obs4: Este indicador será aplicado a chamados de Garantia e/ou de Suporte Técnico, considerando os prazos indicados no TR para correção de falhas de hardware ou software. Obs5.: Esse indicador será aplicado para aferição dos níveis mínimos de serviços de garantia e assistência técnica dos Itens 1 e 2
Início de Vigência	A partir do primeiro dia útil da emissão do Termo de Recebimento Definitivo - TRD.
Faixas de ajuste no pagamento e Sanções	De <=0 a 0,10 – Glosa de 0,0%; De 0,11 a 0,20 – Glosa de 11%; De 0,21 a 0,30 – Glosa de 12,0%; De 0,31 a 0,50 – Glosa de 14,0%; De 0,51 a 1,00 – Glosa de 16,0%; Acima de 1 – Será aplicada Glosa de 20% e aplicadas Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento previstas neste Termo de Referência. Obs1.: As incidirão sobre o valor da obrigação não cumprida no item faturado;

Quadroa 06

11.6. Indicador de Verificação de Saúde Operacional (IRSO)

Indicador 05 – Relatório de Saúde Operacional (IRSO)	
Tópico	**Descrição**
Finalidade	Apresentar um relatório com a percepção de regras conflitantes ou mal configuradas, apontamento de melhores práticas a serem aplicadas, visão crítica das configurações aplicadas e apontar melhorias, avaliação do consumo dos recursos dos equipamentos e propor, caso necessário, cenários de melhor aproveitamento dos recursos, entre outros apontamentos que a Contratada achar pertinente para melhor desempenho da solução.
Meta a cumprir	Entrega do relatório dentro do prazo de 5 dias úteis.
Instrumento de medição	Através das ferramentas disponíveis para a gestão de demandas, por controle próprio da USCS ou registros de abertura e encerramento de chamados, desde que aceitos pelo fiscal técnico como meio formal de comunicação com a contratada.
Forma de acompanhamento	Cálculo de prazo de cada chamado ao Nível Mínimo de Serviço exigido, conforme previsto neste Termo.
Periodicidade	Sob demanda ou em periodicidade indicada no Termo para realização de manutenção preventiva
Mecanismo de Cálculo (métrica)	$SADP = \frac{(TEX - TEST)}{TEST}$ Onde: **SADP** – Suporte Atendido dentro do Prazo; **TEX** – Tempo de Execução – corresponde ao período de execução do chamado, da sua data de início até a data de sua conclusão definitiva. **TEST** – Tempo Estimado para a execução do chamado. A data de início será aquela em que foi registrado o chamado junto à contratada em ferramenta própria. A data de conclusão do chamado deverá ser aquela reconhecida pelo fiscal, conforme critérios constantes no Termo de Referência. Para os casos em que o fiscal rejeita o encerramento do chamado, o prazo de execução continua a correr, findando-se apenas quando a contratada solucionar definitivamente o chamado e haja aceitação por parte do fiscal.
Observações	Obs1: Serão utilizados dias úteis na medição. Obs2: Os dias com expediente parcial na Universidade USCS serão considerados como dias úteis no cômputo do indicador. Obs3: Não se aplicará este indicador para as OS ou chamados com execução interrompida ou cancelada por solicitação da USCS. Obs4: Este indicador será aplicado a chamados de Garantia e/ou de Suporte Técnico, considerando os prazos indicados no TR para correção de falhas de hardware ou software. Obs5.: Esse indicador será aplicado para aferição dos níveis mínimos de serviços de garantia e assistência técnica dos Itens 1, e 2.
Início de Vigência	A partir do primeiro dia útil da emissão do Termo de Recebimento Definitivo - TRD.
Faixas de ajuste no pagamento e Sanções	De <=0 a 0,10 – Glosa de 0,0%; De 0,11 a 0,20 – Glosa de 5%; De 0,21 a 0,30 – Glosa de 7%; De 0,31 a 0,50 – Glosa de 10,0%; De 0,51 a 1,00 – Glosa de 13,0%; Acima de 1 – Será aplicada Glosa de 20% e aplicadas Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento previstas neste Termo de Referência. Obs1.: As glosas incidirão sobre o valor da obrigação não cumprida no item faturado;

Quadroa 07

11.7. Indicador de Permanência de Equipamento, Peça ou Componente Backup

Indicador 06 – Indicador de Permanência de Equipamento, Peça ou Componente Backup (IPEB)	
Tópico	**Descrição**
Finalidade	Assegurar que o equipamento de backup da contratada não ultrapasse os 30 dias corridos contados a partir da comunicação realizada pelo sistema de registro da própria da USCS.
Meta a cumprir	30 dias corridos para cada ocorrência
Instrumento de medição	Através das ferramentas disponíveis para a gestão de demandas, por controle próprio da USCS ou registros de abertura e encerramento de chamados, desde que aceitos pelo Fiscal Técnico como meio formal de comunicação com a contratada.
Forma de acompanhamento	Cálculo de prazo de Registro/Resposta de cada solicitação de suporte técnico de garantia em relação ao Nível de Serviço.
Periodicidade	Sob demanda.
Mecanismo de Cálculo (métrica)	$$IPEB = \frac{(TEX - TEST)}{TEST}$$ Onde: **IPEB** – Indicador de Permanência de Equipamento, Peça ou Componente Backup (IPEB); **TEX** – Tempo de Execução – corresponde ao período de execução do chamado, da sua data de início até a data de sua conclusão definitiva. **TEST** – Tempo Estimado para a execução do chamado. A data de início será aquela em que foi registrado encerramento do chamado de suporte técnico da contratada e abertura do chamado de garantia junto ao fabricante; A data de início e de conclusão do chamado deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes no Termo de Referência. Para os casos em que o fiscal rejeita o dia e hora de registro ou de encerramento do chamado, o prazo de execução continua a correr, findando-se apenas quando a contratada solucionar definitivamente o chamado junto ao fabricante e haja aceitação por parte do fiscal técnico.
Observações	Obs1: Serão utilizados dias úteis na medição. Obs2: Os dias com expediente parcial na Universidade USCS serão considerados como dias úteis no cômputo do indicador. Obs3: A contagem do prazo de atendimento se inicia após o Fechamento do chamado de Suporte Técnico da Contratada concomitantemente ao registro de chamado de suporte técnico em Garantia junto ao Fabricante; Obs4: Não se aplicará este indicador para as OS com execução interrompida ou cancelada por solicitação da USCS. Obs5.: Esse indicador será aplicado para aferição dos níveis mínimos de serviços de garantia e assistência técnica dos Itens 1 e 2
Início de Vigência	A partir do primeiro dia útil da emissão do Termo de Recebimento Definitivo - TRD.
Faixas de ajuste no pagamento e Sanções	De <=0 a 0,10 – Glosa de 0,0%; De 0,11 a 0,20 – Glosa de 0,5%; De 0,21 a 0,30 – Glosa de 1,0%; De 0,31 a 0,50 – Glosa de 5,0%; De 0,51 a 1,00 – Glosa de 10,0%; Acima de 1 – Será aplicada Glosa de 12,5% e aplicadas Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento previstas neste Termo de Referência. Obs1.: No caso dos itens 1, 2 e 3, as glosas incidirão sobre o valor da obrigação não cumprida no item faturado;

Quadroa 08

Anexo II do Contrato nº ____/2026

Quadro contendo relação de equipamentos físicos as a service, serviços, quantitativos e preços.

Item	Descrição	Fabricante, Marca, Modelo	Quantidade Equipamento	Cronograma Pagamento	Valor Unitário em Reais	Valor Mensal em Reais	Valor Total em Reais
	Serviço gerenciado de solução para gestão ativos de rede, monitoramento e segurança, incluindo fornecimento de softwares, equipamentos, licenciamentos, suporte técnico especializado, acessórios e garantia.						
	Serviço gerenciado de Switch, incluindo fornecimento de equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.						
1	Switch de acesso **tipo 1 (*As a Service*)**, incluindo equipamentos licenciados, suporte específico do fabricante, acessórios e garantia.		28	24 Meses			
2	Switch de acesso **tipo 2 (*As a Service*)**, incluindo equipamentos licenciados, suporte específico do fabricante, acessórios e garantia.		2	24 Meses			
3	Switch de acesso **tipo 3 (*As a Service*)**, incluindo equipamentos licenciados, suporte específico do fabricante, acessórios e garantia.		2	24 Meses			
4	Implementação – instalação e configuração física da solução de Switch.		32	1 Serviço			
	Serviço gerenciado de Ponto de Acesso (AP), incluindo fornecimento de equipamentos licenciados, suporte técnico específico do fabricante, acessórios e garantia.						
5	Ponto de acesso **tipo 1 (*As a Service*)**, incluindo equipamentos licenciados, suporte específico do fabricante, acessórios e garantia.		185	24 Meses			
6	Ponto de acesso **tipo 2 (*As a Service*)**, incluindo equipamentos licenciados, suporte específico do fabricante, acessórios e garantia.		12	24 Meses			
7	Ponto de acesso **tipo 3 (*As a Service*)**, incluindo equipamentos licenciados, suporte específico do fabricante, acessórios e garantia.		12	24 Meses			
8	Ponto de acesso **tipo 4 (*As a Service*)**, incluindo equipamentos licenciados, suporte específico do fabricante, acessórios e garantia.		6	24 Meses			
9	Ponto de acesso **tipo 5 (*As a Service*)**, incluindo equipamentos licenciados, suporte específico do fabricante, acessórios e garantia.		4	24 Meses			
10	Implementação – instalação e configuração física da solução de Ponto de Acesso.		219	1 Serviço			
	Serviço gerenciado de solução para gestão de ativos de rede, monitoramento e segurança, incluindo fornecimento de softwares, controladora (SaaS), licenciamento e suporte técnico especializado, acessórios e garantia.						
11	Solução para gestão de switches, monitoramento e segurança, incluindo fornecimento de softwares, licenciamento e suporte técnico especializado.		1	24 Meses			
12	Solução para gestão de pontos de acesso, monitoramento, e segurança, incluindo fornecimento de softwares, controladora (SaaS), licenciamento e suporte técnico especializado.		1	24 Meses			
13	Instalação, configuração e parametrização da solução para gerenciamento e gestão do parque de ativos de switches e pontos de acessos (251 equipamentos).		251	1 Serviço			
					Valor Global do Contrato (em reais)		

Anexo III do Contrato nº ____/2026

Distribuição acerca dos Pontos de Acesso WiFi

Estimativa de Ponto de Acesso Wi-Fi's após Site Survey	
CAMPUS BARCELONA	***Quantidade***
Campus - Barcelona - 1º Pavimento - Bloco C	6
Campus - Barcelona - 1º Pavimento e Subsolo Bloco A	10
Campus - Barcelona - 1ºe 2º Pavimento - Bloco C	8
Campus - Barcelona - 2º Pavimento e Cobertura - Bloco A	6
Campus - Barcelona - Anexo Atendimento	1
Campus - Barcelona - Anexo Capela	1
Campus - Barcelona - Anexo Deposito	1
Campus - Barcelona - Anexo Portaria 1	1
Campus - Barcelona - Anexo Portaria 2 e 3	1
Campus - Barcelona - Anexo Portaria 4	1
Campus - Barcelona - Plantas - Bloco E	6
Campus - Barcelona - Subsolo - Bloco B	3
Campus - Barcelona - Subsolo Auditório - Bloco D	9
Campus - Barcelona - Subsolo Manutenção - Bloco G	6
Campus - Barcelona - Subsolo Quadra - Bloco G	5
Campus - Barcelona - Térreo - Bloco A	7
Campus - Barcelona - Térreo - Bloco B	8
Campus - Barcelona - Térreo - Bloco C	6
Campus - Barcelona - Térreo - Bloco D	7
Campus - Barcelona - Térreo (Quadra) - Bloco G	5
Subtotal Campus Barcelona	**98**
CAMPUS CENTRO	***Quantidade***
Campus - Centro - 1º Andar	8
Campus - Centro - 2º Andar	10
Campus - Centro - 3º Andar	12
Campus - Centro - 4º Andar	11
Campus - Centro - 5º Andar	10
Campus - Centro – Subsolo	7
Campus - Centro – Térreo	10
Campus - Centro II – 1	4
Campus - Centro II – 2	3
Subtotal Campus Centro	**75**
CAMPUS CONCEIÇÃO	***Quantidade***
Campus - Conceição - 1º Andar	12
Campus - Conceição – Térreo	10
Total	**22**
CAMPUS ITAPETINGA	***Quantidade***
Campus – Itapetininga	11
Campus - Itapetininga – Atual	13
Subtotal Campus Itapetininga	**24**
TOTAL	**219**

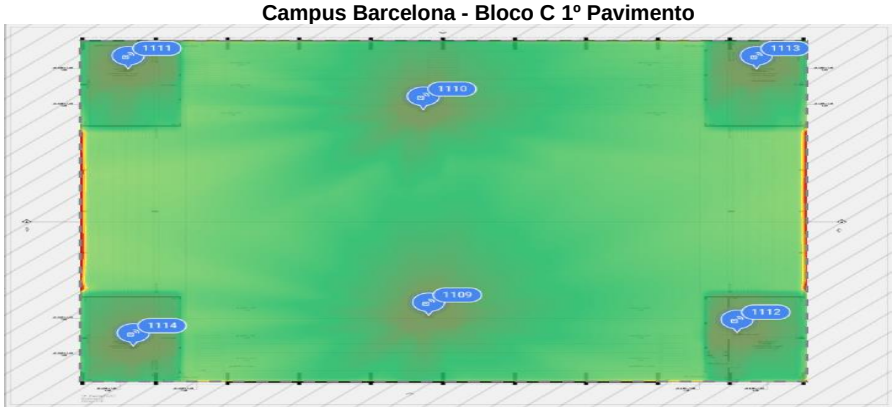
Distribuição acerca dos Switches

Quantidade de Switches por porta	
Switches	**Quantidades**
Switch Tipo 1 (8x portas)	28
Switch Tipo 2 (24 portas)	2
Switch Tipo 3 (48 portas)	2
Total de Switches	32

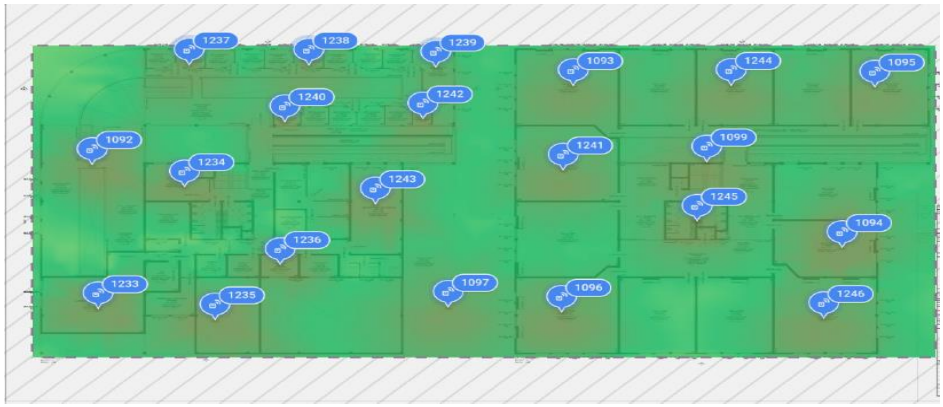
Lay Out e Topologia acerca da Solução proposta para distribuição dos equipamentos WiFi site survey teórico

Campus Barcelona - Disposição dos equipamentos no projeto

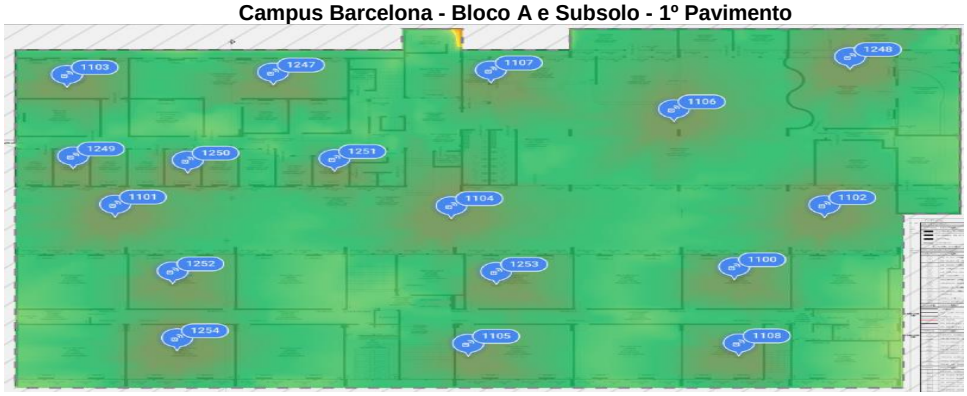
Campus Barcelona - Bloco C 1º Pavimento



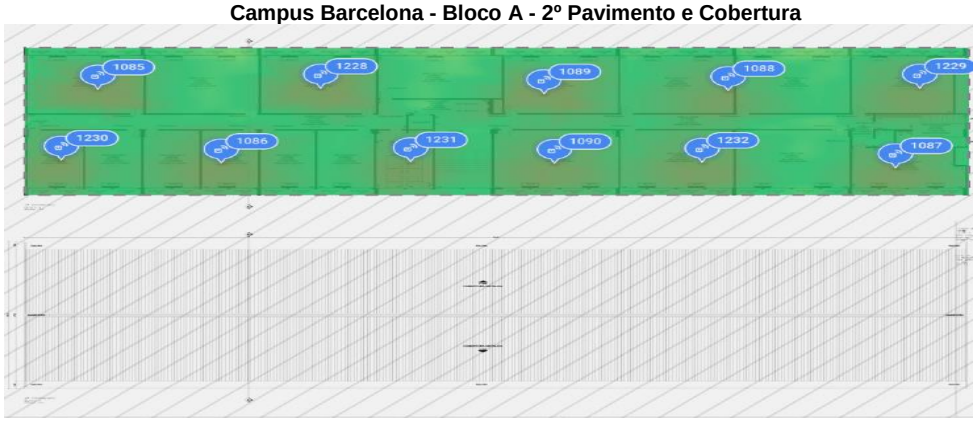
Campus Barcelona - Bloco C 1º e 2º Pavimentos



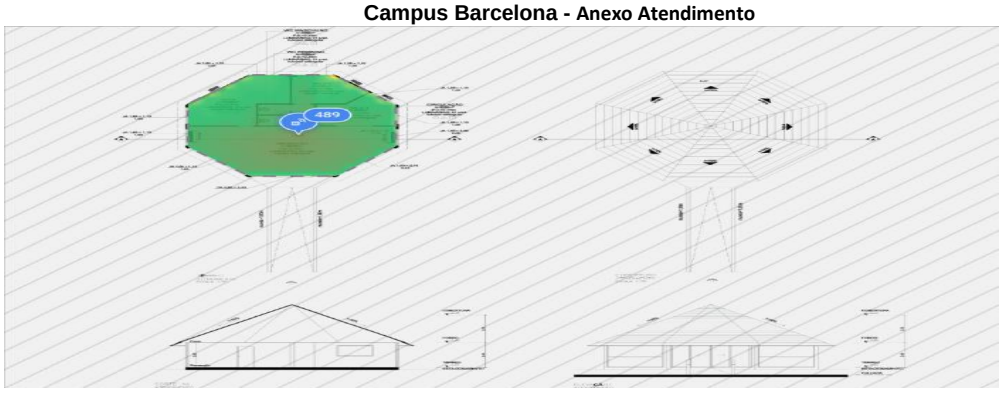
Campus Barcelona - Bloco A e Subsolo - 1º Pavimento



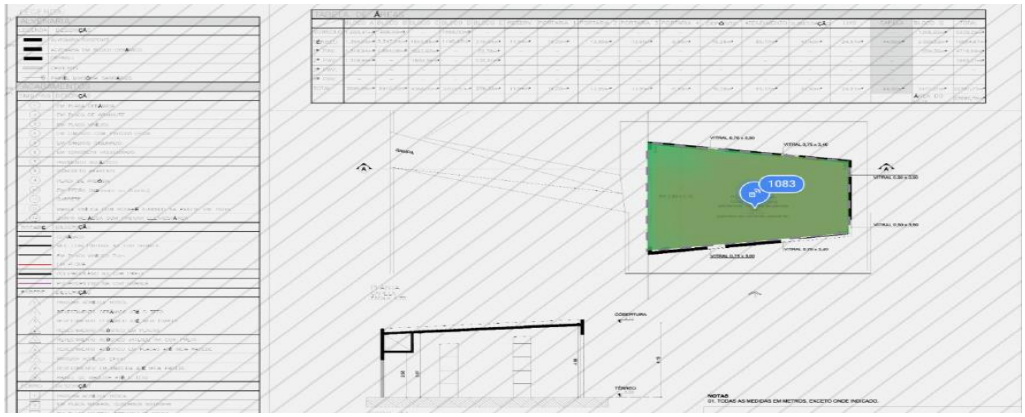
Campus Barcelona - Bloco A - 2º Pavimento e Cobertura



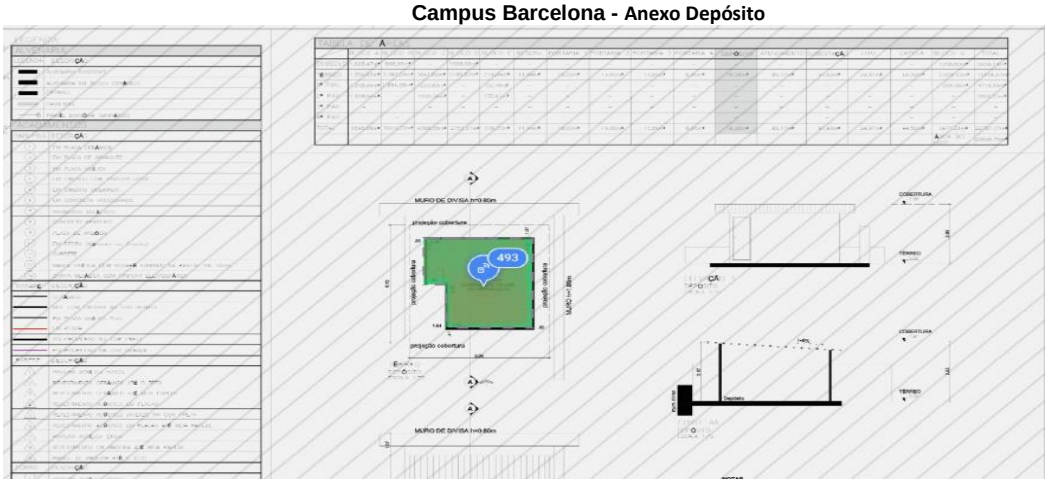
Campus Barcelona - Anexo Atendimento



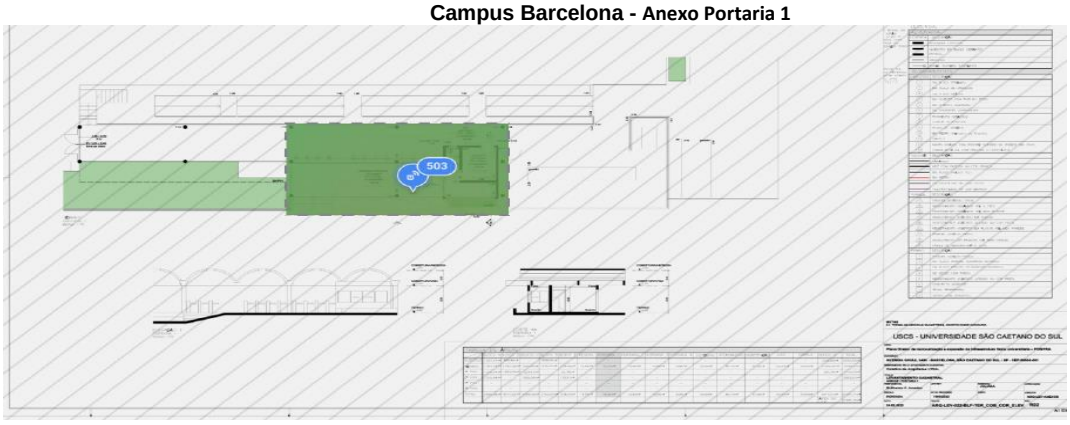
Campus Barcelona - Anexo Capela



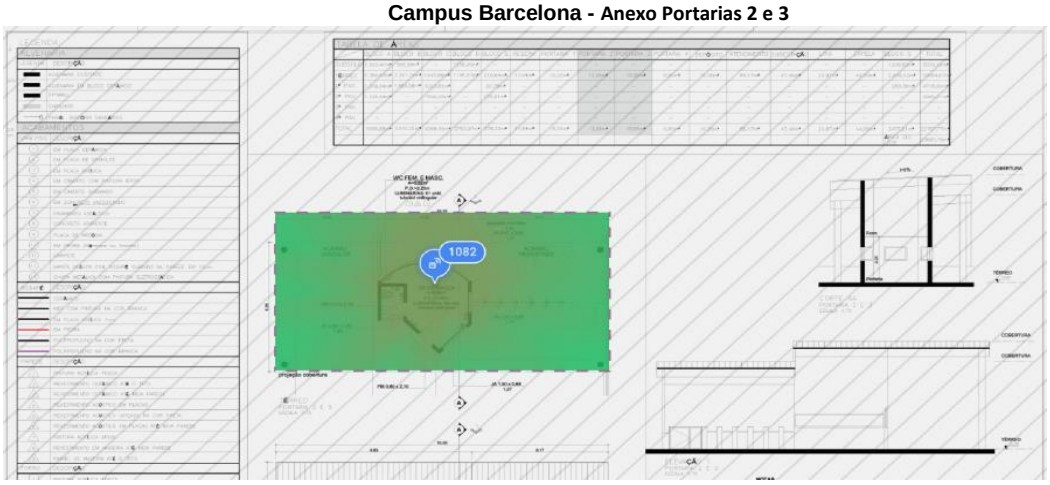
Campus Barcelona - Anexo Depósito



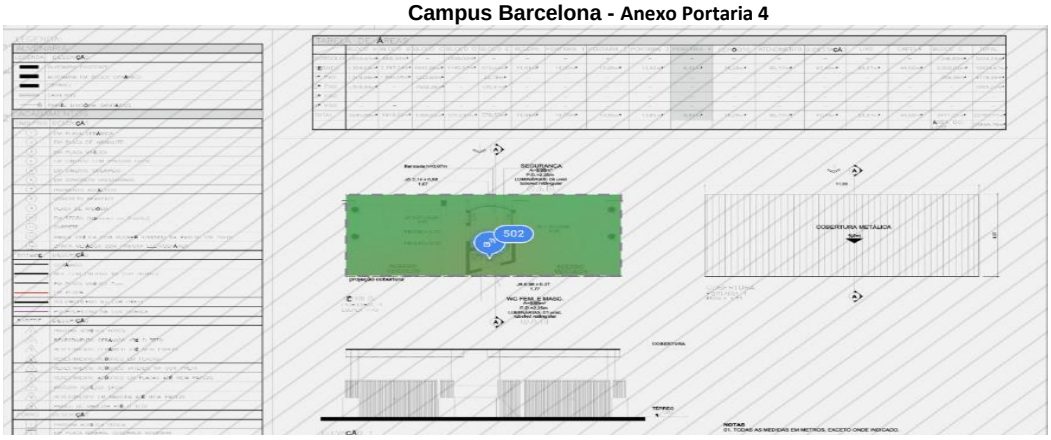
Campus Barcelona - Anexo Portaria 1



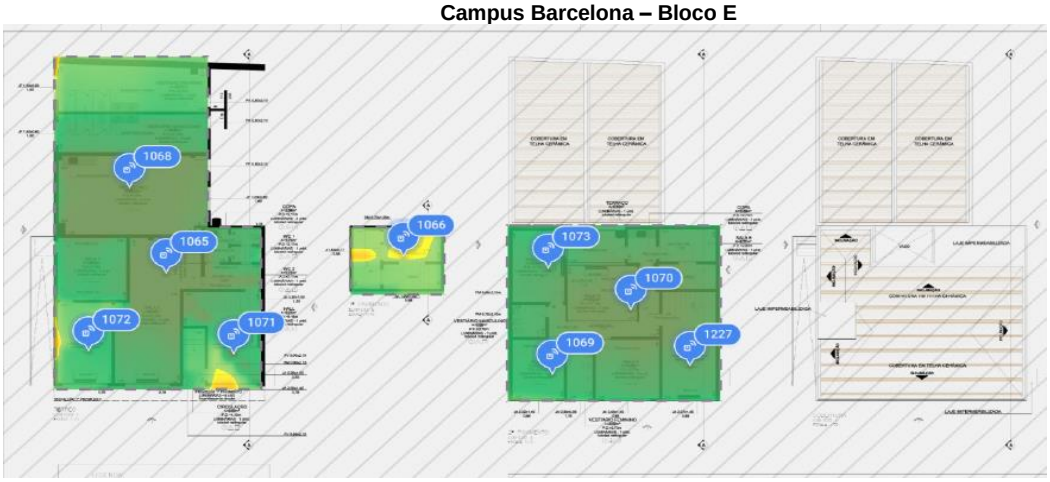
Campus Barcelona - Anexo Portarias 2 e 3



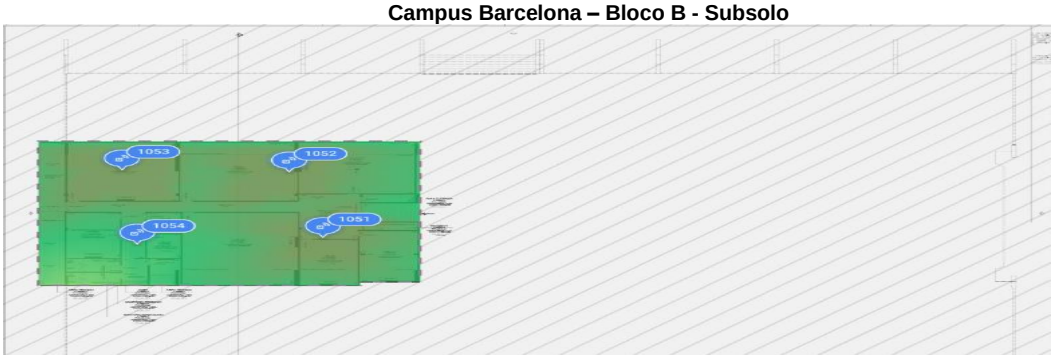
Campus Barcelona - Anexo Portaria 4



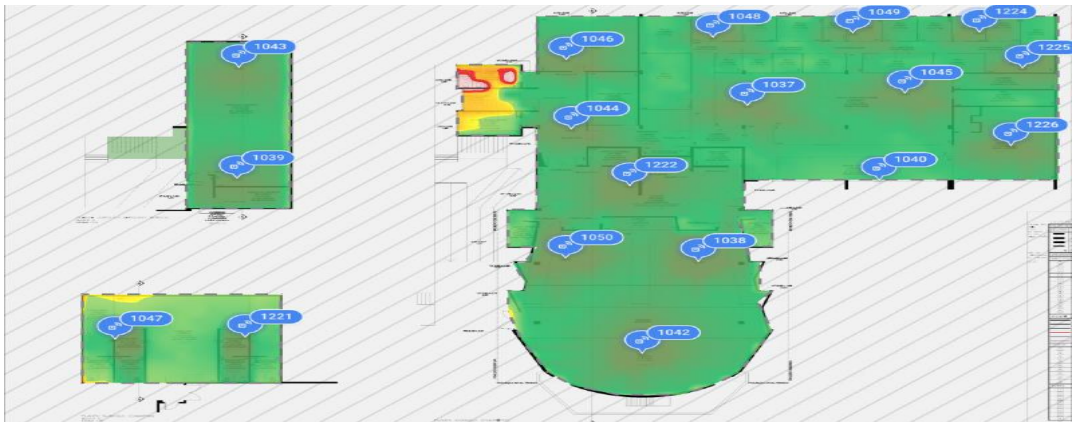
Campus Barcelona – Bloco E



Campus Barcelona – Bloco B - Subsolo

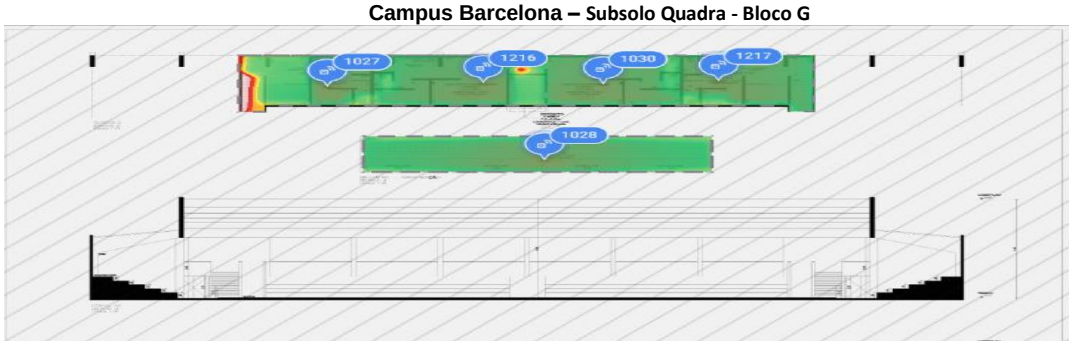


Campus Barcelona – Subsolo Auditório - Bloco D

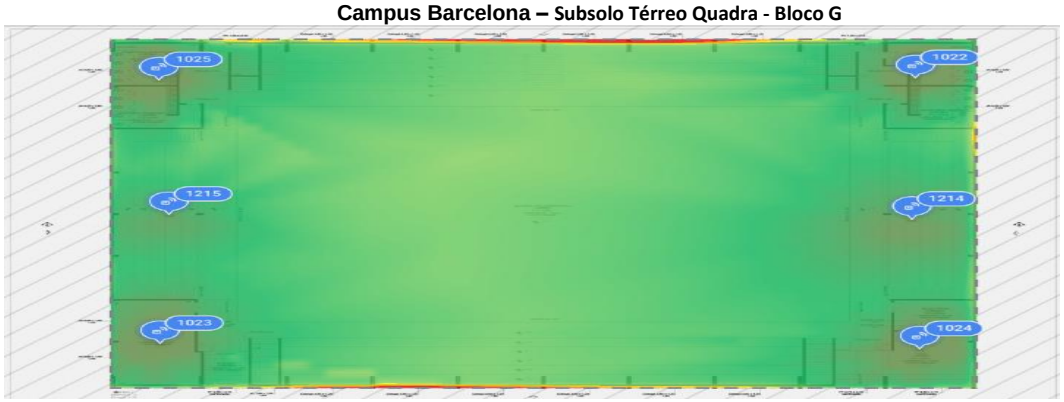


Campus Barcelona – Subsolo Manutenção - Bloco G

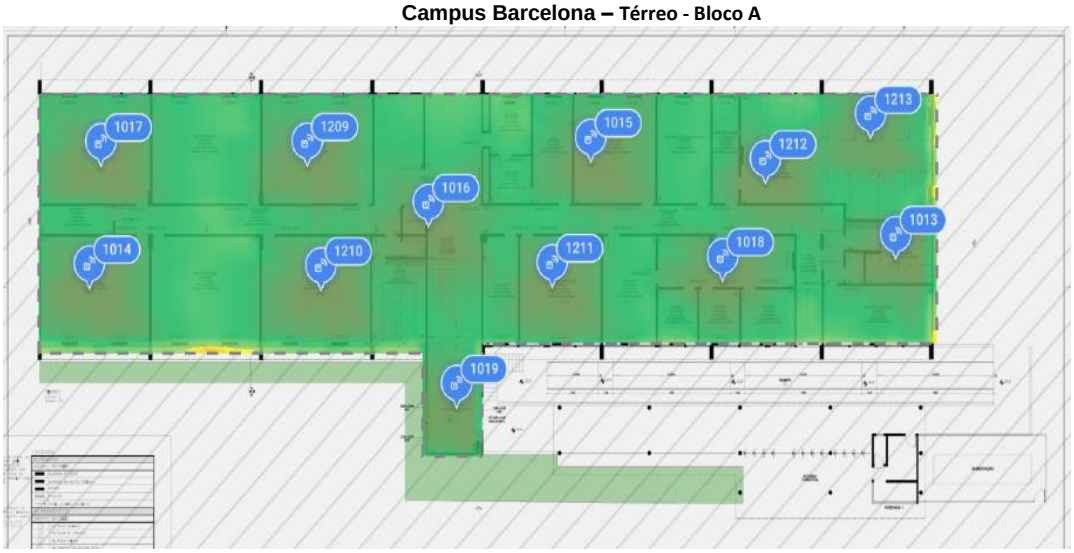
Campus Barcelona – Subsolo Quadra - Bloco G



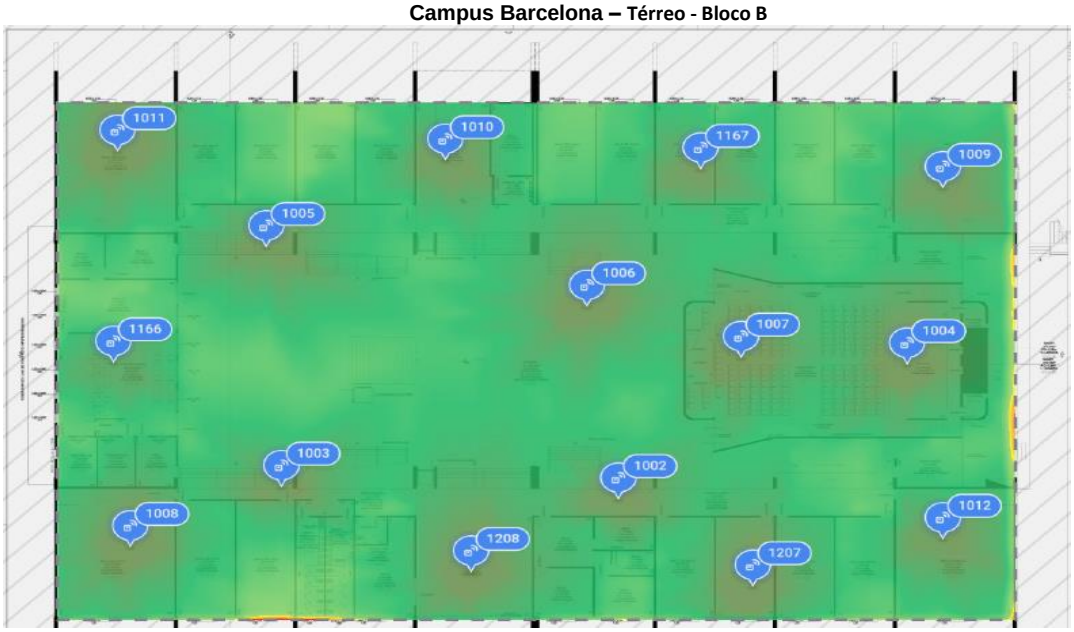
Campus Barcelona – Subsolo Térreo Quadra - Bloco G



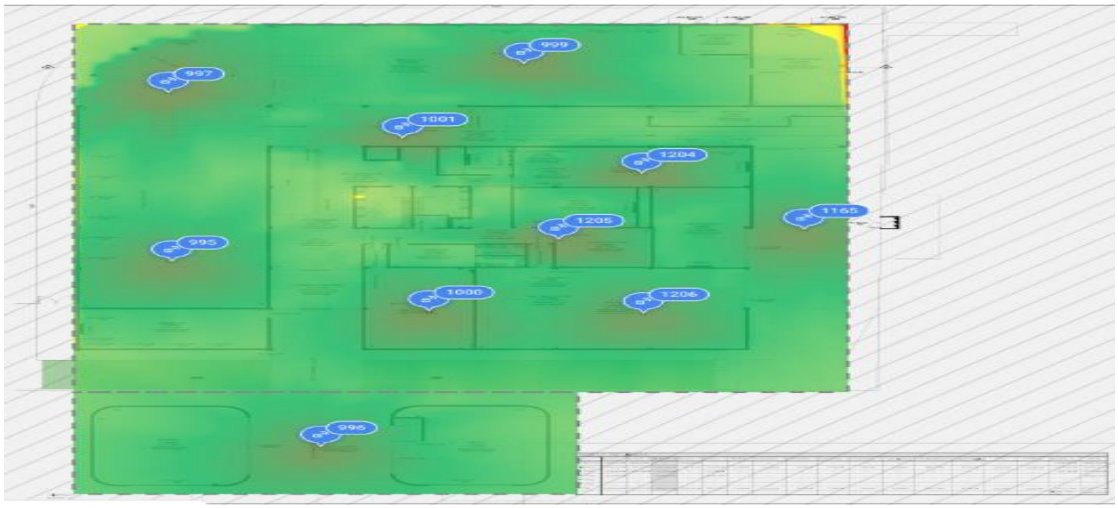
Campus Barcelona – Térreo - Bloco A



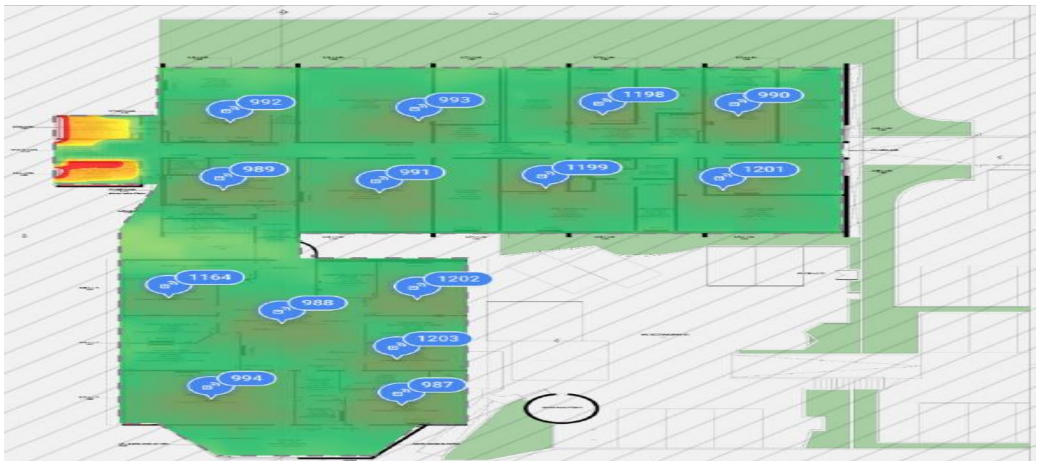
Campus Barcelona – Térreo - Bloco B



Campus Barcelona – Térreo - Bloco C

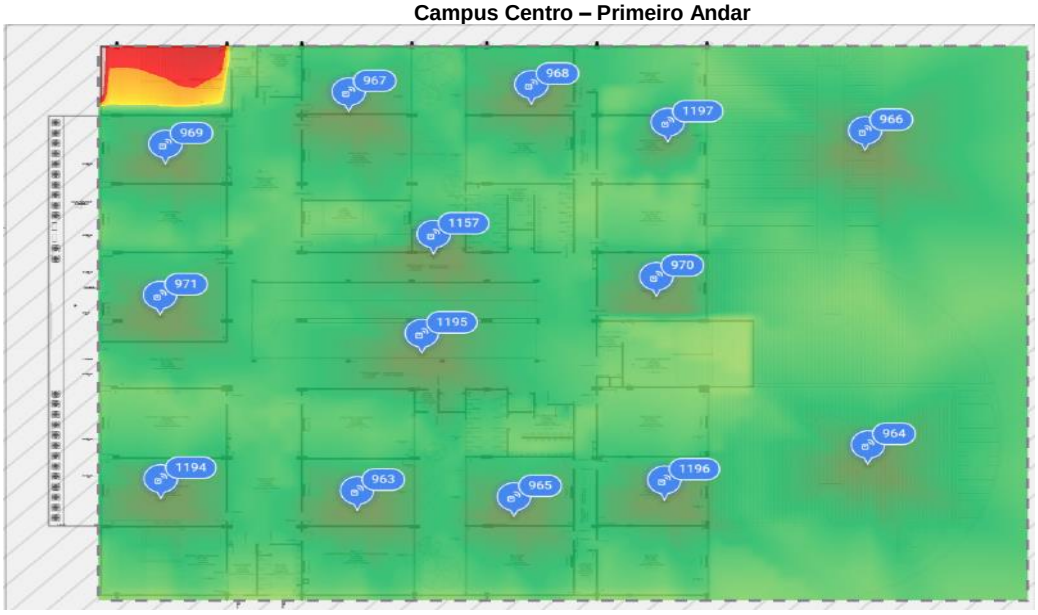


Campus Barcelona – Térreo - Bloco D

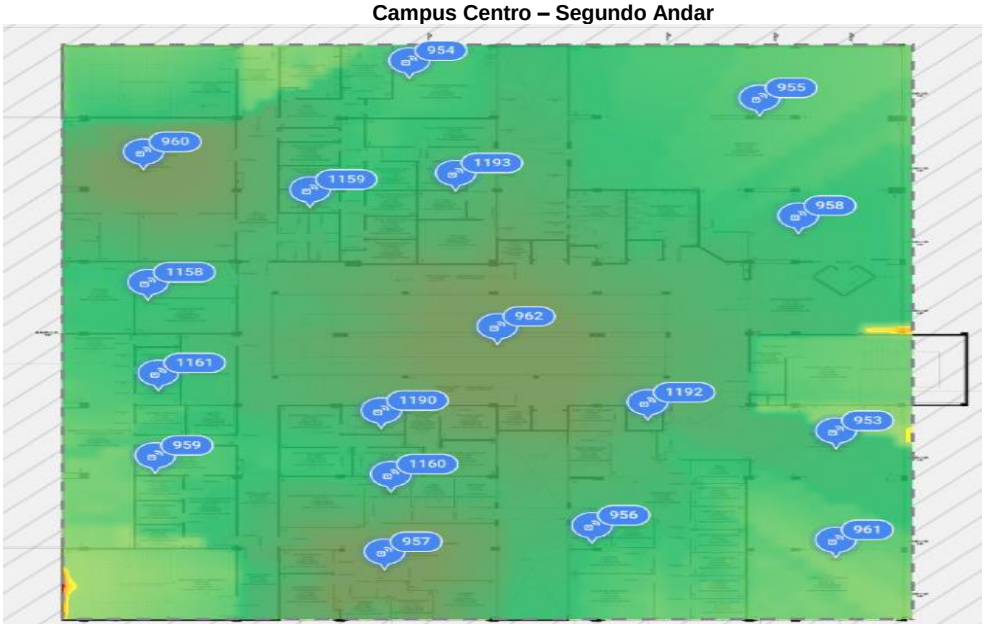


Campus Centro - Disposição dos equipamentos no projeto

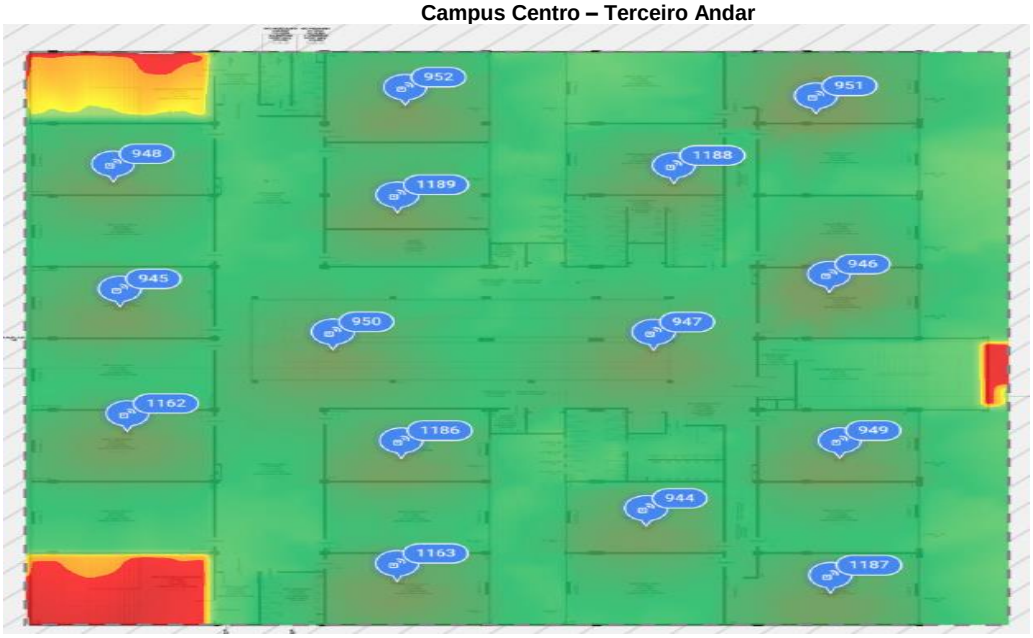
Campus Centro – Primeiro Andar



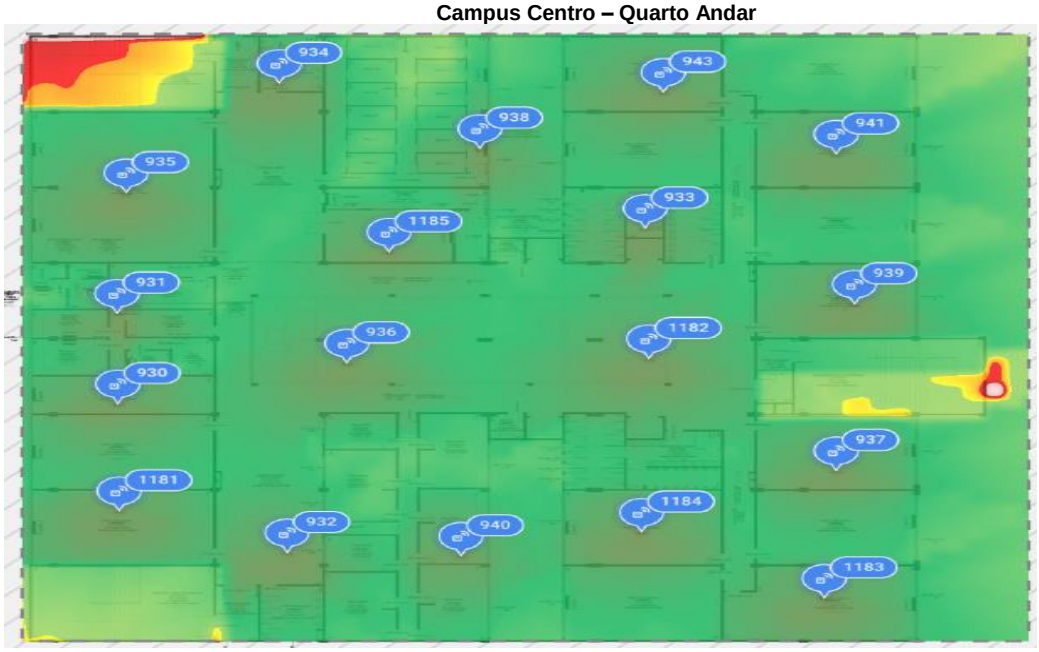
Campus Centro – Segundo Andar



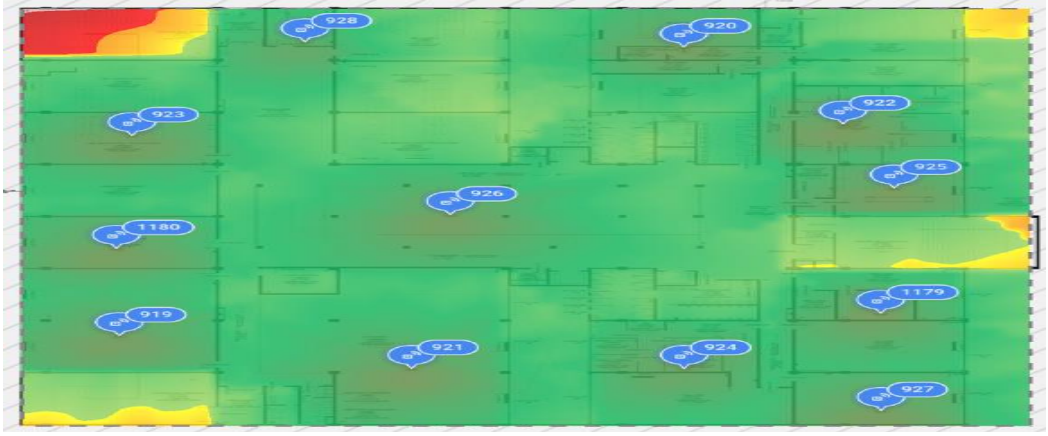
Campus Centro – Terceiro Andar



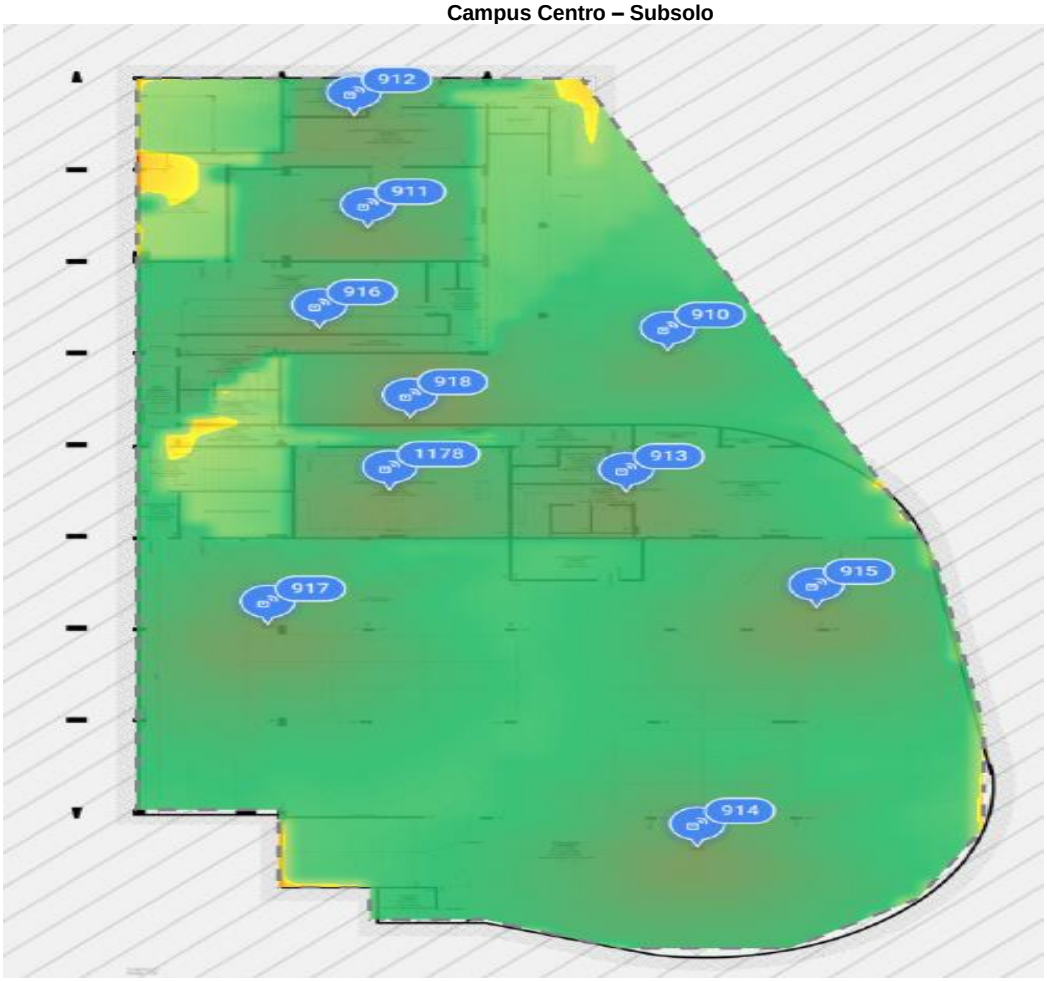
Campus Centro – Quarto Andar



Campus Centro – Quinto Andar



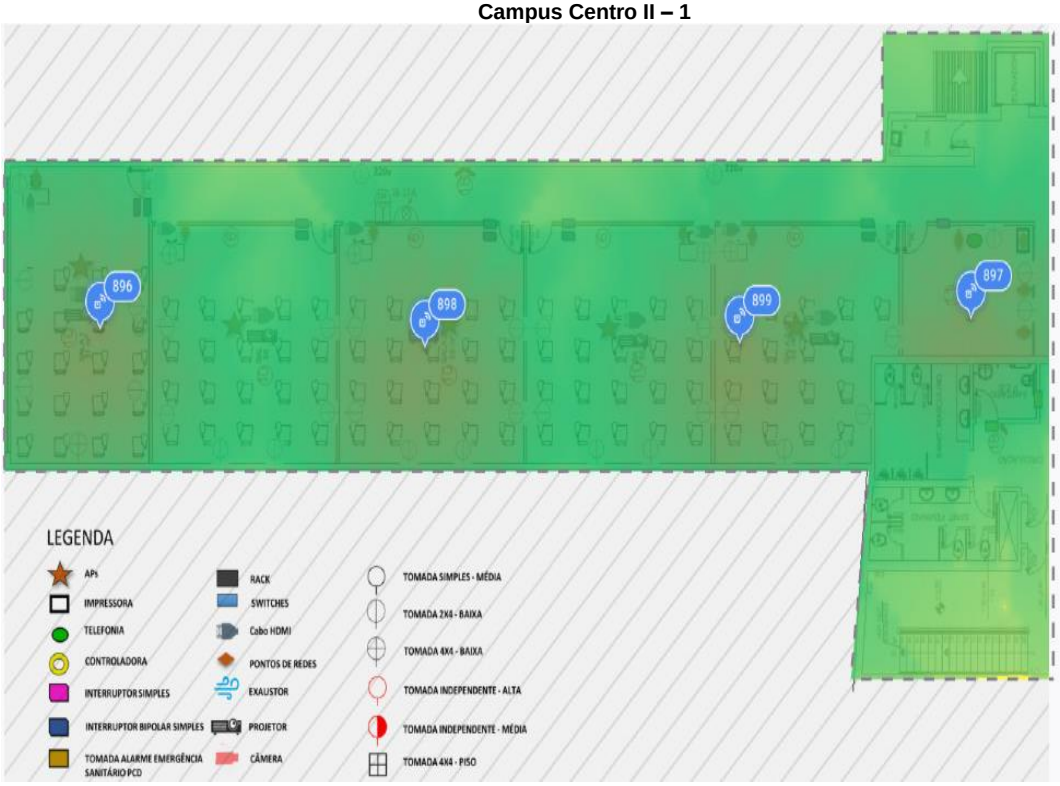
Campus Centro – Subsolo



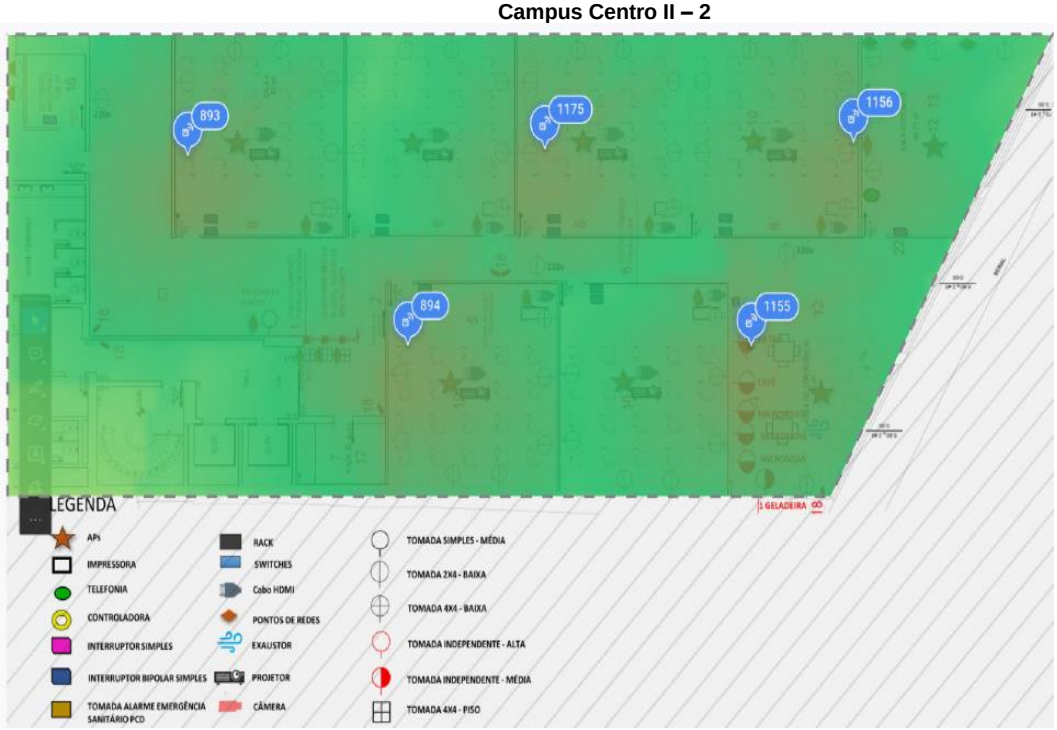
Campus Centro – Térreo

Campus Centro II – Disposição dos equipamentos no projeto

Campus Centro II – 1

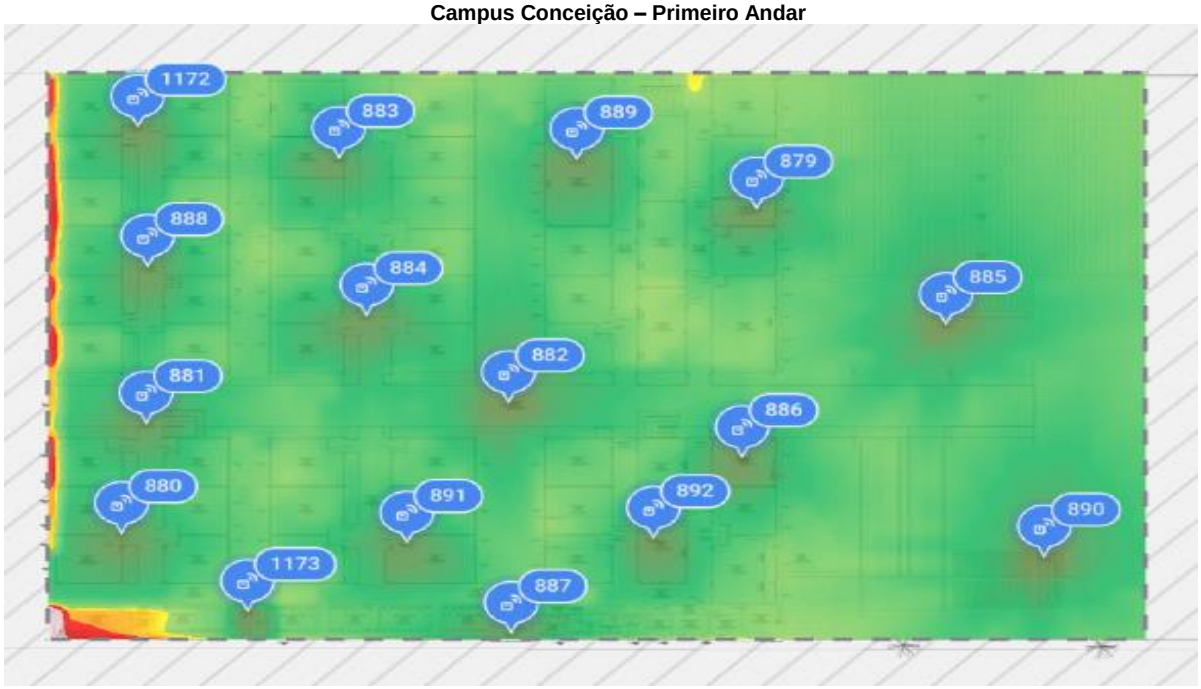


Campus Centro II – 2

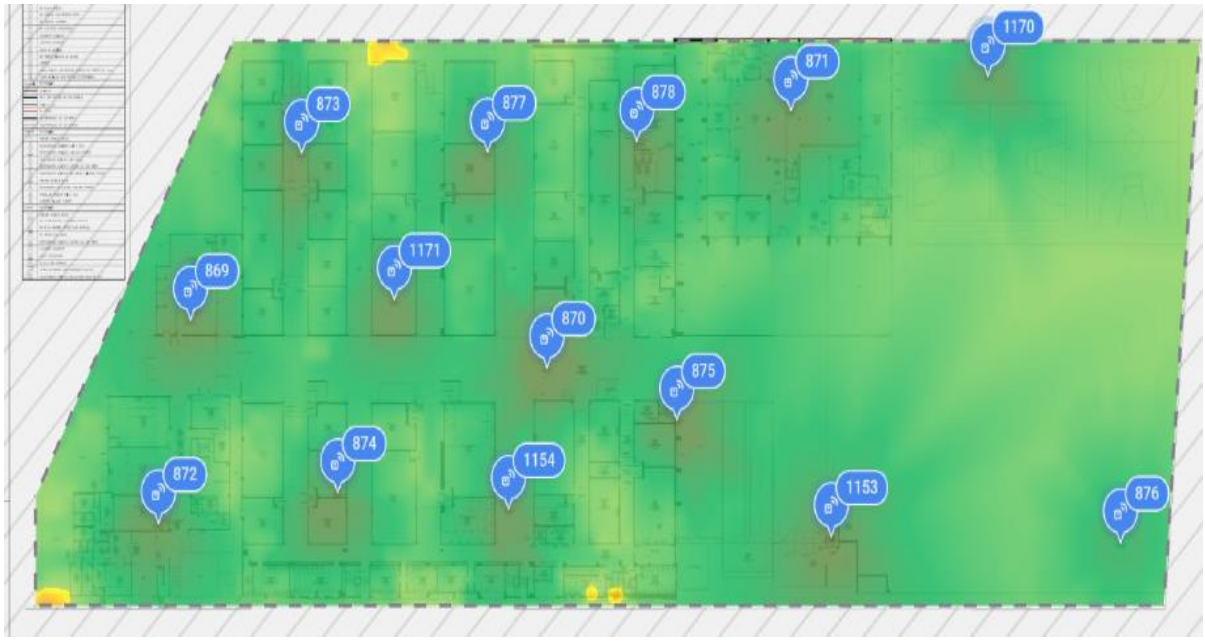


Campus Conceição – Disposição dos equipamentos no projeto

Campus Conceição – Primeiro Andar



Campus Conceição – Térreo

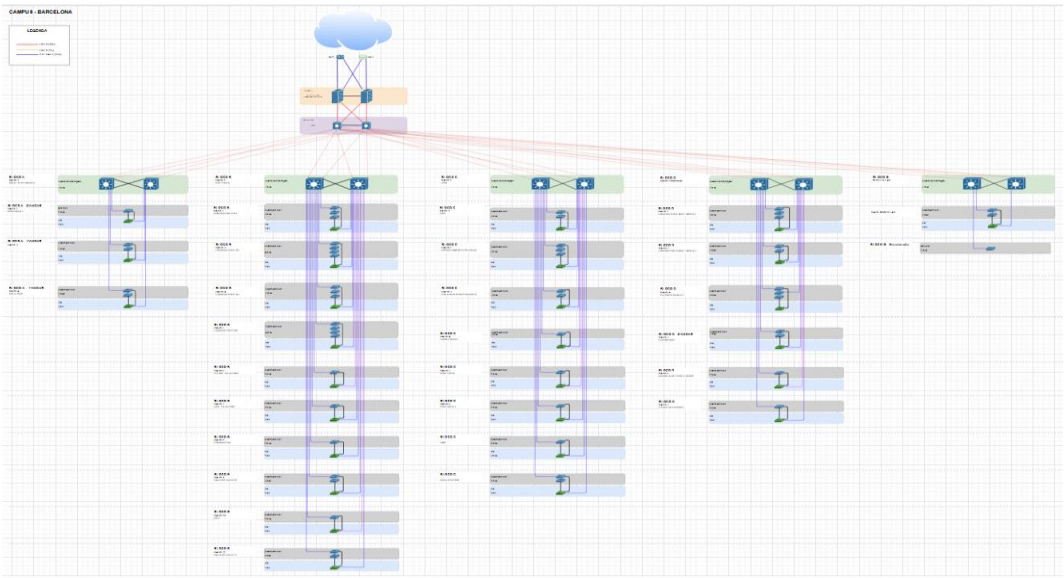


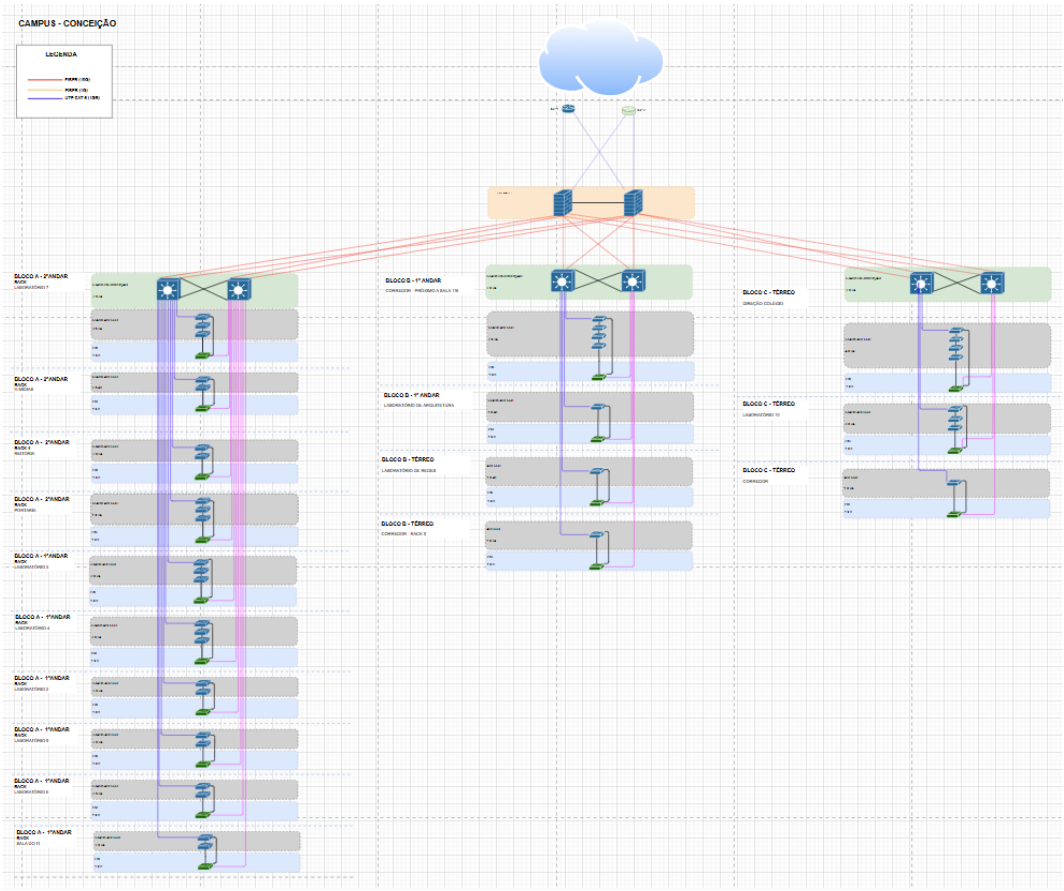
Campus Itapetininga - Disposição dos equipamentos no projeto

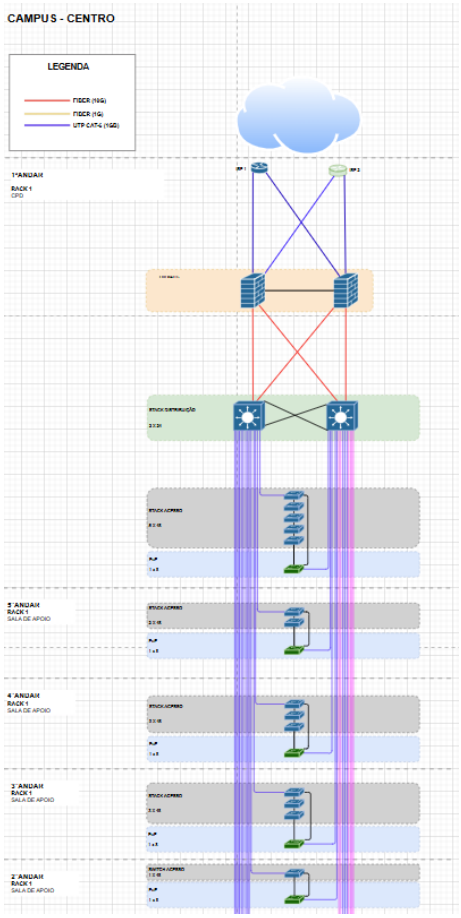
Campus Itapetininga

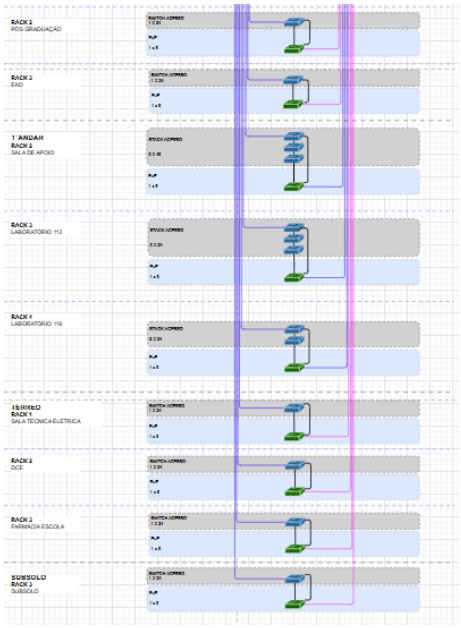
Campus Itapetininga - Atual

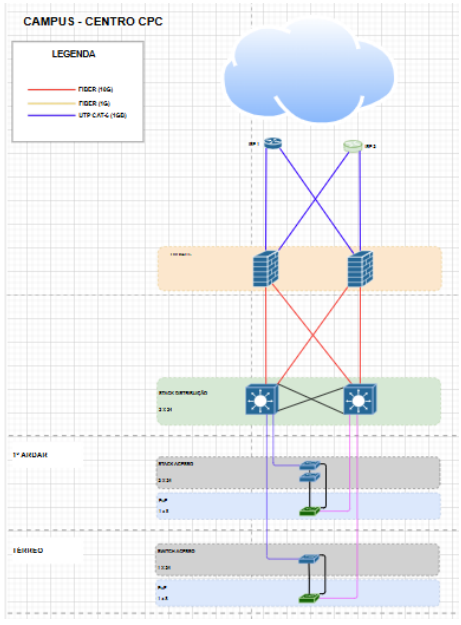
TOPOLOGIA E INTERCONEXÕES

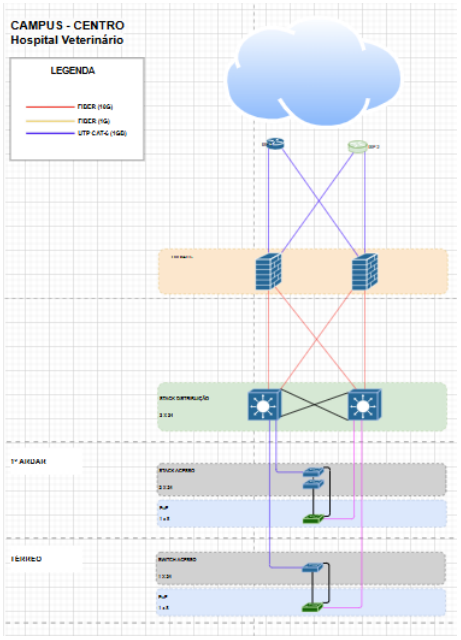


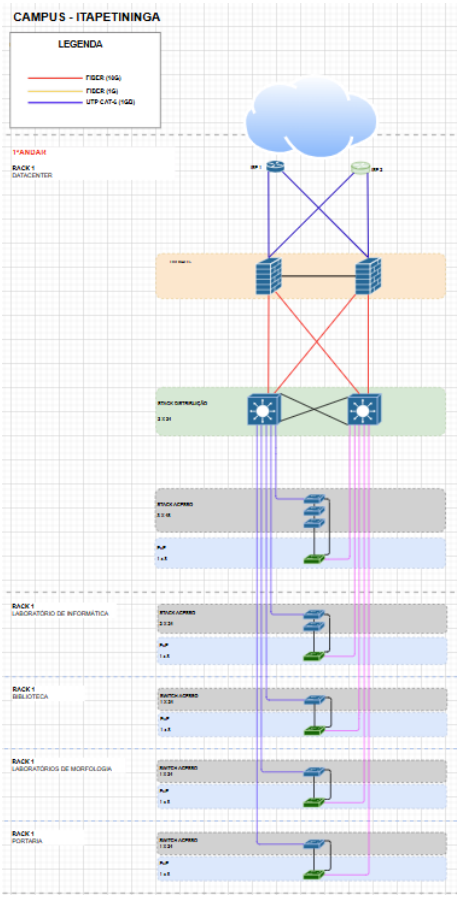


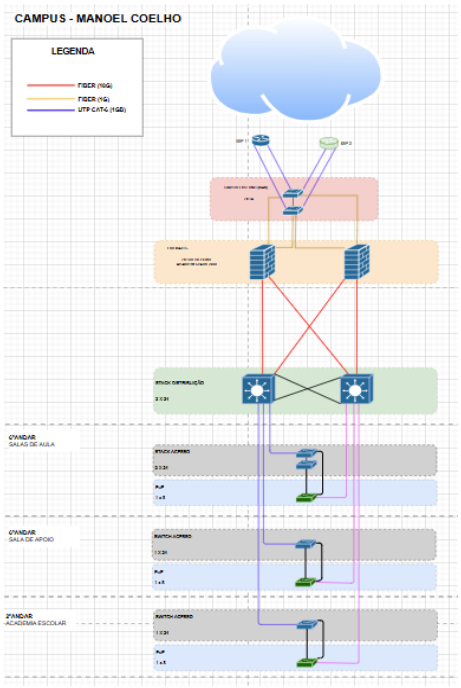

CAMPUS - CENTRO
LEGENDA
1º ANDAR
RACK 1
CPD
5º ANDAR
RACK 1
SALA DE APOIO
4º ANDAR
RACK 1
SALA DE APOIO
3º ANDAR
RACK 1
SALA DE APOIO
2º ANDAR
RACK 1
SALA DE APOIO


RACK 2
PÓS GRADUAÇÃO
RACK 3
EAD
1º ANDAR
RACK 2
SALA DE APOIO
RACK 3
LABORATÓRIO 112
RACK 4
LABORATÓRIO 116
TÉRREO
RACK 1
SALA TÉCNICA ELÉTRICA
RACK 2
DCE
RACK 3
FARMÁCIA ESCOLA
SUBSOLO
RACK 2
SUBSOLO


CAMPUS - CENTRO CPC
LEGENDA
1º ANDAR
TÉRREO


CAMPUS - CENTRO
Hospital Veterinário
LEGENDA
1º ANDAR
TÉRREO


CAMPUS - ITAPETININGA
LEGENDA
FIBER (10G)
FIBER (1G)
UTP CAT-6 (1GD)
1°ANDAR
RACK 1
DATACENTER
RACK 1
LABORATÓRIO DE INFORMÁTICA
RACK 1
BIBLIOTECA
RACK 1
LABORATÓRIOS DE MORFOLOGIA
RACK 1
PORTARIA


CAMPUS - MANOEL COELHO
LEGENDA
FIBER (10G)
FIBER (1G)
UTP CAT-6 (1GD)
0°ANDAR
SALAS DE AULA
0°ANDAR
SALA DE APOIO
2°ANDAR
ACADEMIA ESCOLAR

ANEXO XVII

ANEXO LC-01 - TERMO DE CIÊNCIA E DE NOTIFICAÇÃO
(Contratos)

Contratante: Universidade Municipal de São Caetano do Sul

Contratada: _____

Contrato nº (de origem):_____

OBJETO: Contratação de empresa especializada para para fornecer Solução de Serviço gerenciado para gestão ativos de rede WiFi, monitoramento e segurança, incluindo fornecimento de softwares, equipamentos e licenciamentos na modalidade *As a Service*, suporte técnico especializado, acessórios e garantia para atendimento da Universidade Municipal de São Caetano do Sul, conforme condições e especificações constantes no Termo de Referência do Edital.

Advogado (S)/ nº OAB: (*)_____

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, conforme dados abaixo indicados, 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 do Estado, Caderno do Poder Legislativo, parte do Tribunal de Contas do Estado de São Paulo, 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 do responsável pela contratante estão cadastradas no módulo eletrônico do "Cadastro Corporativo TCESP – CadTCESP", nos termos previstos no artigo 2º da Instrução nº 01/2020, conforme "Declaração de Atualização Cadastral" anexa;

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.

São Caetano do Sul, ___de _____de 2026.

Autoridade Máxima da Universidade Municipal de São Caetano do Sul.

Nome: _____

Cargo: _____

CPF: _____

Responsável pela Homologação e adjudicação do Certame.

Nome: _____

Cargo: _____

CPF: _____

Assinatura:_____

Responsáveis que assinam o instrumento Contratual

Pela USCS

Nome: _____

Cargo: _____

CPF: _____

Assinatura:_____

Pela Contratada

Nome: _____

Cargo: _____

CPF: _____

Assinatura:_____

Ordenador de Despesas da Universidade Municipal de São Caetano do Sul

Nome: _____

Cargo: _____

CPF: _____

Assinatura:_____

Agentes públicos responsáveis pela gestão do instrumento contratual

Gestor do Contrato

Nome: _____

Cargo: _____

CPF: _____

Assinatura: _____

Fiscalizador técnico do Contrato

Nome: _____

Cargo: _____

CPF: _____

Assinatura: _____

Demais Responsáveis (**):
Tipo de ato sob sua responsabilidade:
Nome:_____
Cargo:_____
CPF:_____
Assinatura:_____

Advogado
(*). Facultativo, indicar quando já constituído, informando, inclusive, o endereço eletrônico.

(**) - O Termo de Ciência e Notificação e/ou Cadastro do(s) Responsável(is) 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 Notificação, será ele objeto de notificação específica. (inciso acrescido pela Resolução nº 11/2021).

ANEXO LC-02 - DECLARAÇÃO DE DOCUMENTOS À DISPOSIÇÃO DO TCE-SP

CONTRATANTE: UNIVERSIDADE MUNICIPAL DE SÃO CAETANO DO SUL

CNPJ Nº: 44.392.215/0001-70

CONTRATADA:

CNPJ Nº:

CONTRATO N° ____/2026

DATA DA ASSINATURA: ___/__/2026

VIGÊNCIA: 24 meses.

OBJETO: Contratação de empresa especializada para para fornecer Solução de Serviço gerenciado para gestão ativos de rede WiFi, monitoramento e segurança, incluindo fornecimento de softwares, equipamentos e licenciamentos na modalidade *As a Service*, suporte técnico especializado, acessórios e garantia para atendimento da Universidade Municipal de São Caetano do Sul, conforme condições e especificações constantes no Termo de Referência do Edital.

Valor global R$ _____ (_____).

Declaro, na qualidade de responsável pela entidade supra epigrafada, sob as penas da Lei, que os demais documentos originais, atinentes à correspondente licitação, encontram-se no respectivo processo administrativo arquivado na origem à disposição do Tribunal de Contas do Estado de São Paulo, e serão remetidos quando requisitados.

São Caetano do Sul, ___ de _____ de 2026.

_____

Prof. Dr. Leandro Campi Prearo – Reitor

Universidade Municipal de São Caetano do Sul - USCS

leandro.prearo@online.uscs.edu.br

ANEXO PC-02 - CADASTRO DO RESPONSÁVEL

Entidade: UNIVERSIDADE MUNICIPAL DE SÃO CAETANO DO SUL

Nome:

Cargo:

CPF:

Período de gestão: 01 de março de 2025 a 28 de fevereiro de 2029.

Obs: 1. Todos os campos são de preenchimento obrigatório.

2. Repetir o quadro, se necessário, informando todos os responsáveis durante o exercício.

3. Anexar a “Declaração de Atualização Cadastral” emitida pelo sistema

“Cadastro Corporativo TCESP – CadTCESP”, por ocasião da remessa do presente documento ao TCESP”.

As informações pessoais dos responsáveis estão cadastradas no módulo eletrônico do Cadastro TCESP, conforme previsto no Artigo 2º das Instruções nº01/2020, conforme “Declaração de Atualização Cadastral” ora anexada (s).

_____

Nome e assinatura do responsável pelo preenchimento

ANEXO XVIII
ESTUDO TÉCNICO PRELIMINAR

1. Considerações Iniciais

A USCS, ao longo dos últimos anos, ampliou significativamente sua estrutura física com inauguração de novos *campis*. A título de exemplo, foi inaugurado em março de 2022 o campus Itapetininga e em fevereiro/2024 o Campus Centro II.

A última aquisição de equipamentos de rede data de meados de 2017. Desde então, para as novas instalações tem-se usado de soluções paliativas para o atendimento dessa nova demanda.

Ocorre que, ante o crescimento do número de usuários, chegou-se em determinado ponto próximo ao limite da capacidade dos equipamentos disponíveis, de forma que não é possível a adoção de novas soluções de contorno.

Conforme processo de compra nº 441/2024, que resultou no pregão presencial nº 03/2024, atualmente suspenso *sine die,* foi realizado estudo técnico preliminar que concluiu à época pela contratação de solução da fabricante ARUBA, que era utilizado somente no Campus Centro, com o intuito de manter a padronização do parque tecnológico existente.

Todavia, em melhor análise no curso do processo, entendeu-se por verificar a possibilidade de atendimento das necessidades institucionais com outras soluções, com o mesmo padrão técnico esperado, mas que pudesse ampliar a competitividade do certame, e consequentemente, resultasse na melhor contratação para essa Administração Pública, o que restou confirmado após análise de outras soluções de mercado e de outras contratações públicas.

Há de se destacar que dado o volume previsto no processo de compra nº 441/2024, e em comparação com o volume de ativos atualmente em uso, o quantitativo de itens da nova aquisição é substancialmente superior, de forma que a contratação por *part number* apenas para atender a compatibilidade com aquele pequeno quantitativo poderia resultar em uma contratação excessivamente onerosa à USCS. Ademais, a contratação por *part number* limita a infraestrutura à uma tecnologia defasada em relação a nova realidade do mercado e, que, portanto, vai representar uma menor vida útil dos equipamentos que serão adquiridos.

A nova contratação, independente do objeto ser atrelado a um *part number* ou não, deve manter todos os requisitos de negócio e de tecnologia, inclusive, a compatibilidade com as soluções atualmente utilizadas pela USCS.

Desta forma, é que se torna necessário a análise de soluções que reflitam a nova realidade da USCS, o que se faz por meio deste Estudo Técnico Preliminar.

2. Objetivo

Esse estudo técnico preliminar tem o objetivo de analisar possíveis soluções técnicas que atendam às necessidades da Universidade Municipal de São Caetano do Sul – USCS, ante a necessidade de substituição e ampliação da infraestrutura de rede da Universidade, indicando, quando possível, a solução mais viável para os interesses da Instituição.

3. Descrição da necessidade

3.1 Motivação/Justificativa

Com o aumento do número da oferta de vagas ofertadas pela Instituição para seus cursos, a demanda de serviços em ambiente online foi impactada. Não somente, mas por ocasião da pandemia do COVID-19, a necessidade de digitalização dos serviços exigiu uma maior capacidade da USCS em relação aos serviços de rede.

Além dos equipamentos de interconectividade existentes na USCS, o parque computacional da instituição conta com uma infraestrutura de rede que deve ser considerada no processo de modernização tecnológica. Essa infraestrutura inclui o ambiente de virtualização, baseado em VMware e Microsoft Hyper-V, bem como servidores físicos e virtuais operando com sistemas Windows Server 2019, 2022 e 2025.

Dessa forma, é fundamental que a solução a ser contratada apresente plena compatibilidade e interoperabilidade com o ambiente tecnológico existente, garantindo integração eficiente, estabilidade operacional e continuidade dos serviços de rede e computação.

É importante destacar que a USCS atendia aproximadamente 6 (seis) mil alunos, quando da última aquisição de equipamentos de rede. E, hoje possui mais de 12 (doze) mil, além de 2 (dois) novos *campis*. Cabe dizer ainda, que a USCS possui estruturas dedicadas ao atendimento à comunidade de São Caetano do Sul, como o Colégio Universitário, Hospital Veterinário, Centro de Pesquisas Clínicas, Clínicas Odontológica, dentre outros, ampliando significativamente na necessidade de conectividade para tais atividades.

Estima-se com o aumento do número da oferta de vagas ofertadas pela Instituição para seus cursos mais de 10.000 (dez mil) acessos simultâneos.

3.2 Necessidades de negócio

3.2.1. Continuidade dos serviços de TIC: Prover o aporte tecnológico necessário, para a implantação e a sustentação dos sistemas institucionais, em consonância com a arquitetura tecnológica computacional.

3.2.2. Conformidade: Alinhamento às boas práticas e condições de mercado para assegurar um ambiente tecnológico compatível.

3.2.3. Manutenção e sustentabilidade: Prover e atualizar continuamente os recursos e ferramentas de Tecnologia da Informação.

3.2.4. Garantia e suporte: Manter o parque atualizado com garantia e suporte às aplicações

3.2.5. Segurança e privacidade: Prover mecanismos de segurança, compatível com a camada em que esses equipamentos se enquadram, visando a conferir confidencialidade, integridade e disponibilidade dos dados trafegados nos equipamentos de tecnologia.

3.3 Necessidades tecnológicas

3.3.1. Necessidade tecnológicas - governança

3.3.1.1. Alta disponibilidade: Fornecimento de infraestrutura tecnológica com certa redundância de ativos computacionais, constituindo serviços/sistemas mais resilientes e tolerantes a determinadas falhas em equipamentos e componentes de tecnologia da informação.

3.3.1.2. Mitigação de riscos relativos à mudança e migração: Capacidade de migração das cargas de processamento da infraestrutura atual para a nova com riscos mitigados quanto à continuidade das operações e disponibilidade.

3.3.1.3. Gerenciamento e monitoração: Capacidade de acompanhar, metrificar e realizar atividades em ativos e componentes computacionais por meio de interfaces de gerenciamento, que permitam o monitoramento o uso e a capacidade disponível de tais equipamentos.

3.3.1.4. Escalabilidade e flexibilidade: Capacidade da solução ser adaptável, fornecendo infraestrutura para que os sistemas/serviços abrigados consigam ser expandidos, visando a atender, da melhor forma, às necessidades organizacionais.

3.3.1.5. Auditoria e controle: Fornecer maneiras de controle e auditoria, compatível com a camada em que esses equipamentos de tecnologia da informação se enquadram, visando a propiciar registros de acessos, definir papéis e suas respectivos privilégios e demais funcionalidades empregadas para se permitir o rastreio e controle de usuários.

3.3.1.6. Atualização tecnológica: Capacidade de oferecer o aporte tecnológico necessário para a implantação de novos serviços, em consonância com as novas tecnologias disponíveis no mercado.

3.3.2 Necessidades tecnológicas - requisitos técnicos esperados

3.3.2.1 O levantamento de necessidade técnicas encontram-se descritos no documento em anexo - Apêndice “A” deste Estudo Técnico Preliminar.

3.3.2.2 As especificações técnicas mínimas apuradas para atendimento as necessidades encontram-se descritas no anexo – Apêndice “B” deste Estudo Técnico Preliminar.

3.3.3 Os quantitativos estimados para o atendimento a demanda encontram-se descritos no anexo – Apêndice “A” deste Estudo Técnico Preliminar.

3.3.4 Demais requisitos necessários e suficientes à escolha da Solução de tecnologia da informação

3.3.4.1. Compatibilidade e integração: Compatibilidade e integração com os dispositivos que compões a infraestrutura de tecnologia da informação da USCS, a saber: storages, servidores, firewalls, switches SAN e LAN.

3.3.4.2. Níveis de serviço: Assegurar funcionamento dos sistemas/serviços essenciais de tecnologia de informação, que estão em ambiente produtivo, nos níveis adequados às necessidades da Universidade, conforme catálogo de serviços.

3.3.4.3. Continuidade do negócio: Capacidade de oferecer recursos de tecnologia para processamento de dados, atendendo diversos processos de negócio da USCS que estão dispostos em sistemas/serviços de tecnologia ou que, em algum momento, passam por essa infraestrutura.

3.3.4.4. Economicidade: Capacidade de escolher soluções alcancem os objetivos almejados – eficácia –, buscando obter a relação custo x benefício mais vantajosa para a Administração, bem como preservando os investimentos já realizados em recurso de tecnologia existentes.

4. Levantamento de soluções

Esse tópico tem o escopo de analisar as alternativas de mercado que atendam às necessidades de negócio e tecnologia da USCS, em relação à infraestrutura de redes. Nesse sentido, deverão ser analisados para fins comparativos os seguintes aspectos:

i. Do ponto de vista da parte de serviço agregado: disponibilidade de suporte técnico especializado de acordo com as necessidades de negócio da Instituição, garantia dos equipamentos, instalação/implantação e monitoramento da infraestrutura de rede;

ii. Do ponto de vista dos equipamentos: atendimento aos requisitos descritos pela área de tecnologia, longevidade da solução, possibilidade de ampliação e atualização da alternativa proposta;

iii. Do ponto de vista econômico/financeiro: atendimento ao orçamento da Instituição para resolução da demanda e flexibilidade para ajustes nos quantitativos (acréscimo e decréscimo).

4.1 Alternativas do mercado

Dentre as soluções analisadas, são possíveis as seguintes:

a) Aquisição de ativos de rede (Switch, Ponto de Acesso Wi-Fi e Controladora) e licenciamento, com instalação, garantia e repasse de conhecimento;

b) Aquisição de ativos de rede (Switch, Ponto de Acesso Wi-Fi e Controladora) e licenciamento, com instalação, suporte, garantia, repasse de conhecimento e monitoramento;

c) Contratação de solução gerenciada de ativos de rede (Switch, Ponto de Acesso Wi-Fi e Controladora) incluindo fornecimento de equipamentos licenciados, suporte técnico especializado, acessórios, garantia e monitoramento.

4.1.1 Aquisição de ativos de rede (Switch, Ponto de Acesso Wi-Fi e Controladora) e licenciamento, com instalação, garantia e repasse de conhecimento

i. Do ponto de vista da parte de serviço agregado: Essa modalidade de contrato prevê exclusivamente aquisição direta dos equipamentos com garantia do fabricante e licenciamento. A instalação dos equipamentos deverá ser realizada pela equipe da USCS. Da mesma forma, acontece com o suporte técnico, que deverá ser absorvido pelo departamento de Tecnologia da Informação. O monitoramento da infraestrutura de rede não faz parte do escopo desta modalidade de contratação, devendo também ser absorvido pelo time técnico do departamento de Tecnologia da Informação.

ii. Do ponto de vista dos equipamentos: O atendimento aos requisitos descritos pela área de tecnologia se dará independente da alternativa de mercado, eis que se trata de funcionalidades próprias dos equipamentos. A longevidade dos equipamentos é representada exatamente pela própria vida útil dos equipamentos. Eventual atualização está restrita ao prazo de garantia contratual e vida útil dos equipamentos. Eventual ampliação dependerá da realização de novos processos licitatórios. Eventual necessidade de substituição de equipamento defeituoso será realizada de acordo com garantia contratual;

iii. Do ponto de vista econômico/financeiro: O custo da contratação será validado posteriormente mediante a realização de pesquisa de preço junto ao mercado feito e/ou preço público. Eventual aditamento para ampliação ou decréscimo no que concerne aos equipamentos adquiridos não é viável dada a modalidade contratual.

4.1.2 Aquisição de ativos de rede (Switch, Ponto de Acesso Wi-Fi e Controladora) e licenciamento, com instalação, suporte, garantia, repasse de conhecimento e monitoramento

i. Do ponto de vista da parte de serviço agregado: Essa modalidade de contrato prevê aquisição dos equipamentos licenciados com instalação, garantia, repasse de conhecimento e monitoramento. O suporte desta modalidade se dará de acordo com o NMS (Nível Mínimo de Serviço), definido pela USCS, não onerando equipe da Instituição, que ficará responsável exclusivamente pela gestão contratual.

ii. Do ponto de vista dos equipamentos: O atendimento aos requisitos descritos pela área de tecnologia se dará independente da alternativa de mercado, eis que se trata de funcionalidades próprias dos equipamentos. A longevidade dos equipamentos é representada exatamente pela própria vida útil dos equipamentos. Eventual atualização está restrita ao prazo de garantia contratual e vida útil dos equipamentos. Eventual ampliação dependerá da realização de novos processos licitatórios. Eventual necessidade de substituição de equipamento defeituoso será realizada de acordo com garantia contratual;

iii. Do ponto de vista econômico/financeiro: O custo da contratação será validado posteriormente mediante a realização de pesquisa de preço junto ao mercado e/ou preço público. Eventual aditamento para ampliação ou decréscimo no que concerne aos equipamentos adquiridos não é viável dada a modalidade contratual. Quanto ao serviço de suporte técnico é possível realizar aditivos para acréscimo ou decréscimo dos percentuais fixados em lei.

4.1.3 Contratação de solução gerenciada de ativos de rede (Switch, Ponto de Acesso Wi-Fi e Controladora) incluindo fornecimento de equipamentos licenciados, suporte técnico especializado, acessórios, garantia e monitoramento

i. Do ponto de vista da parte de serviço agregado: Essa modalidade de contrato prevê a entrega de solução gerenciada de ativos de rede (Switch, Ponto de Acesso Wi-Fi e Controladora) com a disponibilização dos equipamentos licenciados devidamente instalados e monitoramento das aplicações.

ii. Do ponto de vista dos equipamentos: O atendimento aos requisitos descritos pela área de tecnologia se dará independente da alternativa de mercado, eis que se trata de funcionalidades próprias dos equipamentos. A longevidade dos equipamentos é equivalente ao prazo de duração contratual, eis que a disponibilização dos equipamentos e acessórios é encargo contratual da contratada. Em eventual necessidade de substituição dos equipamentos, será realizada de acordo com o NMS (Nível Mínimo de Serviço), conforme determinado pela USCS.

iii. Do ponto de vista econômico/financeiro: O custo da contratação será validado posteriormente mediante a realização de pesquisa de preço junto ao mercado e/ou preço público. Eventual ampliação ou decréscimo de serviços poderá ser objeto de aditivo contratual nos limites estabelecidos pela lei.

4.2 Conclusões acerca das alternativas de mercado

4.2.1 Aquisição de ativos de rede (Switch, Ponto de Acesso Wi-Fi e Controladora) e licenciamento, com instalação, garantia e repasse de conhecimento

Essa modalidade de contratação apresenta limitações que comprometem sua viabilidade para atender de forma eficiente às necessidades institucionais.

Primeiramente, a ausência de serviços agregados, como instalação, suporte técnico e monitoramento dos ativos de rede, transfere integralmente essas responsabilidades para a equipe de TI da USCS. No entanto, com o atual contingente não é possível agregar tais demandas. Além disso, não há previsão de realização de concursos públicos para ampliar o quadro funcional, e, devido à especialização do objeto, a instituição não dispõe de recursos humanos qualificados para assumir essas operações, o que demandaria não somente a realização do concurso público, mas também a criação da carreira de especialista por meio de projeto de lei específico para tanto.

Em segundo lugar, a atualização tecnológica fica restrita ao período de garantia e à vida útil dos equipamentos, exigindo novos processos licitatórios para ampliações, o que pode resultar em desatualização tecnológica e dificuldades operacionais.

E, por fim, a rigidez contratual impede ajustes posteriores, limitando a flexibilidade para adequações futuras, seja para ampliações das áreas atendidas ou mesmo para decréscimos.

Diante desses fatores, essa modalidade de contratação se mostra inviável do ponto de vista técnico e econômico.

4.2.2 Aquisição de ativos de rede (Switch, Ponto de Acesso Wi-Fi e Controladora) e licenciamento, com instalação, suporte, garantia, repasse de conhecimento e monitoramento

Essa modalidade de contratação tem como vantagem a inclusão do serviço de suporte técnico e monitoramento dos ativos de rede, em relação à alternativa indicada no item anterior (4.2.1). Também há vantagem em relação à possibilidade de ajustes nos quantitativos do escopo de serviço - suporte técnico e instalação.

Contudo, em relação a flexibilidade contratual no que diz respeito à possibilidade de ajustes nos quantitativos dos itens que serão objeto de aquisição, esta alternativa não comporta, demandando a realização de novas contratações.

A impossibilidade de aditamento para aquisição adicional ou redução de equipamentos compromete a flexibilidade da contratação, dificultando a adequação a eventuais mudanças nas necessidades institucionais. Apesar da possibilidade de ajustes no suporte técnico, essa restrição nos equipamentos pode resultar em custos elevados e menor eficiência operacional a longo prazo.

Dessa forma, essa modalidade não se apresenta como a alternativa mais viável, pois impõe entraves à modernização, limita a capacidade de resposta da Instituição às inovações tecnológicas e pode gerar impactos financeiros desfavoráveis no médio e longo prazo.

4.2.3 Contratação de serviço gerenciado de solução para gestão ativos de rede, monitoramento e segurança, incluindo fornecimento de softwares, equipamentos, licenciamentos, suporte técnico especializado, acessórios e garantia.

A contratação nesta modalidade traz como benefício principal a possibilidade da USCS manter seu parque tecnológico sempre atualizado e, portanto, compatível com as principais soluções de mercado. Além disso, tem como outra vantagem um ganho de escala em relação às necessidades institucionais.

Importante destacar que dentre as alternativas analisadas, é a que oferece a maior resiliência e confiabilidade para a Instituição, tendo em vista que toda a disponibilização e reposição por eventuais falhas deverá ser atendida pela contratada, de acordo com o NMS (Nível Mínimo de Serviço) definidas pela USCS, levando em consideração a criticidade e tolerância à indisponibilidade para tais serviços. Essa abordagem reduz a sobrecarga da equipe interna, permitindo que a Instituição não tenha necessidade de alocação de recursos adicionais para prover qualquer tipo de suporte técnico.

Além disso, a longevidade dos equipamentos está assegurada durante todo o período contratual, com substituições previstas conforme os NMS (Níveis Mínimos de Serviços) estabelecidos, garantindo a continuidade operacional sem riscos de obsolescência tecnológica.

Esta modalidade contratual permite certa flexibilidade em relação a verificação contínua do atendimento aos interesses institucionais e de tecnologia da informação da USCS.

Dessa forma, essa alternativa proporciona maior previsibilidade financeira, modernização contínua e otimização dos recursos institucionais.

4.2.4 Análise comparativa de custos

A análise comparativa de custos não é aplicável ao presente caso, eis que apenas uma alternativa se mostrou viável, não havendo, portanto, parâmetro comparativo que permita a realização de estudo nesse sentido.

De igual forma, para fins de estimativa de custos, dada as especificidades do objeto e dos seus quantitativos, não foi localizada nenhuma contratação com características do volume de quantitativos – número de locais de atendimento, locais de atendimento, número de chamados, quantitativo de usuários internos e externos etc. – que pudessem servir de referência para a estimativa dos custos de contratação.

Assim, deverá ser providenciada a cotação de preços para fins de estimativa de custos.

4.2.5 Justificativa técnica da escolha da solução

Assim, conclui-se que: o contrato na modalidade de serviço se apresenta como a solução mais viável. Essa modalidade permite ajustes com menor impacto, garantindo que os serviços estejam sempre de acordo com as necessidades mais atuais da USCS, tanto no aspecto qualitativo, quanto no aspecto quantitativo. O que não ocorre com as demais alternativas, uma vez que em qualquer uma delas, os equipamentos passam a pertencer à Universidade.

Em outros termos, por exemplo, em eventual caso de redução da demanda, não seria possível a devolução dos equipamentos adquiridos, já que pertencem ao inventário da Instituição. Da mesma forma, é o caso de atualizações tecnológicas que demandem novos padrões de compatibilidade com outras soluções da USCS, que não seriam possíveis em caso de contrato de aquisição de equipamentos, conforme analisado nas demais alternativas.

Em ambos os casos, na modalidade de contratação como serviço é possível reavaliar periodicamente a adequação da solução à realidade da USCS naquele dado momento, podendo concluir-se pela realização até mesmo de uma nova contratação sem impacto financeiro significativo.

O modelo de contratação como serviço se mostra altamente eficaz à medida que a efetividade do serviço é aferida constantemente por meio de acordo de nível de serviço, que preveem, dentro outros: prazo de entrega, atendimento de eventuais chamados para serviço de suporte, qualificação mínima da equipe técnica alocada, metas de desempenho e disponibilidade do serviço contratado. Inclusive, com previsão de glosas contratuais e outras penalidades em caso de não atendimento a contento. Noutro giro, na modalidade de aquisição não há como efetivar tais controles.

5. Parcelamento ou não da contratação

A presente contratação se dará em lote único subdividido em itens agrupados pelos ativos de rede (Switch, Ponto de Acesso Wi-Fi e Controladora), semelhantes. O agrupamento em lote único decorre da necessidade de que todos os serviços sejam, além de compatíveis e integrados entre si, entregues pelo mesmo fornecedor.

Desta forma, tem-se a seguinte formação:

LOTE	ITEM	DESCRIÇÃO	QTDE DE EQUIPAMENTOS	MÉTRICA	QTDE
1	**1**	**Serviço gerenciado de solução para gestão ativos de rede, monitoramento e segurança, incluindo fornecimento de softwares, equipamentos, licenciamentos, suporte técnico especializado, acessórios e garantia.**			
	1.1	**Serviço gerenciado de Switch, incluindo fornecimento de equipamentos licenciados, suporte técnico especializado, acessórios, garantia e monitoramento.**			
	1.1.1	**Switch de acesso tipo 1**, incluindo equipamentos licenciados, suporte técnico especializado, acessórios, garantia e monitoramento.	28	Meses	24
	1.1.2	**Switch de acesso tipo 2**, incluindo equipamentos licenciados, suporte técnico especializado, acessórios, garantia e monitoramento.	2	Meses	24
	1.1.3	**Switch de acesso tipo 3**, incluindo equipamentos licenciados, suporte técnico especializado, acessórios, garantia e monitoramento.	2	Meses	24
	1.1.4	Implementação – instalação e configuração – da solução de Switch.	1	Quantidade de Equipamentos	32
	1.2	**Serviço gerenciado de Ponto de Acesso (AP), incluindo fornecimento de equipamentos licenciados, suporte técnico especializado, acessórios, garantia e monitoramento.**			
	1.2.1	**Ponto de acesso tipo 1** incluindo fornecimento de equipamentos licenciados, suporte técnico especializado, acessórios, garantia e monitoramento.	185	Meses	24
	1.2.2	**Ponto de acesso tipo 2** incluindo fornecimento de equipamentos licenciados, suporte técnico especializado, acessórios, garantia e monitoramento.	12	Meses	24
	1.2.3	**Ponto de acesso tipo 3** incluindo fornecimento de equipamentos licenciados, suporte técnico especializado, acessórios, garantia e monitoramento.	12	Meses	24
	1.2.4	**Ponto de acesso tipo 4** incluindo fornecimento de equipamentos licenciados, suporte técnico especializado, acessórios, garantia e monitoramento.	6	Meses	24
	1.2.5	**Ponto de acesso tipo 5** incluindo fornecimento de equipamentos licenciados, suporte técnico especializado, acessórios, garantia e monitoramento.	4	Meses	24
	1.2.6	Implementação – instalação e configuração – da solução de Ponto de Acesso.	1	Quantidade de Equipamentos	219
	1.3	**Serviço gerenciado de solução para gestão de ativos de rede, monitoramento e segurança, incluindo fornecimento de softwares, licenciamento e suporte técnico especializado, acessórios e garantia.**			
	1.3.1	Solução para gestão de switches, monitoramento e segurança, incluindo fornecimento de softwares, licenciamento e suporte técnico especializado.	1	Meses	24
	1.3.2	Solução para gestão de pontos de acesso, monitoramento e segurança, incluindo fornecimento de softwares, licenciamento e suporte técnico especializado.	1	Meses	24
	1.3.3	Implementação – instalação e configuração – da solução para gestão de Switches e Pontos de Acessos.	1	Qtde de Equipamentos	251

6. Capacitação Profissional

6.1. A empresa a ser contratada deverá indicar que dispõe de equipe técnica mínima compatível com as exigências de cunho técnico/tecnológicos para suportar a implantação, configuração, suporte técnico e manutenção, bem como as atividades necessárias à prestação dos serviços vinculados ao objeto do certame.

6.2. A empresa a ser contratada deverá apresentar, no ato de celebração de contrato, a comprovação de certificação técnica necessária da equipe de trabalho designada para consecução do projeto

7. Subcontratação

A pricípio nNão será admitida a subcontratação, tendo em vista a especificidade do objeto, e que o lote já corresponde à menor unidade divisível para o serviço pretendido.

8. Descrição da solução a ser contratada

8.1 Contratação de solução gerenciada de ativos de rede (Switches, Pontos de Acesso Wi-Fi e Controladora) incluindo fornecimento de equipamentos com licenciamento, suporte técnico especializado, acessórios, garantia e monitoramento para atendimento da Universidade Municipal de São Caetano do Sul – USCS.

8.2 A solução gerenciada de ativos de rede deve abranger a implantação, o fornecimento, configuração, gerenciamento e monitoramento contínuo de Switches, Pontos de Acesso Wi-Fi e Controladora para garantir alta disponibilidade, segurança e desempenho da infraestrutura de TI da USCS.

8.3 A solução prevê a disponibilização de equipamentos de última geração, conforme requisitos e quantitativos a seguir apresentados, devendo todos serem licenciados de modo a garantir o seu funcionamento adequado, bem como a segurança das aplicações da USCS e o suporte contínuo.

8.4 A contratação da solução prevista deve se dar pelo período de 24 (vinte e quatro) meses podendo ser prorrogado ao interesse da administração pública, e nos termos da legislação vigente.

8.5 A solução deve contemplar o serviço técnico especializado e monitoramento da infraestrutura de tecnologia, para atender o seguinte escopo:

8.5.1 O serviço de suporte operacional especializado deverá ser disponibilizado para apoiar as necessidades oriundas dos objetos dos itens deste documento, podendo ser realizado de forma presencial e/ou remota.

8.5.2 O serviço deverá ter as seguintes características:

8.5.2.1 Trabalhar em estreita colaboração com Diretoria de Tecnologia da Informação e Inovação, como equipes de suporte técnico, analistas de rede e equipes de segurança cibernética, para resolver problemas complexos, implementar mudanças e melhorias na infraestrutura de rede da universidade;

8.5.2.2 Acompanhar o monitoramento de rede e da controladora, receber alertas e notificações de problemas de rede, como interrupções de serviço e quedas de conexão. Investigar e resolver esses alertas/notificações, garantindo o mínimo de tempo de inatividade e impacto nos serviços;

8.5.2.3 Realizar verificações regulares de rotina, atualizações de firmware, instalação de patches de segurança e outras atividades para manter a rede em bom estado de funcionamento;

8.5.2.4 Avaliar novas funcionalidades e sugerir ajustes que possam melhorar a eficiência e a segurança da rede;

8.5.2.5 Realizar novas instalações, configurações, suporte técnico, manutenções preventivas e corretivas dos equipamentos e softwares (Switches, Ponto de Acesso Wi-Fi e Controladora);

8.5.2.6 Reportar e elaborar notas técnicas sobre problemas graves para a DTI quando solicitado;

8.5.2.7 Criação e acompanhamento no preenchimento de Requisição de Mudança (RDM) na infraestrutura de rede, seguindo os procedimentos de gerenciamento de mudanças estabelecidos pela USCS. Isso envolve a análise de impacto, planejamento, execução e documentação das alterações realizadas;

8.5.2.8 Monitorar e garantir que os NMS (Níveis Mínimos de Serviços) sejam cumpridos;

8.5.2.9 Colaborar com equipes de projeto para implementar novas soluções de rede, como expansões, migrações ou atualizações tecnológicas de acordo com as demandas da USCS.

8.6 A solução é destinada ao atendimento dos colaboradores, discentes e docentes, bem como toda comunidade que utiliza os serviços da USCS, e deverá ser implementada nos seguintes endereços:

8.6.1. Campus Barcelona: Av. Goiás, 3400, Barcelona, São Caetano do Sul/SP, CEP 09550-051;

8.6.2. Campus Centro: R. Santo Antônio, 50 - Centro, São Caetano do Sul/SP, CEP 09521-160;

8.6.3. Campus Centro II: R. Samuel Klein, 83, Centro, São Caetano do Sul/SP, CEP: 09510-125;

8.6.4. Hospital Veterinário Universitário: R. Pernambuco, 76 - Centro, São Caetano do Sul/SP, CEP 09521-140;

8.6.5. Centro de Pesquisas Clínicas: R. Santo Antônio, 117, Centro, São Caetano do Sul/SP, CEP 09521-160;

8.6.6. Campus Conceição: R. Conceição, 321, Santo Antônio, São Caetano do Sul/SP, CEP 09530- 060;

8.6.7. Campus Itapetininga: Av. Dr. Ciro Albuquerque, 4750 - Taboãozinho, Itapetininga - SP, CEP 18200-021.

8.1. Níveis mínimos de serviço - NMS

8.1.1. Níveis mínimos de serviço exigidos

8.1.1.1. Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pela USCS para aferir objetivamente os resultados pretendidos com a contratação. São considerados para a presente contratação os seguintes indicadores:

8.1.1.2 Para a medição dos índices de nível de serviços, serão considerados os seguintes conceitos:

8.1.1.2.1 **Incidente:** É uma interrupção não planejada de um serviço de TI ou uma redução de qualidade de um serviço de TI;

8.1.1.2.2 **Problema:** é a causa desconhecida de um ou mais incidentes ou os problemas são a causa de um ou mais incidentes;

8.1.1.2.3 **Severidade:** Solicitações de alteração do nível de severidade poderá ser submetida à CONTRATADA e, quando julgadas pertinentes, serão prontamente atendidas, conforme tabela a seguir:

Severidade	Descrição
Crítica	Indisponibilidade total dos serviços.
Alto	Degradação dos serviços.
Normal	Falha parcial dos serviços.

8.1.1.1.1. IMPLEMENTAÇÃO - Serviços de Entrega, Instalação e Configuração da solução:

8.1.1.1.1.1. Todos os produtos (100%) deverão ser entregues nos quantitativos e localidades indicadas, instalados e configurados em conformidade com a especificação, dentro dos prazos máximos estipulados neste Termo, assim como previsto no termo de inserção.

8.1.1.1.1.2. Será verificada a conformidade com as especificações técnicas, assim como mensurado o prazo de entrega da solução, conforme detalhamento dos indicadores de nível de serviço indicados a seguir.

8.1.1.1.1.3. Em caso de eventual falta de instalação ou configuração, decorrentes de falha de infraestrutura que deva ser provida pela USCS, por exemplo, mas não limitado há falha no cabeamento estruturado, de energia, ou *links* de internet, não caberá nenhum tipo glosa ou penalidade a contratada.

8.1.1.1.1.4. Em caso de eventual vício ou defeito no cabeamento estruturado, exclusivamente, seja para *uplink* (interconexão entre switches) ou para conexão de pontos de acesso de rede sem fio (equipamento Wi-Fi), deverá a contratada prover a solução técnica às suas expensas.

8.1.1.1.1.4.1 A manutenção/substituição prevista no item 8.1.1.1.1.4 se limita a substituição de cabeamento e conectores, em pontos de até 100 (cem) metros ou múltiplos de 100 (cem).

8.1.1.1.1.4.2 Para fins de atendimento ao item 8.1.1.1.1.4, deverá a contratada, caso necessário, fornecer cabos, minimamente CAT6 ou fibra óptica(multimodo/monomodo), e conectores compatíveis com a estrutura.

8.1.1.1.2. Serviços de Garantia, Manutenção e Suporte Técnico:

8.1.1.1.2.1. **Severidade 1 – Crítica**: Serviço indisponível para grande número de usuários e/ou com alta degradação de performance. Serviço indisponível para o público interno/externo (docentes, discentes, colaboradores, terceirizados, e público externo), deverá ser iniciado em até 2 (duas) horas e o chamado solucionado em até 4 (quatro) horas corridas;

8.1.1.1.2.2. **Severidade 2 – Alta:** Serviço degradado, com risco iminente de indisponibilidade ou indisponível. Incidentes relacionados a usuários de alta prioridade (limitado a 3% dos usuários), deverá ser iniciado em até 4 (quatro) horas e o chamado solucionado em até 8 (oito) horas úteis;

8.1.1.1.2.3. **Severidade 3 – Normal:** Serviço apresentando problemas sem indisponibilidade ou degradação de performance para os usuários, eventos de alertas proativos sem impacto de negócios, deverá ser iniciado em até 24 (vinte e quatro) horas e o chamado solucionado em até 24 (vinte e quatro) horas úteis;

8.1.1.1.2.4. **Rotineiro:** Operações das ferramentas e equipamentos em geral tais como configuração em geral, parametrização de ferramentais, criação e/ou configurações de usuários e novas redes, deverá ser iniciado em até 24 (vinte e quatro) horas e o chamado solucionado em até 48 (quarenta e oito) horas úteis;

8.1.1.1.2.5. Para atendimento a chamados em que não haja necessidade de troca de peças ou intervenção local, será admitido o atendimento remoto, ao invés de presença no local de instalação da solução;

8.1.1.1.2.6. Horas comerciais, para fins de cálculo do NMS, são as compreendidas entre 8h e 18h, horário de Brasília, em dias úteis, exceto para chamados de **SEVERIDADE 1**, que deverá ser atendido entre 8h e 22h;

8.1.1.1.2.7. Por início de atendimento entende-se o registro do chamado em ferramenta própria da Contratada para início da tratativa, a fim de efetuar a correção do incidente, requisição ou o *troubleshooting* preciso, com interlocução direta com a equipe da USCS;

8.1.1.1.2.8. Um chamado técnico somente poderá ser fechado após o aceite da USCS e o término de atendimento se dará com a disponibilidade do recurso para uso em perfeitas condições de funcionamento.

8.1.1.1.2.9. Um chamado fechado, sem anuência da USCS ou sem que o problema tenha sido de fato resolvido, será reaberto e os prazos serão contados a partir da data de abertura original do chamado, inclusive para efeito de aplicação das multas e sanções previstas.

8.1.1.1.2.10. No final do atendimento, o técnico da contratada deverá elaborar um relatório de ocorrência onde conste o problema causador do chamado, a solução encontrada, as pendências, a data e hora do chamado, do início e do fim do atendimento. Esse relatório deve ter a concordância e assinatura de um técnico da USCS.

8.1.2. **Detalhamento dos indicadores de nível de serviço**

8.1.2.1. Caso a contratada não atinja os níveis mínimos de serviço fixados, não venha a produzir os resultados esperados, deixe de executar as atividades contratadas, deixe de utilizar os materiais e recursos humanos exigidos para fornecimento da solução, ou utilize-os com qualidade ou quantidade inferior à demandada, estará, conforme cada caso, sujeita a aplicação de glosas nos valores estabelecidos para multas e/ou penalidades ou retenção do pagamento até que as pendências sejam sanadas.

No documento termo de referência será aportado os indicadores de verificação de atraso na entrega do objeto; indicador de verificação de suporte atendido dentro do prazo estipulado de acordo com o grau de exigência, aqui definido como crítica alta e normal; indicador de permanência, peça ou componente backup; e indicador de saúde operacional.

Apêndice

Apêndice “A” - Levantamento de Necessidades Técnicas

Apêndice "A" - Levantamento de Necessidades Técnicas

1. Objetivo

O objetivo deste relatório é demonstrar de forma pragmática as informações levantadas na USCS (Universidade Municipal de São Caetano do Sul) sobre os ativos de rede atuais, assim como também a proposição de novos ativos através do site Survey preditivo realizado. Os levantamentos em campo, análise e diagnóstico dos equipamentos de rede (switches, pontos de acesso Wi-fi, controladoras e acessórios) atuais e simulações em software especializado, ao final deste relatório apresentaremos as informações necessárias para instalação de uma solução completa e robusta rede Wi-fi 5, 6 e 7 através das frequências 2.4GHZ, 5GHZ e 6GHZ para os ambientes da USCS.

2. Diagnóstico

O diagnóstico contém informações sobre o ambiente de rede atual (switches, pontos de acesso Wi-fi e controladoras) e também informações para a implantação de uma nova solução para rede wi-fi (switches, pontos de acesso Wi-fi, controladora e acessórios);

- Quantidade atual de pontos de acesso wi-fi, switches e controladoras;
- Quantidade correta de pontos de acesso wi-fi, switches, controladora e acessórios a serem instalados para cobertura total em todos os ambientes;
- Os obstáculos existentes no local;
- Canal a utilizar na rede;
- Instalação de forma correta dos AP.

3. O que é Site Survey?

Site Survey é uma pesquisa em um ambiente de rede sem fio, que busca verificar fatores que podem interferir no funcionamento da rede, o seu propósito é dar uma garantia de funcionamento para rede, o principal objetivo de um Site Survey assegurar que o número, localização e configuração dos pontos de rede forneçam as funcionalidades requeridas e propiciem um ótimo desempenho

4. Tipos de Site Survey

Um Site Survey pode ser feito de várias maneiras e com diferentes ferramentas sejam elas hardware e software;

a. Site Survey Preditivo

É o estudo onde é usado simulações em software para obter o número aproximado de Pontos de Acesso Wi-Fis que serão necessários. No preditivo é possível escolher o posicionamento e também a configuração de cada Pontos de Acesso Wi-Fi para o projeto. Nesse tipo é possível fazer o Site Survey de forma remota.

b. Site Survey AP-on-a-Stick

É um método que consiste em usar um Pontos de Acesso Wi-Fi instalado em suporte e posicionar nos locais onde possivelmente serão instalados. Neste método o analista realizará o Site Survey em cada um desses locais, capturando os dados de qualidade e o tamanho da célula desse Pontos de Acesso Wi-Fi.

c. Site Survey Passivo

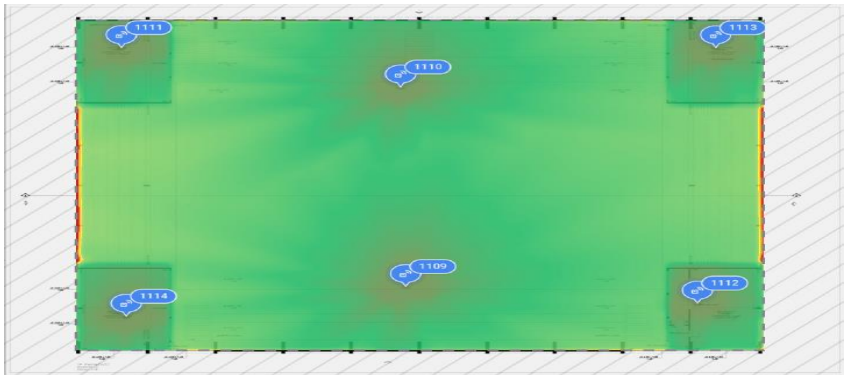
O método passivo é mais ágil e fornece todos os dados necessários para a análise da rede sem fio, nesta modalidade o analista fará o Walk Through pelo local e com o software de análise ele fará a coleta de todo o ambiente Wi-Fi.

d. Site Survey Ativo

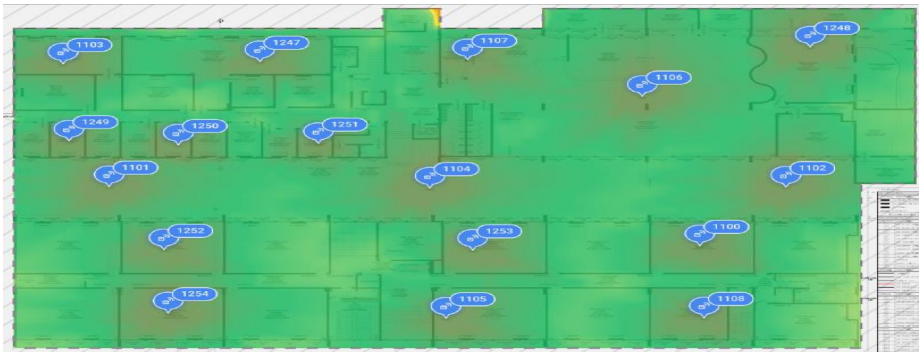
O método ativo é realizado em paralelo ao passivo, pois nessa modalidade o analista configura a rede Wi-Fi do cliente no software de análise, e dessa forma poderão ser feitas algumas medições de performance com o uso de ping e iPerf. O Site Survey Ativo é indicado após a implantação ou para atualização da rede Wi-Fi, assim é possível detectar alguns indicadores como, sinal ruído, SNR, perda de pacotes e roaming.

5 Solução Proposta (Site Survey)

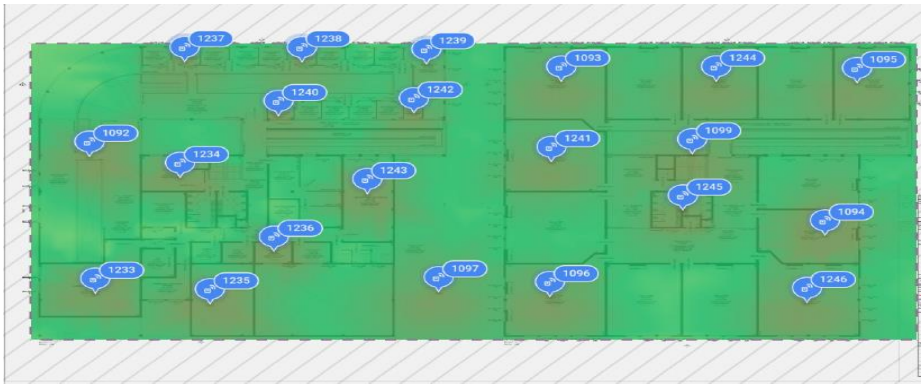
5.1. Planta baixa Campus - Barcelona - 1º Pavimento - Bloco C



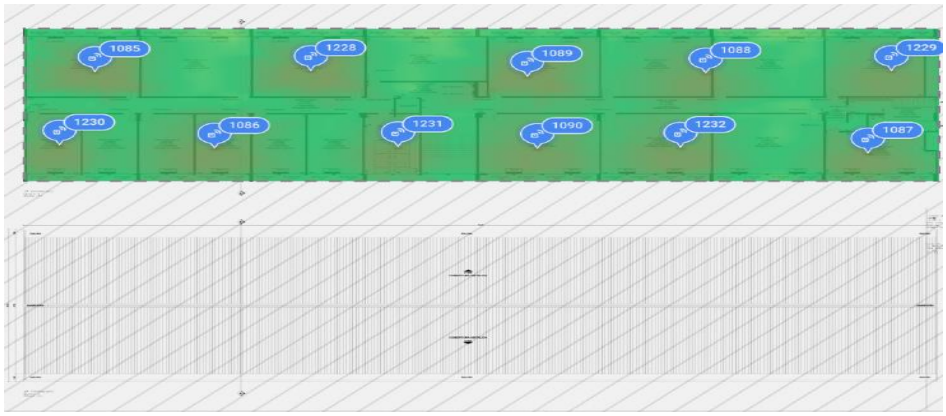
5.2. **Planta baixa Campus - Barcelona - 1º Pavimento e Subsolo - Bloco A**



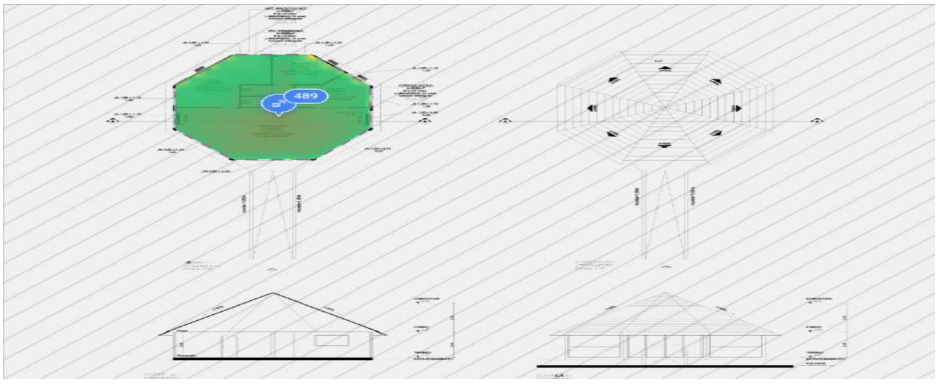
5.3. **Planta baixa Campus - Barcelona - 1º e 2º Pavimento - Bloco C**



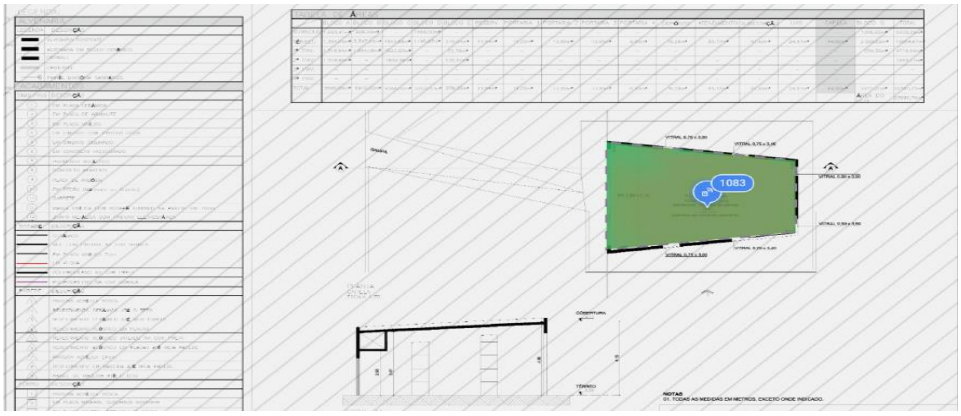
5.4. **Planta baixa Campus - Barcelona - 2º Pavimento e Cobertura - Bloco A**



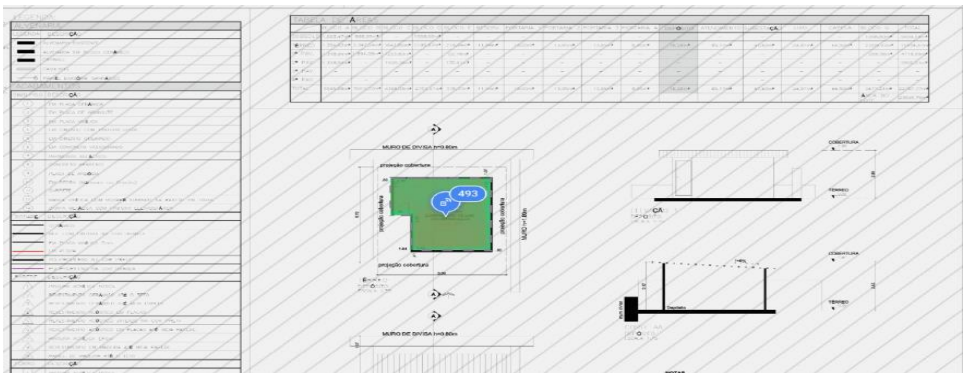
5.5. **Planta baixa Campus - Barcelona - Anexo Atendimento**



5.6. **Planta baixa Campus - Barcelona - Anexo Capela**

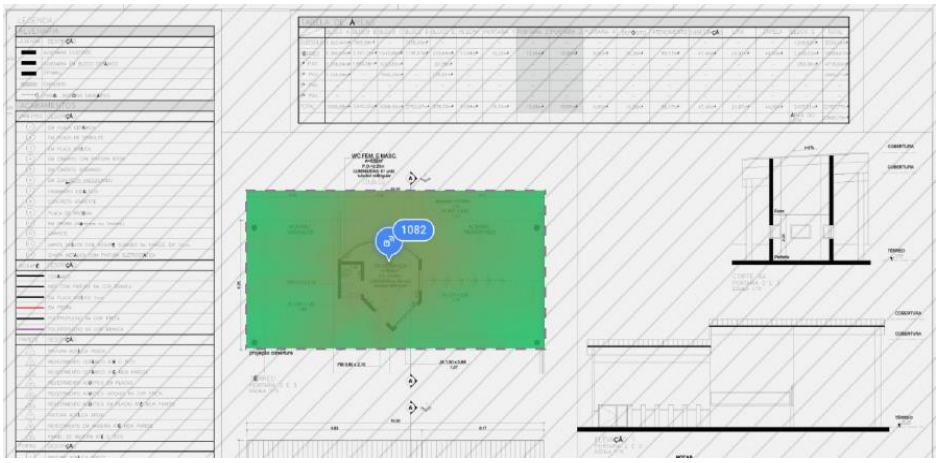


5.7. **Planta baixa Campus - Barcelona - Anexo Depósito**

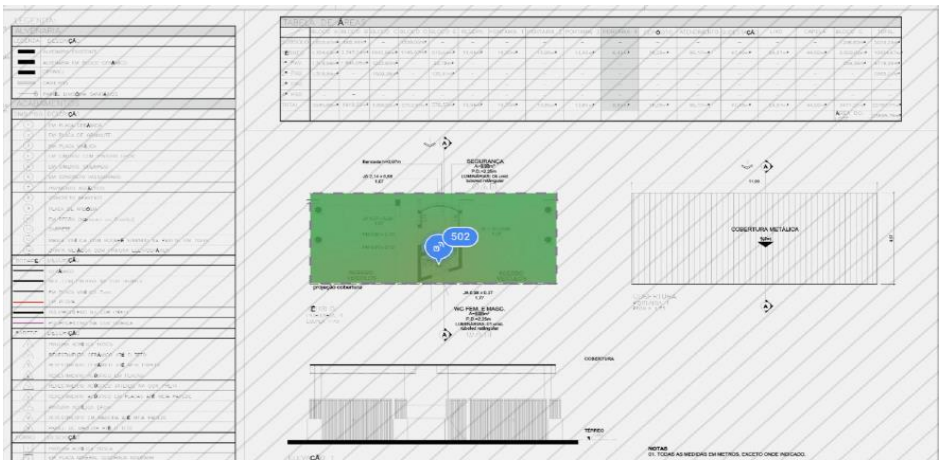


5.8. **Planta baixa Campus - Barcelona - Anexo Portaria 1**

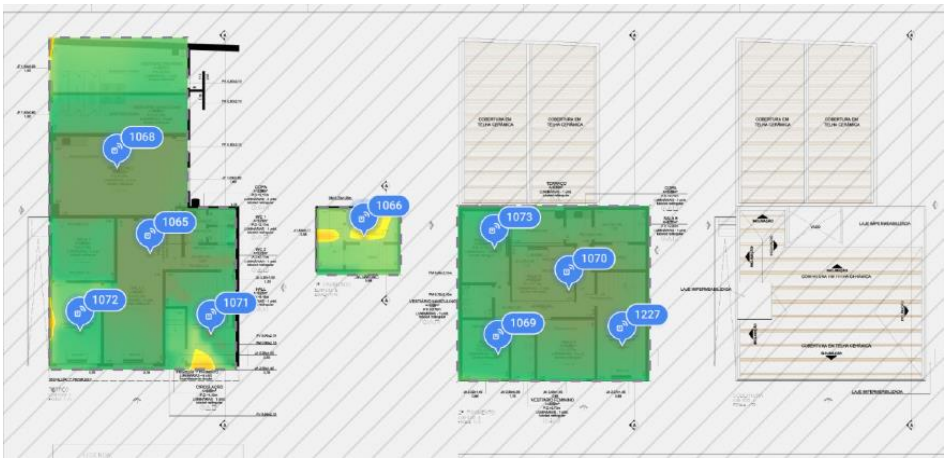
5.9. **Planta baixa Campus - Barcelona - Anexo Portaria 2 e 3**



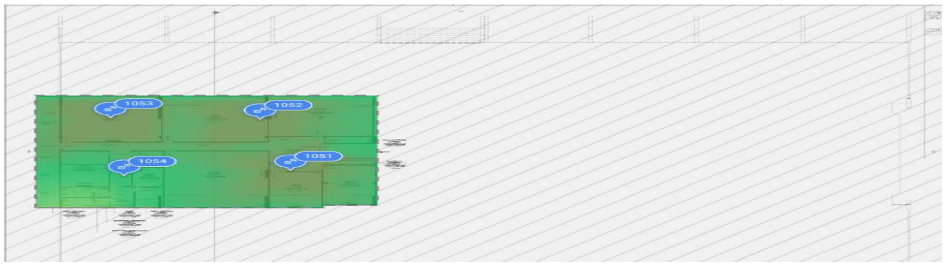
5.10. **Planta baixa Campus - Barcelona - Anexo Portaria 4**



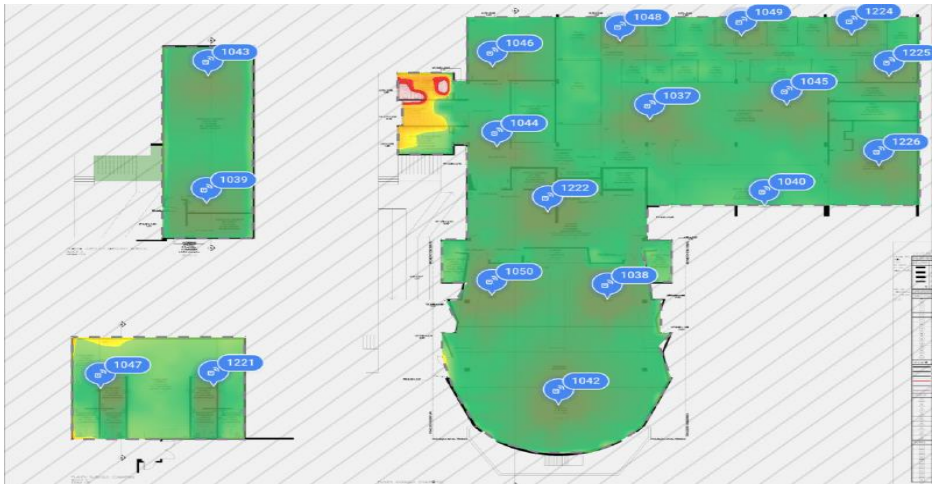
5.11. **Planta baixa Campus - Barcelona - Plantas - Bloco E**



5.12. **Planta baixa Campus - Barcelona - Subsolo - Bloco B**

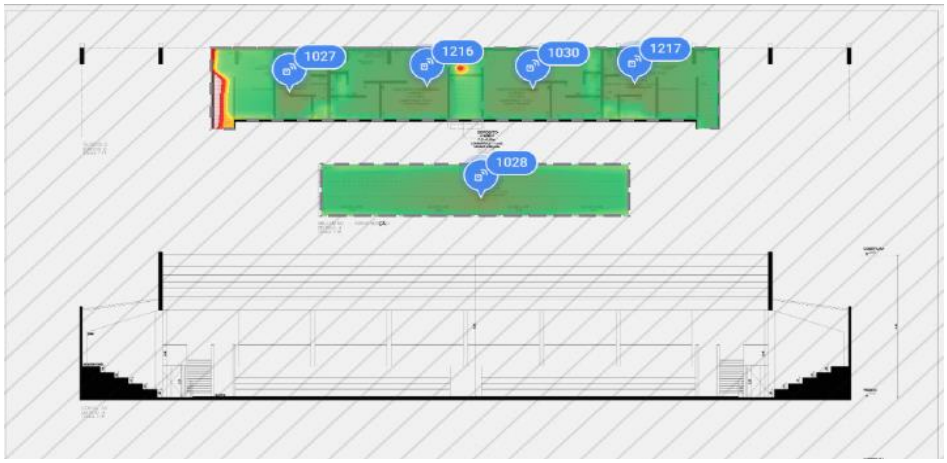


5.13. **Planta baixa Campus - Barcelona - Subsolo Auditório - Bloco D**

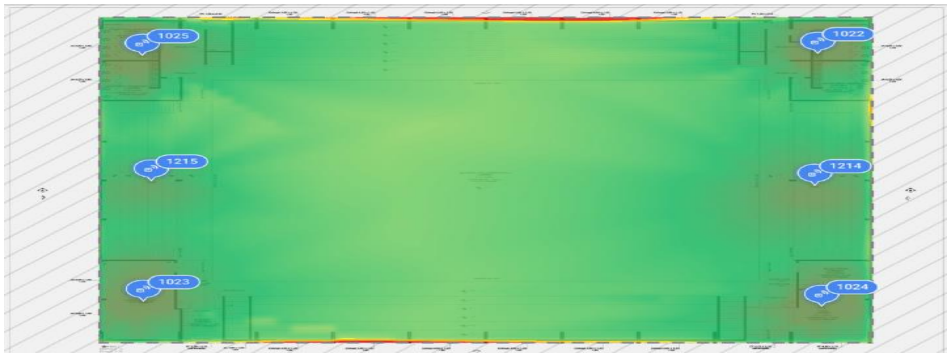


5.14. **Planta baixa Campus - Barcelona - Subsolo Manutenção - Bloco G**

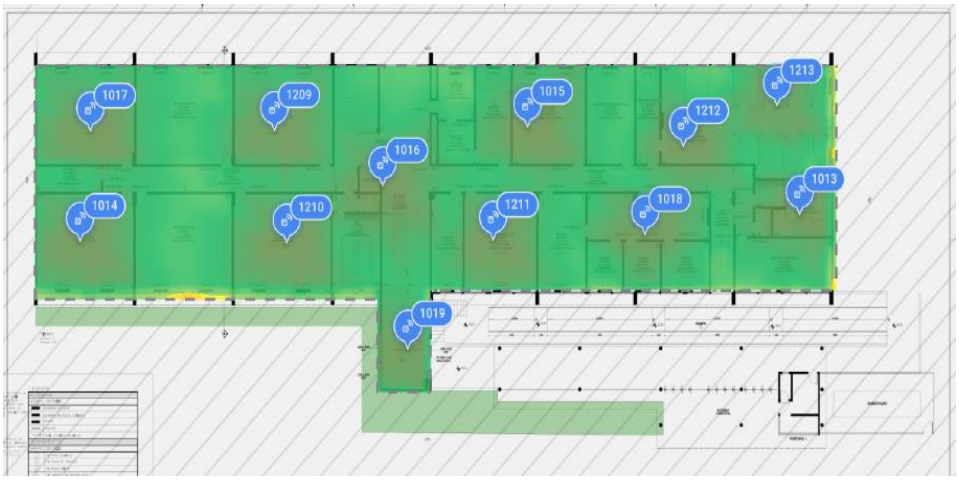
5.15. **Planta baixa Campus - Barcelona - Subsolo Quadra - Bloco G**



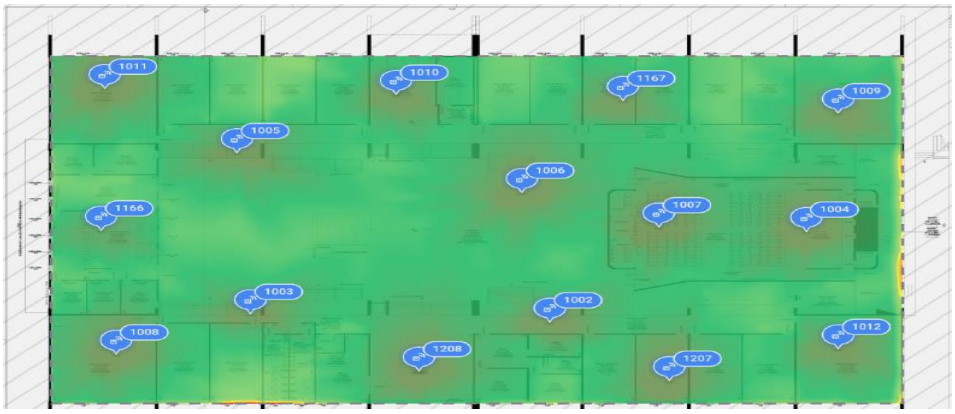
5.16. **Planta baixa Campus - Barcelona - Térreo (Quadra) - Bloco G**



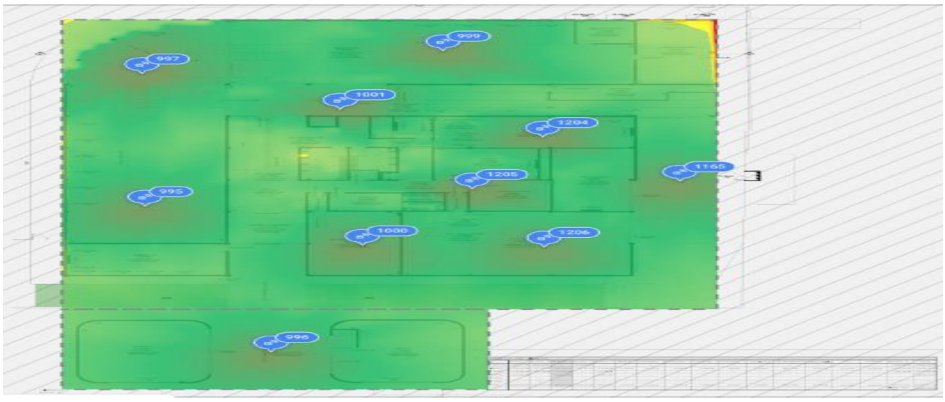
5.17. **Planta baixa Campus - Barcelona - Térreo - Bloco A**



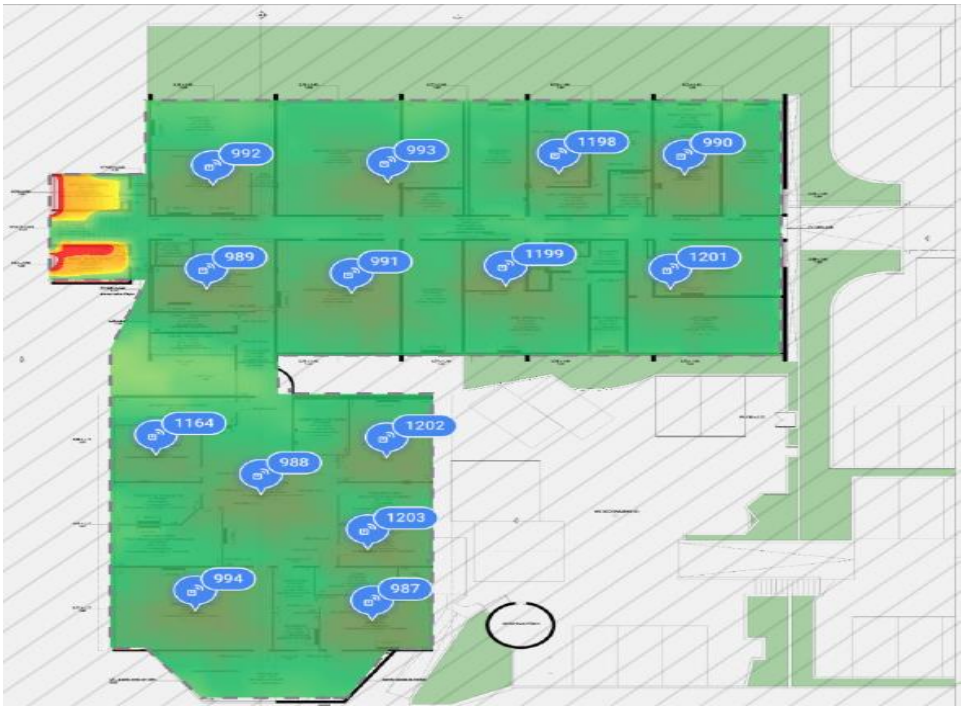
5.18. **Planta baixa Campus - Barcelona - Térreo - Bloco B**



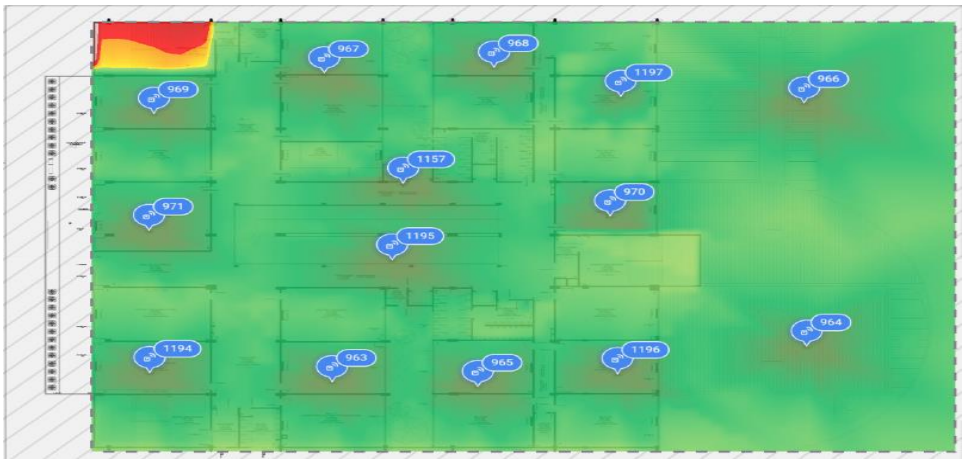
5.19. **Planta baixa Campus - Barcelona - Térreo - Bloco C**



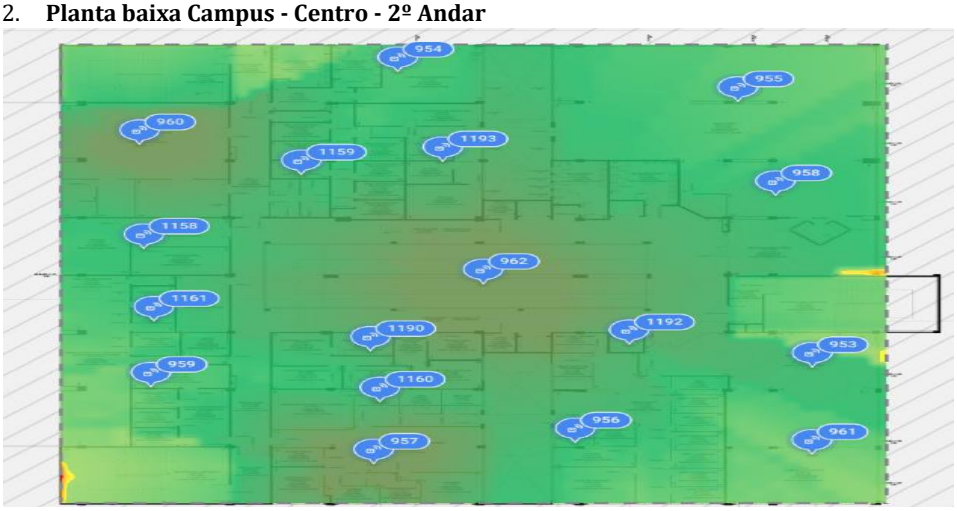
5.20. **Planta baixa Campus - Barcelona - Térreo - Bloco D**



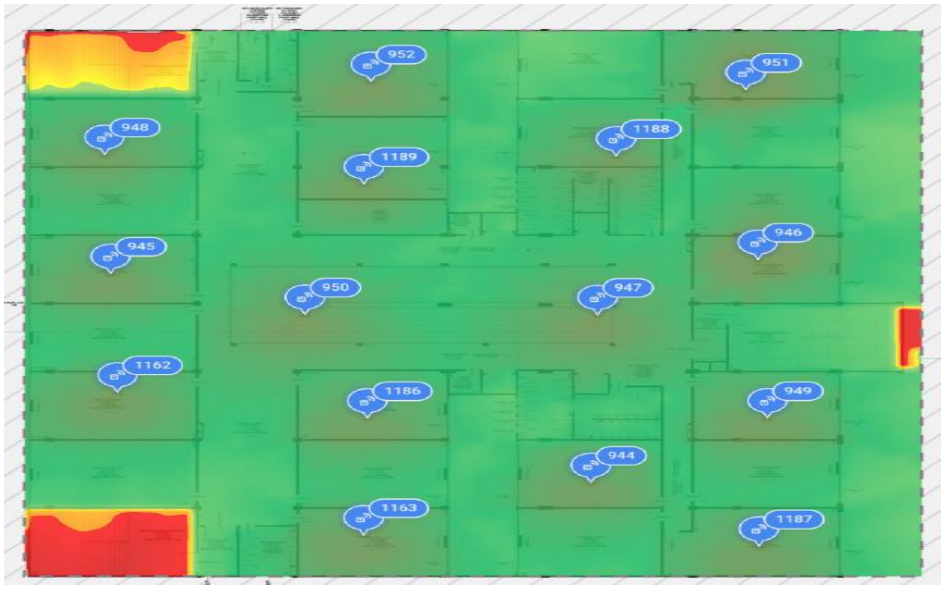
5.21. **Planta baixa Campus - Centro - 1º Andar**



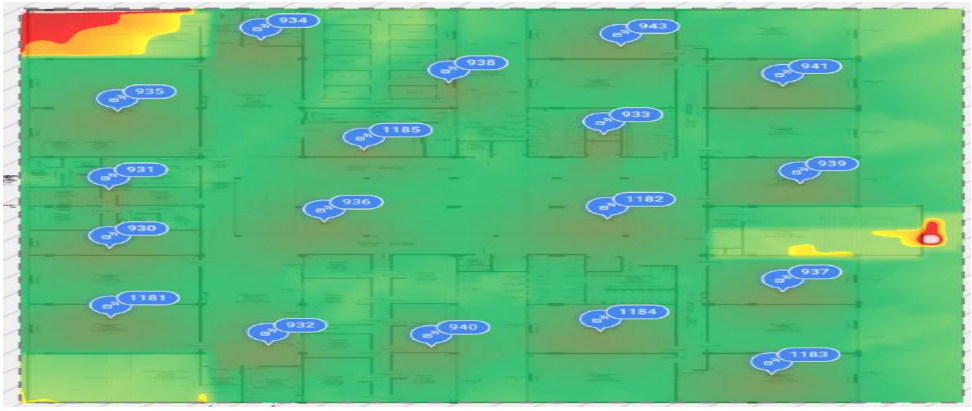
5.22. **Planta baixa Campus - Centro - 2º Andar**



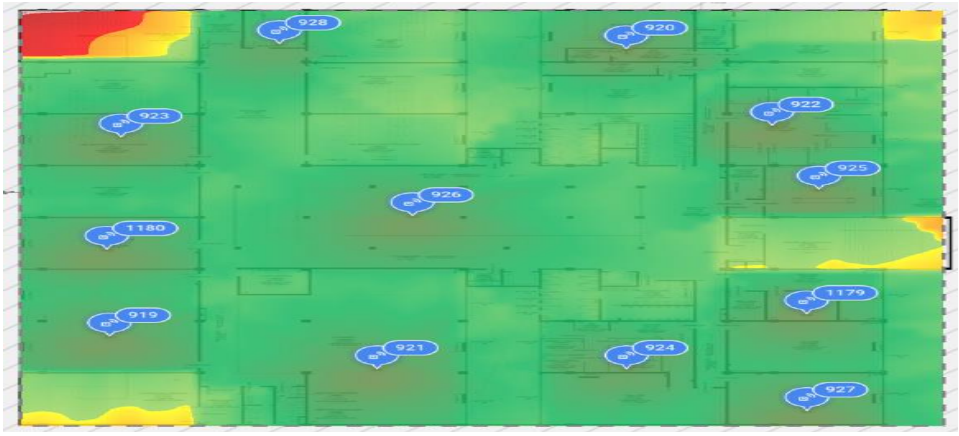
5.23. **Planta baixa Campus - Centro - 3º Andar**



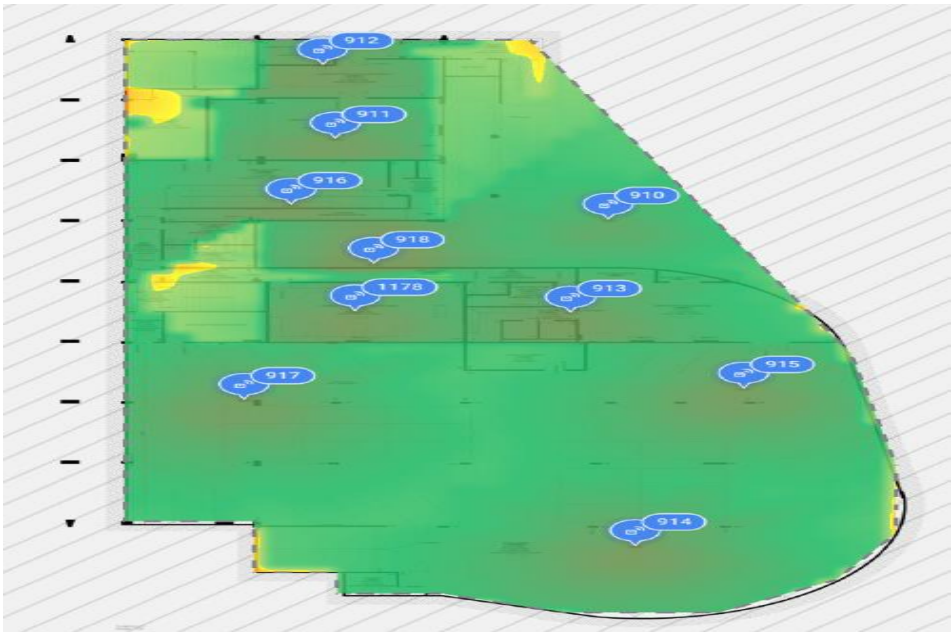
5.24. **Planta baixa Campus - Centro - 4º Andar**



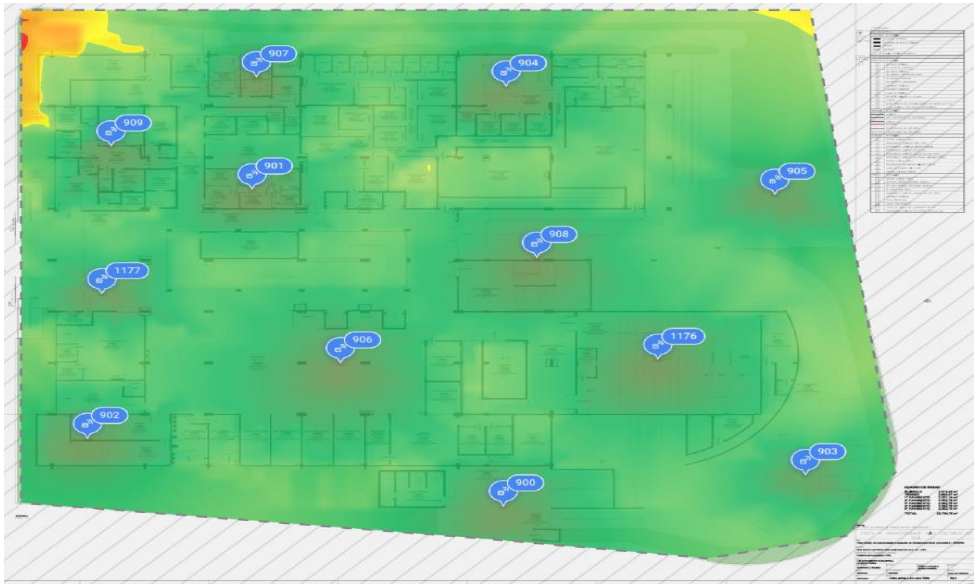
5.25. **Planta baixa Campus - Centro - 5º Andar**



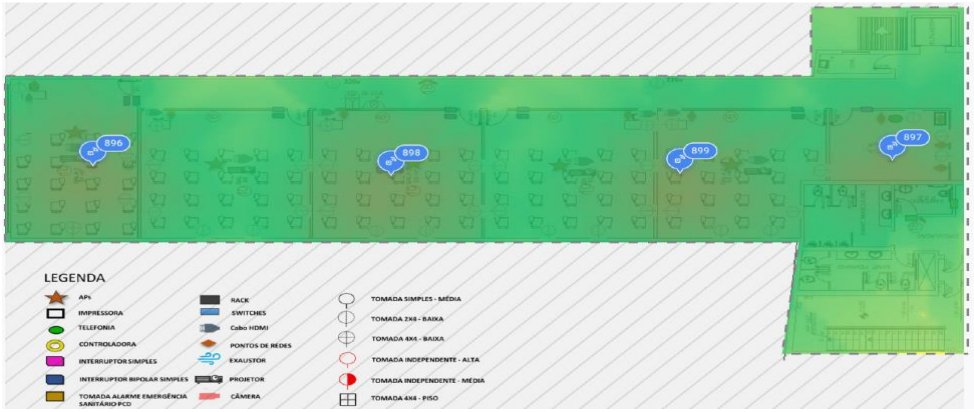
5.26. **Planta baixa Campus - Centro – Subsolo**



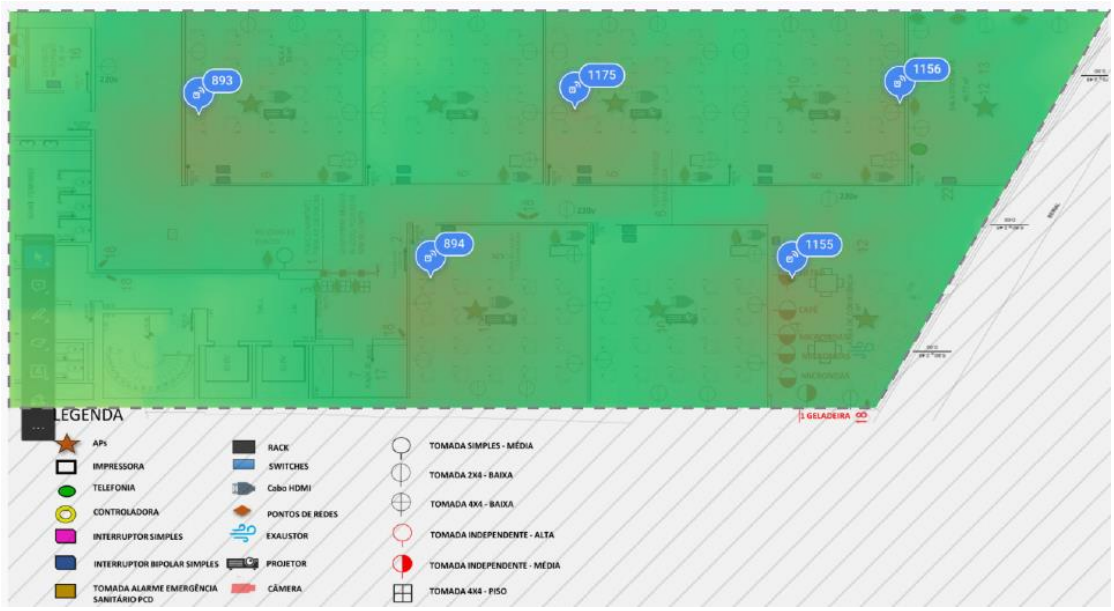
5.27. **Planta baixa Campus - Centro – Térreo**



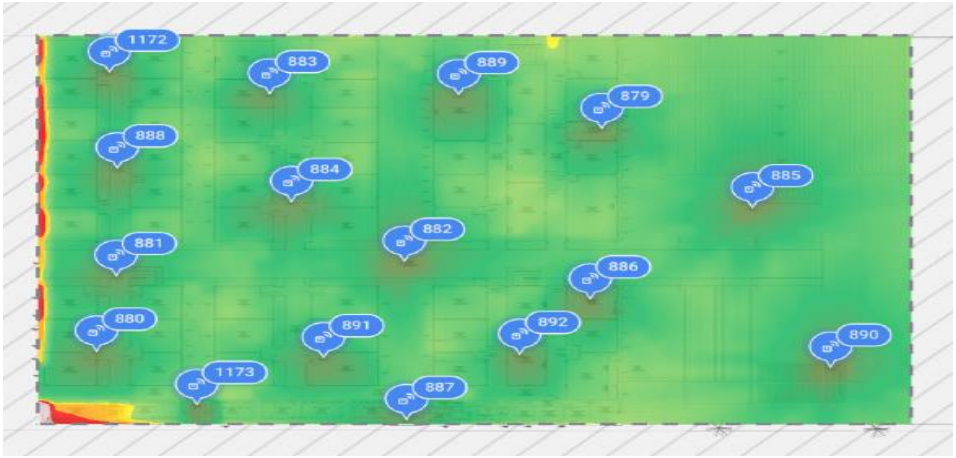
5.28. **Planta baixa Campus - Centro II – 1**



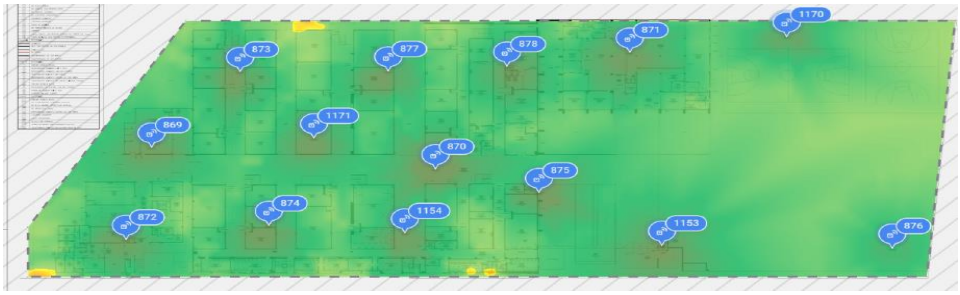
5.29. **Planta baixa Campus - Centro II – 2**



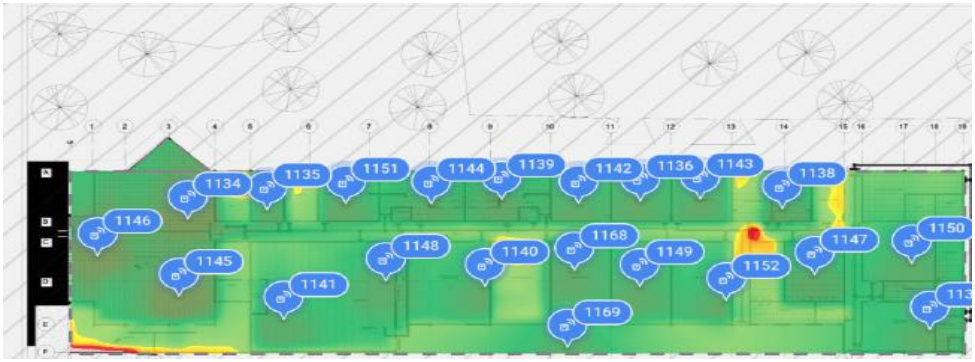
5.30. **Planta baixa Campus - Conceição - 1º Andar**



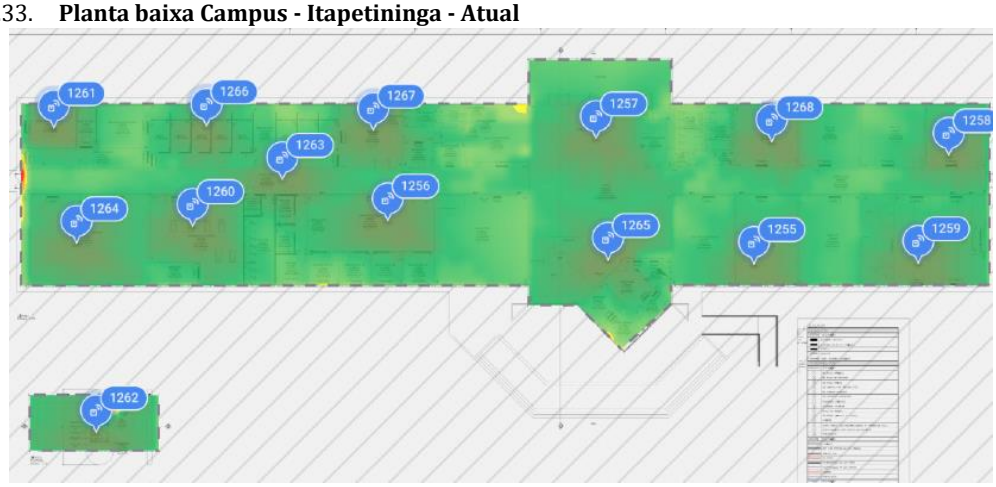
5.31. **Planta baixa Campus - Conceição - Térreo**



5.32. **Planta baixa Campus - Itapetininga**



5.33. **Planta baixa Campus - Itapetininga - Atual**



6. **Estimativa de Pon tos de Acesso Wi-Fi**

A estimativa para os pontos de acesso foi baseada na infraestrutura atual, bem como nas necessidades de instalação dos novos equipamentos, podendo haver alterações para melhor distribuição e qualidade do serviço:

Estimativa de Ponto de Acesso Wi-Fi's após Site Survey	
CAMPUS BARCELONA	***QTDE***
Campus - Barcelona - 1º Pavimento - Bloco C	6
Campus - Barcelona - 1º Pavimento e Subsolo Bloco A	10
Campus - Barcelona - 1ºe 2º Pavimento - Bloco C	8
Campus - Barcelona - 2º Pavimento e Cobertura - Bloco A	6
Campus - Barcelona - Anexo Atendimento	1
Campus - Barcelona - Anexo Capela	1
Campus - Barcelona - Anexo Deposito	1
Campus - Barcelona - Anexo Portaria 1	1
Campus - Barcelona - Anexo Portaria 2 e 3	1
Campus - Barcelona - Anexo Portaria 4	1
Campus - Barcelona - Plantas - Bloco E	6
Campus - Barcelona - Subsolo - Bloco B	3
Campus - Barcelona - Subsolo Auditório - Bloco D	9
Campus - Barcelona - Subsolo Manutenção - Bloco G	6
Campus - Barcelona - Subsolo Quadra - Bloco G	5
Campus - Barcelona - Térreo - Bloco A	7
Campus - Barcelona - Térreo - Bloco B	8
Campus - Barcelona - Térreo - Bloco C	6
Campus - Barcelona - Térreo - Bloco D	7
Campus - Barcelona - Térreo (Quadra) - Bloco G	5
Subtotal Campus Barcelona	**98**
CAMPUS CENTRO	***QTDE***
Campus - Centro - 1º Andar	8
Campus - Centro - 2º Andar	10
Campus - Centro - 3º Andar	12
Campus - Centro - 4º Andar	11
Campus - Centro - 5º Andar	10
Campus - Centro – Subsolo	7
Campus - Centro – Térreo	10
Campus - Centro II – 1	4
Campus - Centro II – 2	3
Subtotal Campus Centro	**75**
CAMPUS CONCEIÇÃO	***QTDE***
Campus - Conceição - 1º Andar	12
Campus - Conceição – Térreo	10
Total	**22**
CAMPUS ITAPETINGA	***QTDE***
Campus – Itapetininga	11
Campus - Itapetininga – Atual	13
Subtotal Campus Itapetininga	**24**
TOTAL	**219**

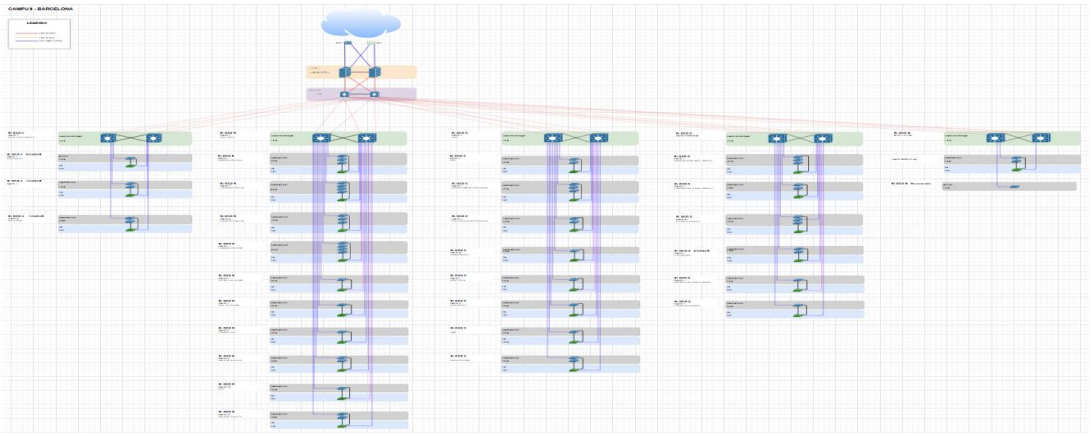
7. **Estimativa de Switches**

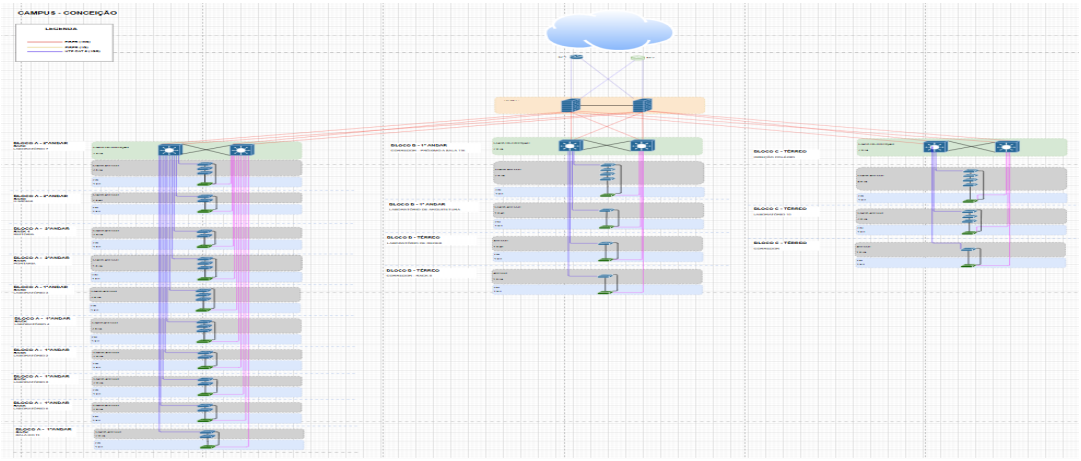
A estimativa para a conectividade de switches foi baseada na infraestrutura atual, bem como nas necessidades de instalação dos novos equipamentos, podendo haver alterações para melhor distribuição e qualidade do serviço:

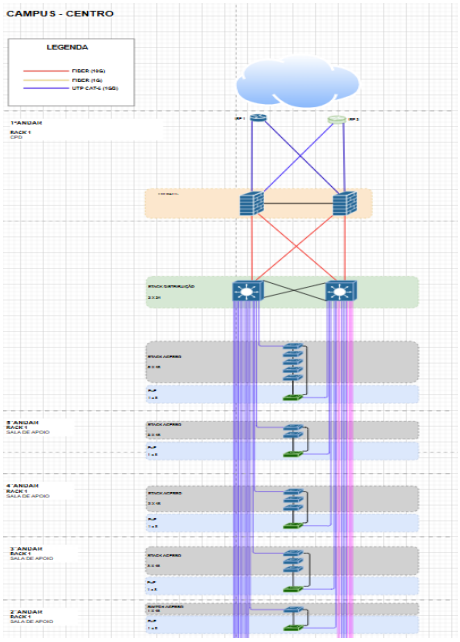
Quantidade de Switches por porta	
Switches	**Quantidades**
Switch Tipo 1 (8x portas)	28
Switch Tipo 2 (24 portas)	2
Switch Tipo 3 (48 portas)	2
Total de Switches	32

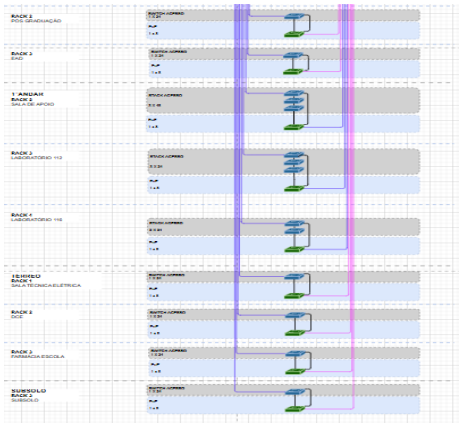
8. **Situação para nova solução de rede**

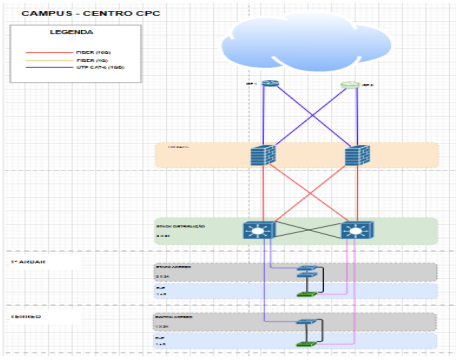
8.1. **Topologias e Interconexão Switches**

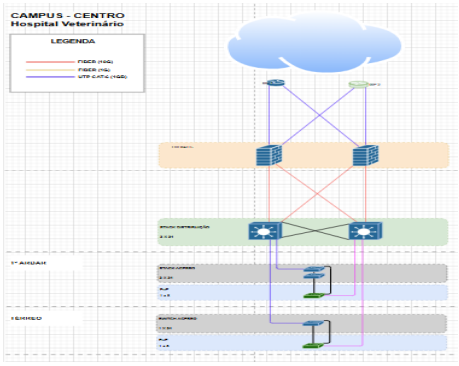


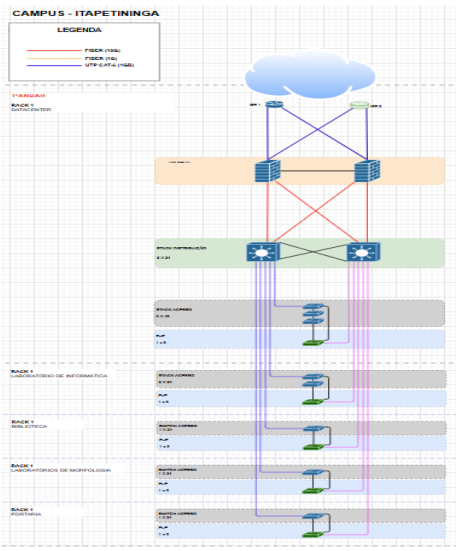


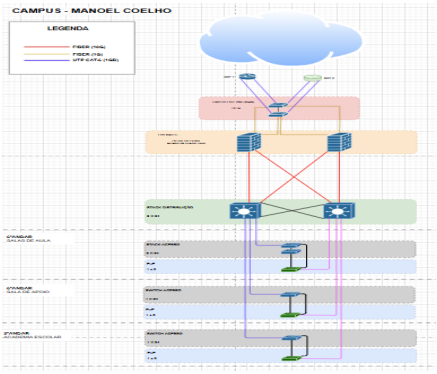












9. Considerações Finais

Com base nos resultados obtidos, o objeto do trabalho foi atingido com sucesso. Como visto, foi possível verificar os locais escolhidos condizentes com aplicação das informações de topologias, plantas baixas e infraestrutura atual.
Embora o projeto tenha sido bem-sucedido, podem ocorrer melhorias para aumentar a precisão e praticidade nas execuções de medição.
Portanto, mesmo que algumas melhorias tornem o módulo desenvolvido mais eficiente e/ou prático para executar sua função, o sistema desenvolvido atende todos os objetivos propostos no escopo do trabalho, sendo assim uma ferramenta muito útil para a execução de site Survey de uma rede e a estimativa necessária para construção de um projeto de troca e modernização de conectividade da Universidade Municipal de São Caetano do Sul.

_____
Alessandro Parada
Diretor de Tecnologia da Informação e Inovação

ANEXO XIX
PLANO DE GESTÃO DE RISCO
MODERNIZAÇÃO DA INFRAESTRUTURA TECNOLÓGICA DE REDE WiFi

1. INTRODUÇÃO

A gestão de riscos é essencial para aumentar a capacidade da USCS de lidar com incertezas, estimular a transparência, contribuir para o uso eficiente de recursos públicos e melhorar a entrega de serviços de rede e conectividade à comunidade acadêmica.

Este documento visa orientar as atividades relacionadas ao projeto de contratação de Serviço Gerenciado de solução para gestão de ativos de rede, monitoramento e segurança, incluindo fornecimento de softwares, equipamentos (switches, pontos de acesso Wi-Fi, controladoras), licenciamentos, suporte técnico especializado, acessórios, garantia e monitoramento, conforme descrito no Projeto Básico da Universidade de São Caetano do Sul, de forma a prever eventos que possam comprometer os objetivos do projeto e a adequada execução contratual durante sua vigência.

O Plano está alinhado às diretrizes da Lei nº 14.133/2021, especialmente no que se refere à necessidade de gestão de riscos nas fases de Planejamento da contratação e Gestão do contrato.

1.1. Objetivo

O plano tem como objetivo orientar a gestão de riscos desde o início do projeto até a sua conclusão, fornecendo uma abordagem para identificar, analisar, avaliar, tratar, monitorar e comunicar os riscos associados ao projeto de reestruturação da rede WiFi.

1.2. Escopo e Abrangência

Este plano abrange todas as fases do projeto, incluindo;
- A aquisição, entrega, instalação, configuração, testes e aceitação dos equipamentos de rede (Switches, APs Wi-Fi, Controladora e demais acessórios);
- A implantação da solução de monitoramento e gestão de ativos de rede;
- A configuração de políticas de segurança, autenticação e controle de acesso, conforme Projeto Básico;
- Os serviços gerenciados de monitoramento, suporte técnico especializado, operação assistida, manutenções preventivas e corretivas e atendimento aos NMS (Níveis Mínimos de Serviço);
- A migração da infraestrutura atual para a nova, com mitigação de riscos de indisponibilidade;
- A gestão do contrato durante toda a vigência, considerando renovações, aditivos e encerramento contratual.

1.3. Termos, Definições, Acrônimos e Abreviações

- Risco: Efeito da incerteza nos objetivos do projeto.
- Controle: Medida que mantém e/ou modifica o risco.
- TI: Tecnologia da Informação.
- Vulnerabilidade: Fraqueza que pode ser explorada por uma ameaça.
- Stakeholder: Parte interessada no projeto.
- NMS: Níveis Mínimos de Serviço, conforme definido no Projeto Básico e na futura minuta contratual.

2. RISCOS DO PROJETO

2.1. Identificação dos Riscos

2.1.1. Os principais riscos identificados para o projeto são:

(a) Atraso na entrega dos equipamentos:

- Causa: Problemas logísticos ou atrasos dos fornecedores.
- Consequência: Atraso no cronograma de implantação, extensão do período de convivência com a infraestrutura legada e possível impacto na disponibilidade e qualidade do serviço para até 10.000 acessos simultâneos previstos.
- Controle: Estabelecimento de prazos claros e acompanhamento contínuo com os fornecedores.

(b) Incompatibilidade dos novos equipamentos com a infraestrutura existente e com a demanda de uso:

- Causa: Especificações técnicas inadequadas, erros de dimensionamento, falha em considerar cenários de pico de uso ou peculiaridades da topologia da USCS.
- Consequência: Gargalos de desempenho, queda de qualidade da experiência dos usuários, necessidade de reconfigurações e possíveis custos adicionais.
- Controle: Validação rigorosa das especificações, testes de compatibilidade antes da implementação em ambiente controlado e aceitação somente mediante atendimento integral aos requisitos do Projeto Básico.

(c) Falhas na instalação e configuração:

- Causa: Erros técnicos ou falta de capacitação da equipe.
- Consequência: Indisponibilidade de rede WiFi, retrabalho e alongamento do cronograma.
- Controle: Exigência de equipe qualificada, plano de implantação e migração aprovado, e acompanhamento rigoroso das atividades de instalação.

(d) Interrupções de energia durante a implementação:

- Causa: Falhas na infraestrutura elétrica, ausência de redundância adequada de energia ou incidentes na concessionária.
- Consequência: Atrasos nas atividades de implantação, risco de danos nos equipamentos e indisponibilidade temporária da rede WiFi.
- Controle: Uso de geradores e sistemas de energia redundantes.

(e) Descumprimento dos NMS (Níveis Mínimos de Serviço) e dos tempos de resposta/solução de chamados:

- Causa: Dimensionamento inadequado da equipe de suporte, ausência de monitoramento contínuo, processos internos ineficientes do fornecedor.
- Consequência: Indisponibilidade recorrente, degradação da qualidade do serviço, aumento da insatisfação dos usuários e risco reputacional para a USCS.
- Controle: Definição clara de NMS e SLAs em contrato, relatórios periódicos de desempenho, reuniões de acompanhamento e aplicação de sanções contratuais quando cabível.

2.2. Tabela de Riscos Identificados e Classificados

Risco	Probabilidade	Impacto	Probabilidade Numérica	Impacto Numérico
Atraso na entrega dos equipamentos	Alta	Alto	3	3
Incompatibilidade dos novos equipamentos com a infraestrutura existente	Média	Muito Alto	2	4
Falhas na instalação, configuração, migração e operação assistida	Alta	Alto	3	3
Interrupções de energia durante a implementação	Média	Médio	2	2
Descumprimento dos NMS e SLAs de suporte	Média	Alto	2	3

Essa análise ajuda a identificar quais riscos possuem maior prioridade de tratamento, com base na combinação da sua probabilidade de ocorrência e impacto sobre o projeto. Riscos com alta probabilidade e alto impacto, como "Atraso na entrega dos equipamentos" e "Falhas na instalação e configuração", devem ser tratados com maior urgência e atenção.

2.3. Análise de Riscos

Cada risco identificado será analisado quanto à probabilidade de ocorrência e impacto. Utilizaremos uma matriz de probabilidade e impacto para essa análise:

- Probabilidade: Baixa, Média, Alta, Muito Alta.
- Impacto: Baixo, Médio, Alto, Muito Alto.

A matriz abaixo visualiza a distribuição dos riscos com base em sua probabilidade de ocorrência e impacto.

Os parâmetros que serão utilizados como base para construção dos níveis de risco estão dispostos na tabela que segue. Para este caso foram adotados 4 valores básicos:

Impacto \ Probabilidade	Baixa	Média	Alta	Muito Alta
Muito Alto	0	2	0	0
Alto	0	1	2	0
Médio	0	2	0	0
Baixo	0	0	0	0

A figura a seguir apresenta a Matriz Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco.

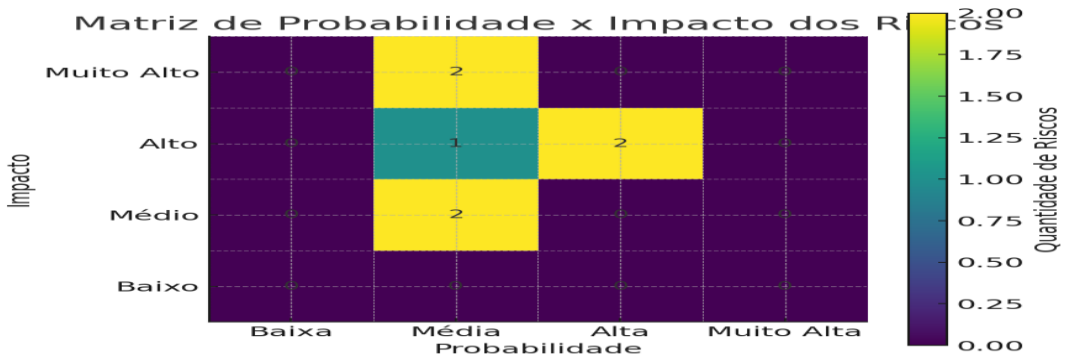


Figura 1: Matriz de Probabilidade x Impacto

2.4. Avaliação de Riscos

Os riscos serão avaliados para determinar a necessidade de ações adicionais. Riscos de alta probabilidade e alto impacto terão prioridade no tratamento.

Riscos de alta probabilidade e alto ou muito alto impacto (por exemplo, atraso na entrega, falhas de instalação/migração e incompatibilidade/desempenho) terão prioridade máxima de tratamento.

Riscos de probabilidade média e impacto muito alto (incidentes de segurança, incompatibilidade grave, descumprimento crítico de NMS) terão tratamento prioritário, com foco em controles preventivos.

Riscos de probabilidade média e impacto médio (falhas no monitoramento, interrupções pontuais de energia) serão acompanhados e terão planos de mitigação proporcionais ao seu impacto.

2.5. Tratamento de Riscos

Para cada risco, serão definidas estratégias de tratamento:
- Mitigar: Ações de prevenção e redução da probabilidade e/ou impacto (treinamento, melhoria de processos, redundâncias, validações técnicas).
- Transferir: Transferir total ou parcialmente o risco a terceiros (seguro, cláusulas contratuais, garantias).
- Aceitar: Aceitar o risco quando o custo de mitigação for desproporcional ao benefício ou quando o risco residual for considerado tolerável.
- Evitar: Modificar planos para eliminar o risco por completo.

A tabela resume a abordagem de tratamento proposta para cada risco, garantindo que ações adequadas sejam tomadas para minimizar os impactos negativos no projeto

Risco	Probabilidade	Impacto	Avaliação	Tratamento Proposto
Atraso na entrega dos equipamentos e início dos serviços	Alta	Alto	Alta probabilidade e alto impacto	**Mitigar**: prazos claros, cláusulas de penalidade, acompanhamento próximo e marcos contratuais.
Incompatibilidade dos novos equipamentos com a infraestrutura existente	Média	Muito Alto	Média probabilidade, impacto muito alto	**Mitigar**: testes de compatibilidade, pilotos, validação rigorosa das especificações e cenários de pico.
Falhas na instalação, configuração, migração e operação assistida	Alta	Alto	Alta probabilidade e alto impacto	**Mitigar**: plano de migração aprovado, janelas de mudança, RDM, equipe certificada e supervisão da DTI.
Interrupções de energia	Média	Médio	Probabilidade e impacto médios	**Mitigar/Aceitar**: uso de nobreaks, planejamento, coordenação com infraestrutura; aceitação parcial do risco residual.
Descumprimento dos NMS e SLAs	Média	Alto	Probabilidade média, impacto alto	**Mitigar/Transferir**: definição contratual de NMS e SLAs, monitoramento e penalidades contratuais.

3. METODOLOGIA

A metodologia empregada no Plano de Gestão de Riscos para o projeto de reestruturação da infraestrutura de redes da Universidade segue as diretrizes da ISO 31000 (Gestão de Riscos) e utiliza ferramentas específicas para assegurar uma gestão eficiente e eficaz dos riscos.

3.1. Diretrizes

3.1.1. Sistematicidade e Transparência:

- Objetivo: Garantir que o processo de gestão de riscos seja sistemático e transparente.
- Aplicabilidade: Utilizar procedimentos padronizados para identificar, analisar, avaliar e tratar riscos.

3.1.2. Integração com os Processos Organizacionais:

- Objetivo: Integrar a gestão de riscos aos processos de planejamento e execução do projeto.
- Aplicabilidade: Alinhar a gestão de riscos aos objetivos estratégicos do projeto, conforme descrito no memorial descritivo.

3.1.3. Baseada em Melhores Práticas:

- Objetivo: Adotar práticas reconhecidas internacionalmente para a gestão de riscos.
- Aplicabilidade: Utilizar as normas ISO 31000 e ISO 31010 como referência.

3.1.4. Proporcionalidade:

- Objetivo: Ajustar o nível de gestão de riscos à complexidade e criticidade do projeto.
- Aplicabilidade: Implementar medidas de gestão de riscos de acordo com o impacto e a probabilidade dos riscos identificados.

3.2. Ferramentas e Aplicabilidade

3.2.1. Brainstorming

- Descrição: Técnica para gerar uma lista de riscos através da participação de diferentes stakeholders.

- Aplicabilidade: Utilizada na fase inicial do projeto para identificar possíveis riscos com a participação de especialistas e membros da equipe do projeto.

3.2.2. Checklists

- Descrição: Listas pré-definidas de riscos comuns para assegurar que todos os riscos relevantes sejam considerados.

- Aplicabilidade: Utilizada para garantir a identificação de riscos que possam ser esquecidos ou negligenciados durante o brainstorming.

3.2.3. Entrevistas Estruturadas e Semiestruturadas

- Descrição: Coleta de informações sobre riscos através de entrevistas com stakeholders chave.

- Aplicabilidade: Utilizadas para obter insights detalhados sobre riscos específicos e suas possíveis causas e consequências.

3.2.4. Questionários

- Descrição: Ferramenta de coleta de dados padronizada para identificar e avaliar riscos.

- Aplicabilidade: Distribuídos aos membros da equipe e stakeholders para coletar informações sobre a percepção de riscos.

3.2.5. Análise SWOT

- Descrição: Identificação de forças, fraquezas, oportunidades e ameaças relacionadas ao projeto.

- Aplicabilidade: Utilizada para fornecer uma visão abrangente dos fatores internos e externos que podem impactar o projeto.

3.2.6. Matriz de Probabilidade e Impacto

- Descrição: Ferramenta para avaliar e priorizar riscos com base em sua probabilidade de ocorrência e impacto.

- Aplicabilidade: Utilizada na fase de avaliação de riscos para determinar quais riscos necessitam de tratamento prioritário.

3.2.7. Técnica 5W2H

- Descrição: Ferramenta de planejamento que define "o quê", "por quê", "quem", "onde", "quando", "como" e "quanto" para cada risco.
- Aplicabilidade: Utilizada na fase de tratamento de riscos para detalhar as ações necessárias para mitigar os riscos.

3.3. Aplicabilidade das Ferramentas no Escopo do Projeto

3.3.1. Identificação de Riscos:

- Brainstorming, Checklists, Entrevistas Estruturadas e Semiestruturadas: Aplicadas para identificar riscos relacionados à aquisição, instalação, configuração e operação dos novos equipamentos de rede.

3.3.2. Análise de Riscos:

- Matriz de Probabilidade e Impacto: Avaliação quantitativa e qualitativa dos riscos identificados, considerando a probabilidade de ocorrência e o impacto no projeto.

3.3.3. Avaliação de Riscos:

- Matriz de Probabilidade e Impacto: Priorização dos riscos para determinar quais requerem ações imediatas.

3.3.4. Tratamento de Riscos:

- Técnica 5W2H: Detalhamento das ações de mitigação, responsáveis, prazos e recursos necessários para tratar cada risco identificado.

3.3.5. Monitoramento e Controle:

- Relatórios de Acompanhamento de Risco: Acompanhamento contínuo e revisão periódica dos riscos e das ações de mitigação.

4. PROCESSO DE GESTÃO DE RISCOS

4.1. Estabelecimento do Contexto

Considerar o ambiente interno e externo, objetivos estratégicos do projeto, stakeholders envolvidos e fatores que possam afetar os resultados.

4.2. Monitoramento e Análise crítica

O acompanhamento contínuo dos riscos será realizado, com revisões semestrais ou conforme necessário. Serão realizadas reuniões de status para avaliação dos riscos e eficácia das medidas implementadas.

4.3. Comunicação e Consulta

As informações sobre riscos serão comunicadas às partes interessadas por meio de relatórios periódicos e reuniões de acompanhamento.

5. CRONOGRAMA

As atividades de gestão de riscos seguirão o cronograma do projeto, com revisões e atualizações periódicas conforme necessário.

6. APROVAÇÃO E ASSINATURA

O Plano de Gerenciamento de Riscos deverá ser assinado pela Equipe de Planejamento da Contratação, nas fases de Planejamento da Contratação e de Seleção de Fornecedores, e pela Equipe de Fiscalização do Contrato, na fase de Gestão do Contrato.

_____

Alessandro Parada

Diretor de Tecnologia da Informação e Inovação