Fls. nº

EDITAL 032/2025

PROCESSO Nº 056/2025
PREGÃO ELETRÔNICO Nº 031/2025

Torna-se público, para conhecimento dos interessados, que o **Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul**, inscrito no CNPJ sob o nº 17.813.026/0001-51, com sede na Rua Coronel Vidal, nº 800, São Dimas, Juiz de Fora - MG, por meio de sua equipe de Pregão, realizará licitação, na modalidade **PREGÃO**, na forma **ELETRÔNICA**, nos termos da **Lei nº 14.133 de 2021**, da Resolução CISDESTE nº08/2023 e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

DA SESSÃO PÚBLICA DO PREGÃO ELETRÔNICO:

Data e horário da sessão: 09/01/2026 às 09:10 horas.

Data e horário final para envio de Proposta: 09/01/2026 às 09:00 horas.

MODO DE DISPUTA: Aberto.

Critério de Julgamento: MENOR PREÇO **-** GLOBAL realizada em único item.

1. DO OBJETO

1.1. O objeto da presente licitação é a Contratação de empresa especializada na prestação de SERVIÇOS TÉCNICOS na área de TECNOLOGIA DA INFORMAÇÃO E TELECOMUNICAÇÕES, para atender as necessidades do CISDESTE, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

2. DA PARTICIPAÇÃO NO PREGÃO

2.1. Os interessados em participar deste Pregão deverão credenciar-se, previamente, perante o sistema eletrônico provido pela **BLL Compras**, por meio do sítio **https://bll.org.br/**, onde poderão obter maiores informações, podendo sanar eventuais dúvidas pela central de atendimentos do Portal.

2.1.1. Para ter acesso ao sistema eletrônico, os interessados deverão dispor de chave de identificação e senha pessoal, obtidas junto ao provedor do sistema eletrônico, onde também deverão se informar a respeito do seu funcionamento e regulamento, obtendo instruções detalhadas para sua correta utilização.

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 Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

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

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

2.3. Poderão participar dessa licitação qualquer empresa que atendam as condições do edital (Competição ampla).

2.4. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133, de 2021, para o agricultor familiar, o produtor rural pessoa física e para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006.

2.5. Não poderão disputar esta licitação:

2.5.1. aquele que não atenda às condições deste Edital e seus anexos;

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

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

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

2.5.5. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles

seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

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

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

2.5.8. agente público do órgão ou entidade licitante;

2.5.9. pessoas jurídicas reunidas em consórcio*[1]*;

---

[1] NOTA EXPLICATIVA: Considerando que é ato discricionário da Administração diante da avaliação de conveniência e oportunidade no caso concreto; e considerando que existem no mercado diversas empresas com potencial para atender satisfatoriamente às exigências previstas neste edital, entende-se que é conveniente a vedação de participação de empresas em "consórcio" no Pregão em tela.

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

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

2.6. O impedimento de que trata o item 2.5.4 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.

2.7. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 2.5.2 e 2.5.3 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

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

2.9. O disposto nos itens 2.5.2 e 2.5.3 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

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

2.11. A vedação de que trata o item 2.5.8 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

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

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

3.3. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço, observado o disposto nos itens 7.1.1 e 7.12.1 deste Edital.

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

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

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

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

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

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

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

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

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

3.7. A falsidade da declaração de que trata os itens 3.4 ou 3.6 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

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

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

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

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

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

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

3.12. O valor final mínimo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

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

3.13. O valor final mínimo na forma do item 3.11 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

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

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

4. DO PREENCHIMENTO DA PROPOSTA

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

4.1.1. valor, conforme definido neste edital e na plataforma de realização do pregão;

4.1.2. Marca, se for o caso;

4.1.3. Fabricante, se for o caso;

4.1.4. Descrição do objeto, contendo as informações similares à especificação do Termo de Referência;

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

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

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

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

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

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

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

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

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

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

5.2.1. Será desclassificada a proposta que identifique o licitante.

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

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

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

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

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

5.6. O lance deverá ser ofertado conforme critério de julgamento definido no preâmbulo desse edital.

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

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

5.9. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R$ 10,00 (dez reais)

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

5.11. O PROCEDIMENTO SEGUIRÁ DE ACORDO COM O MODO DE DISPUTA ADOTADO NESTE EDITAL.

5.12. Caso seja adotado para o envio de lances no pregão eletrônico o **modo de disputa "ABERTO"**, os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

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

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

5.12.3. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

5.12.4. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

5.12.5. Após o reinício previsto no item supra, os licitantes serão convocados para apresentar lances intermediários.

5.13. Caso seja adotado para o envio de lances no pregão eletrônico o **modo de disputa "ABERTO E FECHADO"**, os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

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

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

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

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

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

5.14. Caso seja adotado para o envio de lances no pregão eletrônico o **modo de disputa "FECHADO E ABERTO"**, poderão participar da etapa aberta somente os licitantes que apresentarem a proposta de menor preço e os das propostas até 10% (dez por cento) superior àquela, em que os licitantes apresentarão lances públicos e sucessivos, até o encerramento da sessão e eventuais prorrogações.

5.14.1. Não havendo pelo menos 3 (três) propostas nas condições definidas no item 5.14, poderão os licitantes que apresentaram as três melhores propostas, consideradas as empatadas, oferecer novos lances sucessivos.

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

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

5.14.4. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

5.14.5. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

5.14.6. Após o reinício previsto no subitem supra, os licitantes serão convocados para apresentar lances intermediários.

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

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

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

5.18. 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.22.2.2. empresas brasileiras;

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

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

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

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

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

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

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

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

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

6. DA FASE DE JULGAMENTO

6.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 2.5 do edital, especialmente quanto

à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

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

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

6.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

6.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

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

6.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação.

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

6.4. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

6.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com os itens 2.4 e 3.6 deste edital.

6.6. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos.

6.7. Será desclassificada a proposta vencedora que:

6.7.1. contiver vícios insanáveis;

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

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

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

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

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

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

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

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

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

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

6.11. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço.

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

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

6.13. Caso o Termo de Referência exija a apresentação de amostra, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no Termo de Referência, sob pena de não aceitação da proposta.

6.14. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

6.15. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

6.16. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

6.17. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

7. DA FASE DE HABILITAÇÃO

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

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

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

7.3. Os documentos exigidos para fins de habilitação poderão ser apresentados em original ou por cópia nos termos do inciso IV do art. 12 da Lei Federal nº 14.133/2021.

7.4. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido pelo Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133/2021.

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

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

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

7.8. Os documentos exigidos para habilitação detalhados no Termo de Referência serão enviados **por meio da plataforma de Pregão Eletrônico escolhido pela administração, em formato digital, no prazo de MÍNIMO DE DUAS HORAS**, prorrogável por igual período, contado da solicitação do pregoeiro.

7.9. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir.

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

7.11. **A exigência dos documentos de habilitação que constem do Termo de Referência somente será feita em relação ao licitante vencedor.**

7.12. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para:

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

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

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

7.13.1 - Nos termos dos Acórdãos 1211/2021 e 2443/2021 do Plenário do TCU, a vedação à inclusão de novo documento, prevista no art. 64 da Nova Lei de Licitações (Lei 14.133/2021) não alcança documento destinado a atestar condição de habilitação preexistente à abertura da sessão pública, que não foi juntado com os demais comprovantes de habilitação e/ou da proposta, por equívoco ou falha, o qual deverá ser solicitado e avaliado pelo pregoeiro/agente de contratação.

7.13.2 - Na falta de documento relativo à fase de habilitação em pregão que consista em mera declaração do licitante sobre fato preexistente ou em simples compromisso por ele firmado, deve o pregoeiro conceder-lhe prazo razoável para o saneamento da falha, em respeito aos princípios do formalismo moderado e da razoabilidade, bem como ao art. 2º, caput, da Lei 9.784/1999. Acórdão 988/2022-Plenário.

7.14. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no subitem 7.8.

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

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

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

8. DOS RECURSOS

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

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

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

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

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

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

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

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

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

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

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

8.10. Os autos do processo permanecerão com vista franqueada aos interessados no Departamento de Licitação, situado na Rua Coronel Vidal, 800, São Dimas, neste município.

9. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

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

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

9.3. A impugnação e o pedido de esclarecimento deverão ser realizados na Plataforma Eletrônica BLL Compras, no seguinte endereço eletrônico https://bll.org.br/.

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

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

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

10. DA HOMOLOGAÇÃO

10.1. Depois de homologado o resultado deste Pregão, a licitante vencedora será convocada para assinar o contrato, dentro do prazo de até 03 (três) dias úteis de sua convocação, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste edital.

10.1.1. O prazo de convocação de que trata o item 11.1 poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação da licitante vencedora durante seu transcurso, devidamente justificada, e desde que o motivo apresentado seja aceito pela Administração.

11. FORMALIZAÇÃO DO CONTRATO

11.1. Será permitida a assinatura eletrônica do contrato, mediante uso da certificação digital ICP Brasil, caso o representante legal da licitante a possua, no mesmo prazo indicado no item 11.1.

11.2. O Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul poderá enviar o contrato para assinatura da licitante, que deverá devolvê-lo assinado no prazo previsto no item 11.1.

11.3. Caso a licitante vencedora convocada não realize a assinatura do contrato no prazo estabelecido no item 11.1, será facultado à Administração, através do Pregoeiro, convocar os licitantes remanescentes, na ordem de classificação, observando-se o disposto nos §§2º e 4º do art. 90 da Lei nº 14.133/2021.

11.4. Por ocasião da assinatura do contrato, verificar-se-á, se a licitante vencedora mantém as condições de habilitação e, ainda, se atende ao disposto no §4º do art. 91 da Lei nº 14.133/2021.

12. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

12.1. Comete infração administrativa o licitante, o adjudicatário ou o contratado que, com dolo ou culpa cometer quaisquer das infrações previstas no art. 155 da Lei nº 14.133, de 2021, quais sejam:

a. Dar causa à inexecução parcial do contrato (inciso I do art. 155 da Lei 14.133/2021);

a.1. Dar causa à inexecução parcial do contrato significa que o licitante ou o contratado, por ação ou omissão, provoca a não realização de uma ou mais obrigações específicas previstas no contrato, sem que essa inexecução comprometa a sua totalidade.

b. Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo (inciso II do art. 155 da Lei 14.133/2021);

b.1. Dar causa à inexecução parcial do contrato que cause grave dano significa que o licitante ou o contratado, por ação ou omissão, provoca a não realização de uma ou mais obrigações específicas previstas no contrato, sem que essa inexecução comprometa a sua totalidade, sendo agravada pelo fato de gerar prejuízos significativos à Administração Pública, ao funcionamento dos serviços públicos ou ao interesse coletivo.

c. Dar causa à inexecução total do contrato (inciso III do art. 155 da Lei 14.133/2021);

c.1. Dar causa à inexecução total do contrato refere-se à situação em que o contratado, por meio de ação ou omissão, impede completamente a realização do objeto contratual, levando à sua não execução integral.

d. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo(a) agente de contratação/comissão de contratação durante o certame (inciso IV do art. 155 da Lei 14.133/2021);

e. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando (inciso V do art. 155 da Lei 14.133/2021):

e.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

e.2. recusar-se a enviar o detalhamento da proposta quando exigível;

e.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou

e.4. deixar de apresentar amostra;

e.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

f. Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta (inciso VI do art. 155 da Lei 14.133/2021);

f.1. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

g. Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado (inciso VII do art. 155 da Lei 14.133/2021);

h. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato (inciso VIII do art. 155 da Lei 14.133/2021);

i. Fraudar a licitação ou praticar ato fraudulento na execução do contrato (inciso IX do art. 155 da Lei 14.133/2021);

j. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza (inciso X do art. 155 da Lei 14.133/2021);

j.1. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances;

k. Praticar atos ilícitos com vistas a frustrar os objetivos deste certame (inciso XI do art. 155 da Lei 14.133/2021);

L. Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013 (inciso XII do art. 155 da Lei 14.133/2021).

12.1.1. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação.

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

a) Advertência no caso da falta prevista no subitem "a" do item 12.1 deste edital de licitação, quando não se justificar a imposição de penalidade mais grave;

b) Multa:

1. moratória de 0,2% (dois décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, bem como pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia, quando exigida, até o limite de 30 (trinta) dias;

1.1. O atraso superior a 30 dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

2. Compensatória, para as infrações descritas nas alíneas h, i, j, k, L do subitem 12.1, de 10% a 30% do valor do Contrato.

3. Compensatória, para a inexecução total do contrato prevista na alínea "c", "f" do subitem 12.1, de 5% a 20 % do valor do Contrato.

4. Para infração descrita na alínea "b" do subitem 12.1, a multa será de 5% a 15% do valor do Contrato.

5. Para infrações descritas nas alíneas "d", "e", "g" do subitem 9.1, a multa será de 1% a 10 % do valor do Contrato.

6. Para a infração descrita na alínea "a" do subitem 12.1, a multa será de 0,5% a 5% do valor do Contrato.

7. A multa será recolhida no prazo máximo de 30 dias úteis, a contar da comunicação oficial.

c) Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, nos casos das alíneas "b" a "g" do subitem 12.1 deste edital de licitação, quando não se justificar a imposição de penalidade mais grave;

d) Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos das alíneas "h" a "L", do subitem 12.1, bem como pelas infrações administrativas previstas, b, c, d, e, f, g do subitem 12.1, que justifiquem a imposição da penalidade mais grave conforme §5º do art. 156 da Lei 14.133/2021.

12.3. Na aplicação das sanções serão considerados:

12.3.1. A natureza e a gravidade da infração cometida;

12.3.2. As peculiaridades do caso concreto;

12.3.3. As circunstâncias agravantes ou atenuantes;

12.3.4. Os danos que dela provierem para a Administração Pública;

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

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

12.5. A aplicação das sanções previstas neste edital de licitação, não exclui em hipótese alguma, a obrigação de reparação integral do dano causado ao Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul .

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

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

12.8. A aplicação das sanções (penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar) realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021.

12.9. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

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

12.11. Para a garantia da ampla defesa e contraditório dos licitantes, as notificações serão enviadas para o endereço comercial, ou enviadas eletronicamente para os endereços de e-mail informados na proposta comercial, ou cadastrados pela empresa no Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul .

12.11.1. Os endereços de e-mail informados na proposta comercial e/ou cadastrados e ou fornecidos serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

12.11.2 As notificações poderão ser enviadas também por outros meios, desde que comprovadamente enviadas.

12.12 - Os débitos do Contratado para com a Administração Contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o Contratado possua com o mesmo órgão ora Contratante.

12.13. Quando se tratar de registro de preços, as regras previstas nesta tópica, especialmente as relacionadas às infrações administrativas, procedimentos e sanções, aplicam-se à gestão da ata de registro de preços.

13. DAS DISPOSIÇÕES GERAIS

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

13.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, **a sessão será automaticamente transferida para o primeiro**

dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

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

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

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

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

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

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

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

13.10. O Edital está disponibilizado, na íntegra, no endereço eletrônico da Plataforma indicada no item 2.1 deste edital e no site do Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul através do endereço http://www.cisdeste.saude.mg.gov.br/editais/licitacoes/, também poderão ser lidos e/ou obtidos na sala da CPL da CISDESTE, localizada na Rua Coronel Vidal, nº 800, São Dimas, neste município nos dias úteis, no horário das 08:00:00 às 17:30:00 horas, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

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

13.11.1. Anexo I – Termo de Referência;

13.11.1.1. Anexo I do TR – Planilha Orçamentária;

13.11.1.2. Anexo II do TR – Descritivo Técnico do Projeto de Infraestrutura e Serviços;

Fls. nº

13.11.2. Anexo II – Modelo de Proposta;

13.11.3. Anexo III – Minuta de Termo de Contrato;

13.11.4. Estudo Técnico Preliminar – Apêndice do TR.

13.11.4.1 - Anexo I do ETP – Descritivo Técnico do Projeto de Infraestrutura e Serviços.

Juiz de Fora, 17/12/2025.

Daudiceia Renata Moreira
Coordenadora de Compras e Licitação

ANEXO I

TERMO DE REFERÊNCIA

1 - OBJETO

1.1 - Contratação de empresa especializada na prestação de SERVIÇOS TÉCNICOS na área de TECNOLOGIA DA INFORMAÇÃO E TELECOMUNICAÇÕES, para atender as necessidades do CISDESTE, conforme condições e especificações contidas neste termo de referência.

2 - DA PADRONIZAÇÃO

1.2 - A contratação se dará em observância ao princípio da padronização, em consonância com o disposto no inciso IV do art. 19 da Lei 14.133/2021 e da Resolução CISDESTE nº 08/2023.

3 - DA ADEQUAÇÃO DA MODALIDADE LICITATÓRIA ELEITA

3.1 - Considerando as características do(s) serviço(s) a ser(em) contratado(s), o objeto desta contratação foi caracterizado como serviço(s) comum(ns), conforme Estudo Técnico Preliminar, possuindo, desse modo, padrões de desempenho e características gerais e específicas, usualmente e amplamente encontrados no mercado correlato.

4 - DESCRIÇÃO E ESPECIFICAÇÃO DO OBJETO

Item	Descrição	Unid.	Quant.
1	Suporte técnico ao usuário (via telefone, e-mail, acesso remoto e presencial); manutenção preventiva e corretiva; suporte a serviços; monitoramento; gerência proativa; fornecimento e manutenção de solução de e-mail; atualização de softwares e firmware dos equipamentos.	mês	12
2	Fornecimento e gerência de 05 (cinco) links de Internet destinados aos setores Administrativo e de Regulação.	mês	12
3	Fornecimento e gerência de 01 (um) link de Internet destinado ao setor de Almoxarifado.	mês	12

5 - PRAZO DE VIGÊNCIA

5.1 - O prazo de vigência da contratação será 12 (doze) meses, contados da data de assinatura do contrato, podendo ser prorrogado por até 10 anos nos termos do art. 106 e 107 da Lei 14.133/21, desde que a autoridade competente ateste que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado ou a extinção contratual sem ônus para qualquer das partes, conforme Estudo Técnico Preliminar.

6 - DA FUNDAMENTAÇÃO E DA DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO (ART. 6º, INCISO XXIII, ALÍNEA "B", DA LEI Nº 14.133, DE 2021)

6.1 - A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

7 - DA DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E DA ESPECIFICAÇÃO DO PRODUTO (ART. 6º, INCISO XXIII, ALÍNEA "C", E ART. 40, §1º, INCISO I, DA LEI Nº 14.133, DE 2021)

7.1 - A descrição da solução como um todo encontra-se pormenorizada em tópico específico do(s) Estudo(s) Técnico(s) Preliminar(es) e seus anexos, apêndice deste Termo de Referência.

8 - REQUISITOS DA CONTRATAÇÃO

8.1 - Os requisitos da contratação relacionados a natureza do objeto e a sustentabilidade encontra-se pormenorizado em tópico específico do(s) Estudo(s) Técnico(s) Preliminar(es), apêndice deste Termo de Referência.

8.2 - Registre-se que, eventual exigência de documentação de habilitação técnica e econômica, será tratado no tópico específico deste TR (CRITÉRIOS DE SELEÇÃO DO FORNECEDOR) de modo que sua inclusão aqui seria redundante.

8.3 - Indicação de marcas ou modelos (41, inciso I, da Lei nº 14.133, de 2021)

8.3.1 - Na presente contratação NÃO será indicado marcas, características ou modelo(s).

8.4 - Da vedação de utilização de marca/produto na execução do serviço

8.4.1 - Para a contratação do objeto NÃO haverá vedação ou restrições com relação ao emprego de marca ou produto de bens empregados em sua execução.

8.5 - Da exigência de carta de solidariedade

8.5.1 - Não será exigido Carta de Solidariedade emitida pelo fabricante.

8.6 - Subcontratação

8.6.1 - NÃO será admitida a subcontratação do objeto contratual.

8.7 - Garantia da contratação

8.7.1 - Não haverá exigência de garantia contratual da execução.

9 - MODELO DE EXECUÇÃO DO OBJETO

9.1 - CONDIÇÕES DE EXECUÇÃO

9.1.1 - O prazo de execução do(s) serviços(s) começará a fluir a partir do 1º (primeiro) dia útil seguinte ao do recebimento da Ordem de Serviço, a ser emitido pelo Setor de Compras ou pelo setor requisitante.

9.1.2 - Para a execução do objeto a CONTRATADA deverá seguir a seguinte dinâmica:

9.1.2.1 - Os serviços serão prestados no seguinte endereço:

- Sede Administrativa e Central de Regulação: Rua Coronel Vidal, n°800 - Bairro São Dimas - Juiz de Fora - MG.

- Almoxarifado: Rua Coronel Vidal, nº 1.792 Galpão: 09 - Bairro São Dimas - Juiz de Fora - MG.

9.1.2.2 - Além da execução presencial nas instalações acima, a CONTRATADA deverá prestar:

a) suporte remoto para usuários, servidores, rede, telefonia IP, firewalls, switches, roteadores, serviços virtualizados e demais ativos mencionados no Anexo II;

b) atendimento emergencial presencial quando a natureza da ocorrência impedir solução remota;

c) monitoramento proativo e contínuo dos serviços críticos (servidores, links, telefonia, VPN, firewall, virtualização etc.);

d) gestão dos links de Internet, com comunicação direta com as operadoras contratadas;

e) suporte técnico nas unidades e bases operacionais, quando necessário para correção de incidentes que afetem a comunicação com o Complexo Regulador.

9.1.2.3 - Considerando que o CISDESTE opera serviço essencial (SAMU 192) em regime ininterrupto (24h/dia, 7 dias/semana), a CONTRATADA deverá assegurar:

a) Atendimento remoto 24h, inclusive sábados, domingos e feriados;

b) Atendimento presencial mínimo em horário comercial, com deslocamento emergencial em situações críticas;

c) Plano de contingência para indisponibilidades que afetem telefonia, rede, servidores ou comunicação com bases;

d) Resposta imediata a incidentes de alta criticidade.

9.1.2.3 - A execução deverá observar:

a) abertura, acompanhamento e encerramento de chamados em sistema de gestão de tickets (próprio da CONTRATADA ou disponibilizado pelo CISDESTE);

b) emissão de relatórios periódicos de atendimento, incidentes, manutenções, configurações e atualizações;

c) comunicação tempestiva ao setor requisitante diante de eventuais riscos, vulnerabilidades ou falhas críticas;

d) registro de acesso remoto e presencial para fins de auditoria.

9.1.2.4 - Para garantir a plena execução dos serviços, a CONTRATADA deverá:

I - manter equipe técnica qualificada e compatível com os níveis de complexidade descritos neste Termo;
II - executar manutenções preventivas e corretivas;
III - atualizar sistemas, firmwares, máquinas virtuais, serviços e regras de firewall;
IV - administrar, monitorar e configurar a central telefônica IP Asterisk;
V - manter a integridade dos ambientes virtualizados, com políticas de backup e recuperação;
VI - preservar a documentação técnica, inventários, diagramas e configurações;
VII - garantir confidencialidade e segurança das informações tratadas;
VIII - cumprir os prazos de atendimento estabelecidos na matriz de criticidade.

9.1.2.5 - A dinâmica de execução acima descrita está intimamente vinculada às características da infraestrutura detalhada no ANEXO II – DESCRITIVO TÉCNICO DO PROJETO DE INFRAESTRUTURA E SERVIÇOS, devendo a CONTRATADA observar permanentemente tais especificações para assegurar a continuidade e a estabilidade das operações do CISDESTE.

10 - MODELO DE GESTÃO DO CONTRATO

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

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

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

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

10.5 - Após a assinatura do contrato ou instrumento equivalente, o(a) Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul, **poderá** convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

10.6 - A responsabilidade pela gestão do contrato caberá ao(à) servidor(a) ou comissão designados, conforme item 10.8 deste termo, o(a) qual será responsável pelas atribuições definidas em regulamento próprio do(a) Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul.

10.7 - A responsabilidade pela fiscalização do contrato caberá ao(à) servidor(a) ou comissão designados, conforme item 10.8 deste TR, o(a) qual será responsável pelas atribuições definidas em regulamento próprio do(a) Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul.

10.8 - Os responsáveis pela gestão e fiscalização do contrato serão designados por ato administrativo próprio do Contratante.

10.9 - A gestão e a fiscalização do contrato serão exercidas pelo Contratante, que realizará a fiscalização, o controle e a avaliação dos bens fornecidos, bem como aplicará as penalidades, após o devido processo legal, caso haja descumprimento das obrigações contratadas.

11 - CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

11.1 - A avaliação da execução do objeto utilizará o disposto neste item.

11.1.1 - Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

11.1.1.1 - Não produzir os resultados acordados;

11.1.1.2 - Deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

11.1.1.3 - Deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

12 - DO RECEBIMENTO

12.1 - Os serviços serão recebidos provisoriamente, no prazo de 2 (dois) dias, pelos fiscal(is), mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a , da Lei nº 14.133).

12.1.1 - O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

12.1.2 - O fiscal do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico e administrativo.

12.2 - O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

12.2.1 - A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021)

12.2.2 - O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

12.2.3 - Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

12.3 - Os serviços serão recebidos definitivamente no prazo de 2 (dois) dias, contados do recebimento provisório, pelo gestor do contrato, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

12.3.1 - Realizar a análise de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções;

12.3.2 - Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nas documentações apresentadas, quando for o caso;

12.3.3 - Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

12.3.4 - Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

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

12.5 - Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

12.6 - 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.

12.7 - Quando a fiscalização e a gestão do contrato justificadamente forem exercidas por um único servidor, caberá a ele praticar todos os atos relacionados ao recebimento provisório e definitivo do objeto.

12.8 - O recebimento provisório e definitivo poderá ser substituído por recibo ou outra forma simples, quando justificadamente, forem suficientes para atestar o atendimento das exigências contratuais.

13 - LIQUIDAÇÃO

13.1 - Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período.

13.2 - os documentos fiscais de cobrança deverão ser emitidos contra a(o) CISDESTE, CNPJ nº 17.813.026/0001-51, situada a Rua Coronel Vidal, 800, São Dimas, Juiz de Fora.

13.2.1 - Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

a) o prazo de validade;b) a data da emissão;c) os dados do contrato e do órgão contratante;d) o período respectivo de execução do contrato;e) o valor a pagar; ef) eventual destaque do valor de retenções tributárias cabíveis.

13.3 - Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus à contratante;

13.4 - A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133/2021.

13.5 - A Administração deverá realizar consulta para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

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

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

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

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

14 - PRAZO DE PAGAMENTO

14.1 - O pagamento será efetuado no prazo máximo de até 10 dias úteis, contados da finalização da liquidação da despesa, conforme seção anterior.

14.2 - No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA (Índice de preços ao consumidor) de correção monetária.

15 - FORMA DE PAGAMENTO

15.1 - O pagamento será realizado através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

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

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

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

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

16 - REAJUSTE

16.1 - Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado.

16.2 - Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do IPCA (Índice de preços ao

consumidor) acumulado dos últimos doze meses, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

16.3 - Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

16.4 - No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

16.5 - Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

16.6 - Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

16.7 - Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

16.8 - O reajuste será realizado por apostilamento.

17 - FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

17.1 - Forma de seleção e critério de julgamento da proposta

17.1.1 - O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo **MENOR PREÇO GLOBAL realizada em único item.**

17.2 - MODO DE DISPUTA

17.2.1 - Modo de disputa – **Aberto.**

17.3 - Exigências de habilitação

17.3.1 - Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

17.4 - Habilitação jurídica (Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva)

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

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

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

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

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

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

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

17.5 - Habilitação fiscal, social e trabalhista

17.5.1 - Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas;

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

17.5.3 - Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

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

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

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

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

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

17.6 - Qualificação Econômico-Financeira

17.6.1 - Será exigido Qualificação Econômico Financeira, conforme exigência abaixo:

Certidão Negativa de Falência e Concordata, expedida pelo distribuidor da sede da licitante.

17.7 - Qualificação Técnica

17.7.1 - A documentação relativa à qualificação técnico-profissional e técnico-operacional observará o art. 67 da Lei nº 14.133/2021 e será restrita às parcelas de maior relevância do objeto, conforme disposto abaixo:

I - Comprovação de Aptidão Técnico-Operacional

A licitante deverá apresentar atestados de capacidade técnica, emitidos por pessoas jurídicas de direito público ou privado, registrados no conselho profissional competente quando aplicável, que comprovem experiência prévia na execução de serviços de complexidade tecnológica equivalente ou superior às parcelas de maior relevância do objeto, a saber:

a) suporte técnico remoto e presencial;
b) administração de redes LAN e WAN;
c) administração de servidores;

d) operação de ambientes virtualizados;
e) administração de firewalls;
f) gestão de central telefônica IP (Asterisk);
g) administração de banco de dados MySQL;
h) suporte a sistemas operacionais Linux e Windows;
i) gestão de rotinas de backup e monitoramento.

Os atestados deverão comprovar que tais serviços foram executados, em períodos sucessivos ou não, pelo **prazo mínimo de 24 (vinte e quatro) meses**, conforme art. 67, §5º da Lei 14.133/2021.

Será admitida a apresentação de **um ou mais atestados**, cujo somatório permita demonstrar a execução dos quantitativos e características mínimas exigidas.

II - Comprovação de Capacidade Técnico-Profissional

A licitante deverá comprovar que possui, **em seu quadro permanente**, na data prevista para entrega das propostas, **profissional devidamente registrado no conselho profissional competente**, detentor de:

a) Atestado de Responsabilidade Técnica (ART ou equivalente) referente à execução de serviços de TI/Telecom que envolvam, no mínimo, as parcelas de maior relevância descritas no inciso anterior;

b) Certidão de Acervo Técnico – CAT, vinculada ao referido atestado, demonstrando experiência em ambientes de suporte técnico, redes LAN/WAN, servidores, virtualização, firewalls, telefonia IP e demais componentes relevantes ao objeto.

III - Atendimento à Legislação Setorial (ANATEL)

Para a atividade de **gestão e fornecimento de link de Internet**, deverá ser apresentado:

- **extrato do Termo de Autorização** emitido pela **ANATEL**, vigente, publicado no Diário Oficial da União, autorizando a empresa a prestar o Serviço de Comunicação Multimídia (SCM).

IV - Validação dos Atestados e Documentos

A Administração poderá, sempre que julgar necessário, solicitar à licitante documentos adicionais para comprovar a legitimidade dos atestados apresentados, tais como:

- cópia do contrato vinculado ao atestado;
- endereço atualizado da contratante que emitiu o atestado;
- indicação do local de execução dos serviços;

- dados de contato do gestor do contrato;
- outros documentos que se façam necessários.

Os atestados poderão ser apresentados em nome da **matriz ou filial** da licitante, conforme previsto na legislação vigente.

17.8 - Vistoria

17.8.1 - Tendo em vista a natureza e as peculiaridades do objeto a ser contratado, a avaliação prévia do local de execução é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, devendo o licitante atestar, sob pena de inabilitação, que conhece o local e as condições de realização do serviço, assegurado a ele o direito de realização de vistoria prévia.

17.8.2 - O licitante que optar por realizar vistoria prévia terá disponibilizado pela Administração data e horário exclusivos, a ser agendado através do e-mail: licitacao@cisdeste.saude.mg.gov.br, de modo que seu agendamento não coincida com o agendamento de outros licitantes.

17.8.3 - Caso o licitante opte por não realizar vistoria, poderá substituir a declaração exigida no presente item por declaração formal assinada pelo seu responsável técnico acerca do conhecimento pleno das condições e peculiaridades da contratação.

18 - ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

18.1 - O custo estimado da contratação encontra-se detalhado no ANEXO I deste Termo de Referência, tendo sido juntado no processo os preços unitários referenciais, das memórias de cálculo e dos documentos que lhe dão suporte, com os parâmetros utilizados para a obtenção dos preços e para os respectivos cálculos.

19 - ADEQUAÇÃO ORÇAMENTÁRIA

19.1 - As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento do(a) Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul.

19.1.1 - A contratação será atendida pela seguinte dotação:

3.3.90.39.00.1.02.01.10.302.0001.2.0003 1.633.000 RATEIO MACRO SUDESTE - GESTÃO DO CONSÓRCIO.

19.2 - A dotação relativa aos exercícios financeiros subsequentes, quando se tratar de serviços e fornecimento contínuos será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

Fls. nº

20 - INFORMAÇÕES COMPLEMENTARES

20.1 - As empresas são responsáveis pela fidelidade e legitimidade das informações prestadas e dos documentos apresentados. A falsidade de qualquer documento apresentado ou a inverdade das informações nele contidas implicará na imediata rescisão contratual, sem prejuízo das sanções administrativas, civis e penais cabíveis.

20.2 - Toda a documentação apresentada neste procedimento e seus anexos são complementares entre si, de modo que qualquer detalhe que se mencione em um documento e se omita em outro será considerado especificado e válido.

Juiz de Fora, 10/12/2025.

Rafael Pontes Miranda
Gerente Administrativo

Luiz Fernandes Novais Oliveira
Assessor Técnico

Acxel Albrecht Araújo
Supervisor de Planejamento e Contratações Públicas

ANEXO I DO TR

PLANILHA DE PREÇO ESTIMADO

O valor estimado foi definido com base na média dos valores, obtidos nas pesquisas de preços de acordo com o mapa de apuração abaixo:

Item	Descrição	Unid.	Quant.	Valor Unit.	Valor Total
1	Suporte técnico ao usuário (via telefone, e-mail, acesso remoto e presencial); manutenção preventiva e corretiva; suporte a serviços; monitoramento; gerência proativa; fornecimento e manutenção de solução de e-mail; atualização de softwares e firmware dos equipamentos.	mês	12	R$ 18.399,66	R$ 220.795,92
2	Fornecimento e gerência de 05 (cinco) links de Internet destinados aos setores Administrativo e de Regulação.	mês	12	R$ 2.360,48	R$ 28.325,76
3	Fornecimento e gerência de 01 (um) link de Internet destinado ao setor de Almoxarifado.	mês	12	R$ 648,38	R$ 7.780,56

O valor total estimado para a contratação é de **R$ 256.902,24 (duzentos e cinquenta e seis mil e novecentos e dois reais e vinte e quatro centavos).**

ANEXO II DO TR

DESCRITIVO TÉCNICO DO PROJETO DE INFRAESTRUTURA E SERVIÇOS

1 - DESCRIÇÃO DO PROJETO

O projeto consiste em definir a melhor solução de Telecomunicações que atenda às necessidades atuais e futuras para o Serviço de Atendimento Móvel de Urgência (SAMU), onde será necessário a contratação de uma empresa, com capacidade de desenvolver, implantar e gerir o seu ambiente tecnológico, baseado na definição de projeto aqui colocada. A empresa deverá implantar e configurar a infraestrutura de Telecomunicações e TI, com enfoque na central de telefonia IP baseada no ASTERISK (O Asterisk é um software Livre, de código aberto, que implementa em software os recursos encontrados em um PABX convencional, utilizando tecnologia de telefonia IP) e seus componentes, fornecer suporte remoto e local na sede do SAMU, conforme descritivo técnico a seguir:

1.1 - REDE - INFRAESTRUTURA DE REDE FÍSICA (NCPI)

1.1.1. Definição

Para substituir sistemas convencionais de telecomunicações e centrais de PBX, a rede de telefonia IP e de dados terá que oferecer uma disponibilidade similar ou superior que irão se colocar a prova num campo onde o conceito de alta disponibilidade já é esperado. Um dos maiores motivos pelos quais os sistemas convencionais PBX possuem uma alta disponibilidade é o fato deles possuírem um sistema com bateria de backup de longa autonomia. Oferecer energia através da rede para o telefone IP (Power over Ethernet - PoE, energia através do cabo de rede IEEE 802.3af) terá que explorar em campo o conceito de fornecer energia para atingir a disponibilidade esperada. Por isso os racks de Telecom convencionais, que eram usados para armazenar dispositivos passivos como painéis de cabos e outros, agora vão precisar acomodar switches PoE de alta potência, roteadores, elementos de comutação ótica e Nobreaks com grande autonomia. A refrigeração e o fluxo de ar nessas salas de Telecom se tornarão importantes para garantir uma operação contínua.

A rede de Telefonia IP e de dados descrita é construída em camadas e cada camada é formada por componentes que residem em uma de suas 4 localizações físicas (Figura 1).

Necessidades de energia e refrigeração para essas quatro localidades variam de acordo com o descrito nas próximas seções e baseados em normas internacionais de operação.

Como tratamos de uma Infraestrutura Física de Rede Crítica (NCPI) que é o alicerce de todas as redes de alta disponibilidade, devemos levar em conta que esta deve ser sólida, escalável, altamente disponível, gerenciável e incluir:

1. Sistemas de energia como Nobreaks, unidades de distribuição de energia (PDUs) e geradores para fornecimento de energia e refrigeração para cargas críticas.
2. Sistemas de refrigeração para manter um ambiente ideal com regulação da temperatura e umidade.
3. Racks com equipamentos de redes críticas como switches L2 e L3, roteadores, gateways E1 e Internet, servidores, etc.
4. Sistemas de segurança física, virtual e proteção contra incêndio.
5. Cabeamento para interconexão dos equipamentos
6. Sistemas de gerenciamento que se comunicam local e remotamente, com serviços integrados para assegurar um funcionamento eficiente 24 horas por dia, 7 dias por semana. 365 dias por ano.
7. Serviços de suporte local, além de manutenção e diagnóstico

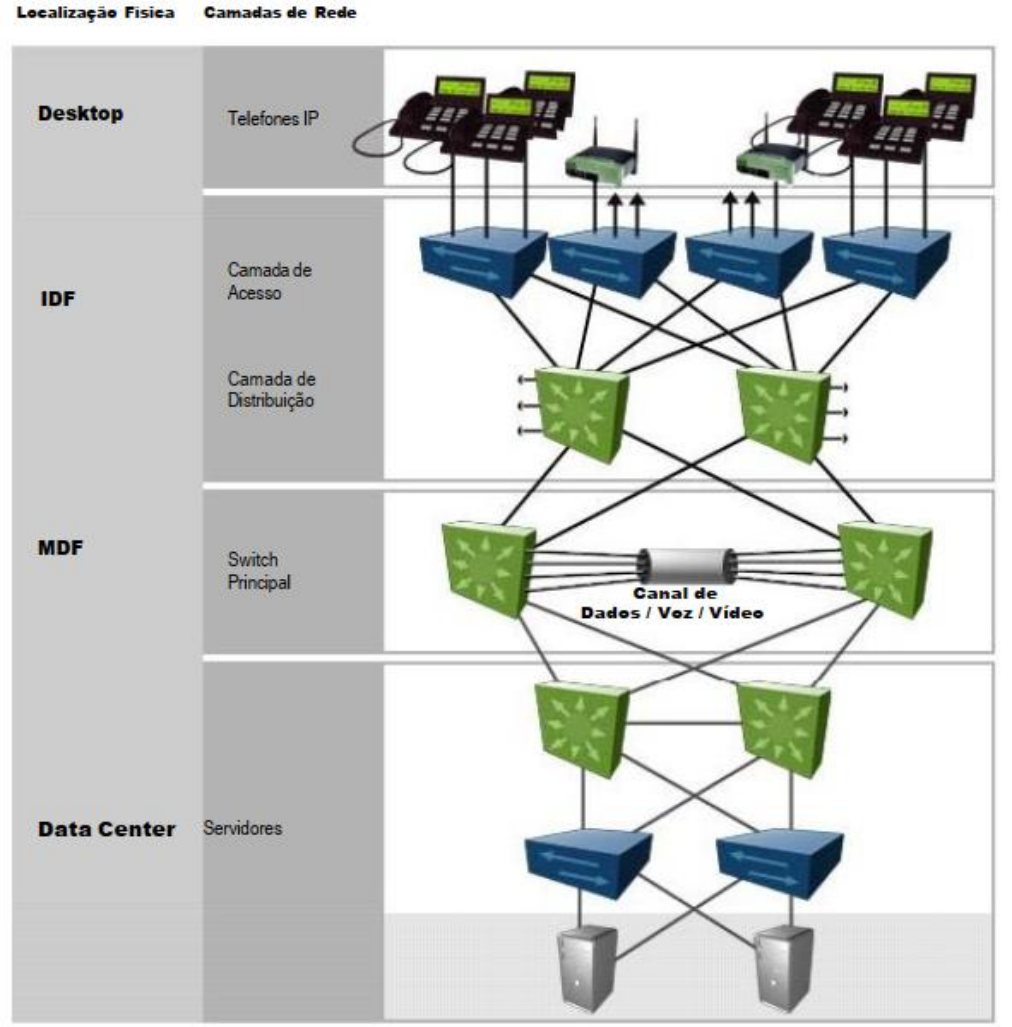


Figura 1 *– Camadas e localizações de uma rede de Telefonia IP Típica.*

1.1.2. Objetivo

Implantar e configurar a infraestrutura de rede, capaz de fornecer dados e telefonia IP para o complexo regulador do SAMU dentro dos padrões para NCPI (figura 1).

A rede terá as definições lógicas e de segurança segmentadas em três partes distintas. Telefonia/Suporte (NCPI) com faixa IP própria, roteador de comunicação e integração VPN com outras redes de emergência. Regulação NCPI com faixa IP própria e seu Firewall. Administrativo e uso geral com faixa IP própria e seu firewall.

1.1.3. Infraestrutura LocaL

Para a implantação deste projeto, foi definido condições mínimas de ambiente, cabeamento, energia e refrigeração que seguem abaixo:

Dispositivos de Comunicação

Os dispositivos de comunicação típicos na ponta, são telefones IP (Figura 2a), assim como computadores e dispositivos de rede sem fio (Figura 2b), oferecendo funções de telefonia e dados. O consumo típico dos telefones IP é de 6-7 Watts, porém alguns dispositivos podem consumir mais energia. A norma, IEEE 802.3af, limita a corrente média drenada por esses dispositivos com cabos CAT5 para 350mA e especifica os pinos através dos quais a energia pode ser transmitida. Com o cumprimento dessa nova norma, aproximadamente 15W de energia poderão ser fornecidos a uma distância de até 100m. Para o consumo de energia acima desta distância, os dispositivos de comunicação terão que contar com fontes externas.

Figura 2a *– Telefone IP.*

Figura 2b *– Roteador Wireless.*

Ambiente

Estes dispositivos localizam-se nos ambientes da regulação médica e setor administrativo, são montados nas baias das mesas da regulação ou usados no ambiente de escritório do administrativo. Para instalações novas ou atualizadas, eles poderão ser alimentados pela linha de dados. Entretanto, em alguns casos, poderão ser alimentados através das tomadas da rede elétrica.

Desafios

Os telefones IP precisam estar tão disponíveis quanto os telefones PBX que eles substituem. Aqui, o maior problema, é assegurar sua operação mesmo durante uma queda de energia prolongada.

Melhores Práticas

Enviar energia através da linha de dados para o telefone (chamada de energia In-Line) é a melhor maneira de resolver este problema. Desta maneira, o telefone é alimentado pelo switch da rede localizado na sala de Telecom suportado por um Nobreak com grande autonomia. Para os dispositivos alimentados pela tomada de rede elétrica (não usando energia In-Line), pode ser usado um Nobreak com um longo tempo de autonomia (quatro, seis, oito horas ou mais).

IDF - Intermediate Distribution Frame (Ambiente de Distribuição Intermediário)

O IDF incorpora as camadas de acesso 2 e 3, com a distribuição de switches, roteadores, painéis de cabos, Nobreaks, bem como qualquer outro equipamento de telecomunicação montado em um rack (Figura 3a e 3b). Os switches utilizados possuem a capacidade de fornecer energia através de linhas de dados para alimentar os dispositivos de comunicação. Para switches sem essa capacidade, uma fonte de energia externa apropriadamente dimensionada é usada para injetar a energia In-Line.

Figura 3a *– IDF (rack de Telecom).*

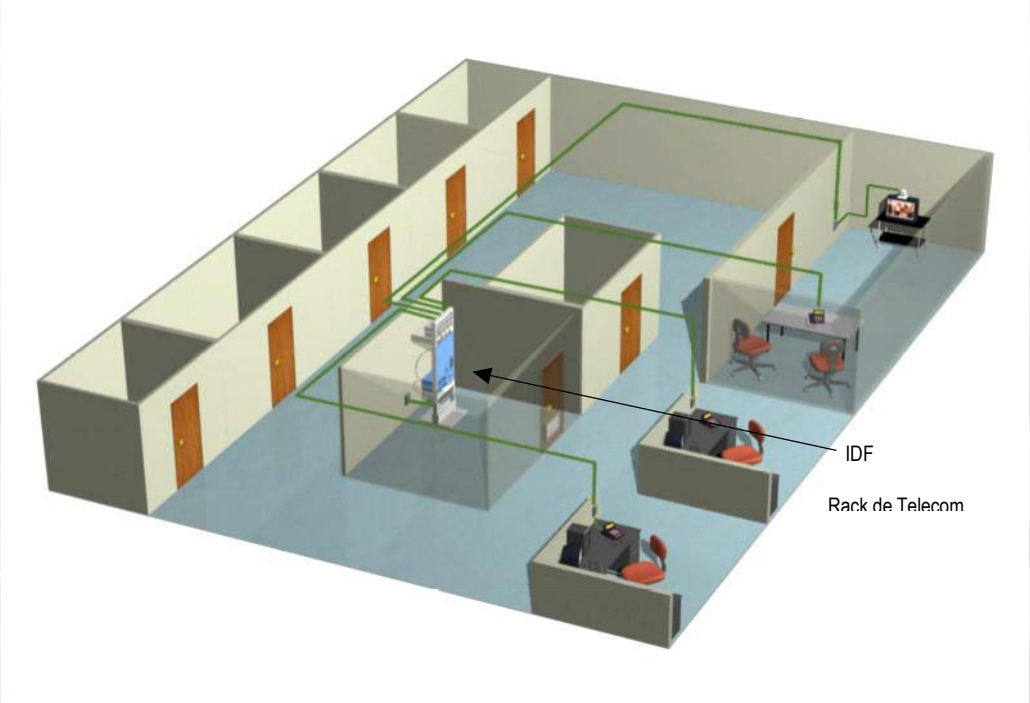


Figura 3b *– Layout Típico do IDF.*

Ambiente

Os IDFs para o projeto de rede do SAMU normalmente ficam na mesma sala dos MDFs e Data Center ou sala de servidores. Redes de telecomunicações convencionais normalmente usam esses racks para painéis de cabos e alguns switches de pequeno porte, porém os novos sistemas de Telefonia IP usam e dissipam consideravelmente mais energia. Estes novos Switches para Telefonia IP são geralmente montados em racks de 19" e tem um padrão de fluxo de ar que varia, dependendo do fabricante, por exemplo, lado a lado, de frente para trás, etc. Um IDF típico utilizará de 1 a 3 racks com equipamentos, e consumirá de 500 W a 4.000 W de energia CA monofásica ou bifásica. O croqui de exemplo é usado como referencial técnico. Nele todas as camadas NCPI são conjugadas.

O ambiente necessário para acomodações dos equipamentos, deverá possuir uma área útil de no mínimo 12m², uma das paredes deve possuir no mínimo 3,60m, sem obstáculos (porta, janela etc.) para instalação dos racks de telecomunicações, conforme figura 3c abaixo:

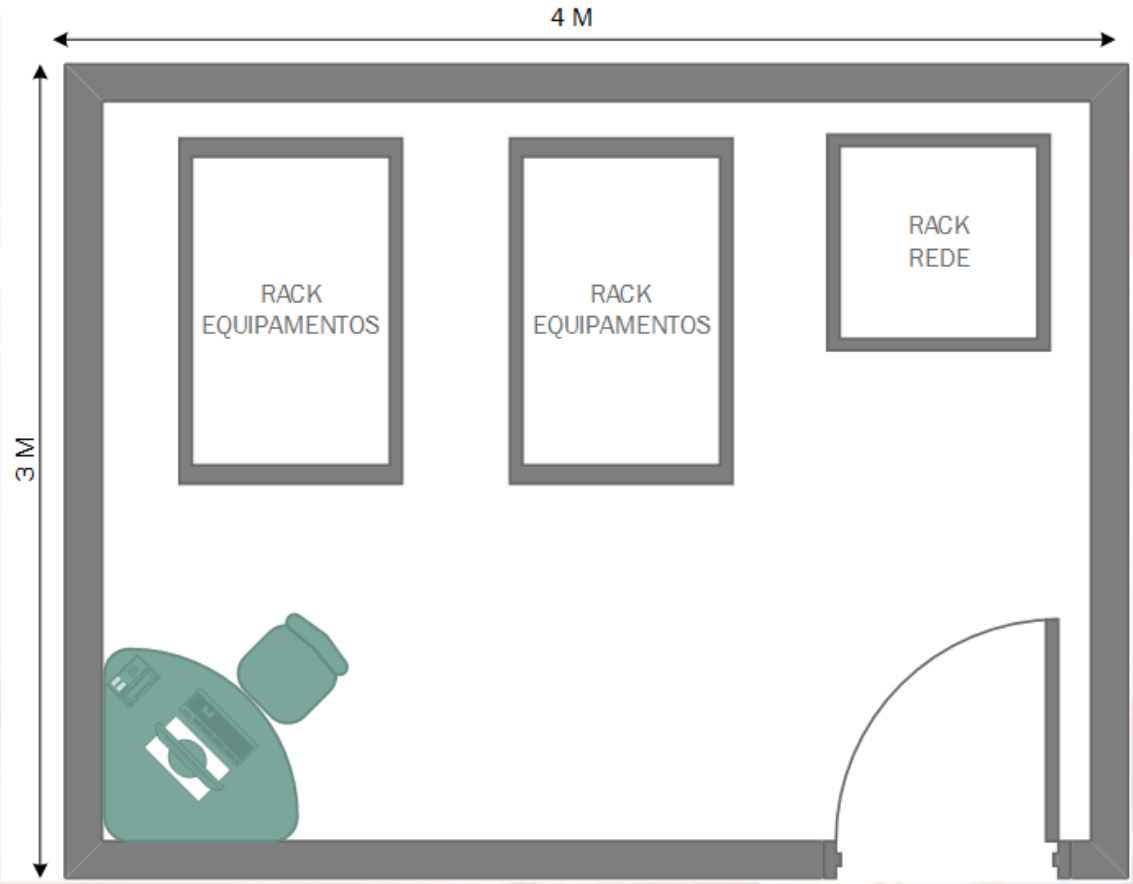


***Figura 3c**: Sala de Equipamentos.*

Desafios

Na implantação da Telefonia IP e rede de dados do SAMU, o IDF precisa do máximo de atenção para a energia e resfriamento. Com um consumo de 500 a 4.000 W, dependendo da arquitetura da rede e switch usado, a definição da tomada adequada, o consumo de energia com o disjuntor correto para os equipamentos de rede, Nobreak e PDUs em uma sala de Telecom é um desafio. O resfriamento e circulação do ar são geralmente um problema maior que não pode ser ignorado nesses ambientes.

Melhores Práticas

Todos os equipamentos no IDF devem ser protegidos por um Nobreak. A configuração do Nobreak é baseada em:

- Total de energia necessária em Watts;
- Autonomia necessária em minutos;
- Nível de redundância ou tolerância a falha desejada;
- Tensões e tomadas necessárias.

O Nobreak é dimensionado pela soma do consumo em Watt das cargas. Um Nobreak montado em rack como o da (Figura 4a) fornecerá aproximadamente quatro noves (99,99%) de disponibilidade de energia, enquanto um com redundância N+1 e by-pass embutido, como o da (Figura 4b), com uma hora de autonomia fornecerá aproximadamente cinco noves (99,999%), suficiente para a maior parte das aplicações.

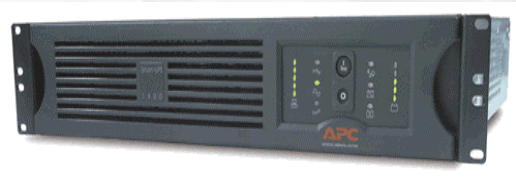


Figura 4a *– APC Smart-UPS.*

Figura 4b *– APC Symmetra RM.*

Nobreaks estão disponíveis com pacotes de baterias que fornecem diferentes tempos de autonomia. Os modelos apresentados nas Figuras 4a e 4b possuem pacotes de bateria opcionais, que podem ser usados para aumentar o tempo de autonomia para até 24 horas.

Mais altos níveis de disponibilidade, como seis ou sete noves, podem ser necessários para algumas aplicações críticas, tais como o SAMU. Tais requisitos podem ser atendidos com o uso de redundância de switches com fontes e cabos de alimentação duplos, Nobreaks redundantes, e arquiteturas elétricas concorrentes com gerador para backup. A empresa responsável pelo serviço deve avaliar essa disponibilidade e recomendar as infraestruturas com alta disponibilidade de energia para tais redes críticas.

Finalmente, identificar os plugs e tomadas necessárias para todos os equipamentos, incluindo o Nobreak da sala de telecom. O ideal é que todos os equipamentos estejam conectados diretamente no painel traseiro do Nobreak ou do transformador, devendo ser evitado o uso de réguas de tomadas adicionais ou PDUs para montagem em rack. Entretanto se existirem muitos equipamentos isso pode não ser prático e um PDU em Rack deve ser usado. Nesse caso, deve ser usado um PDU desenvolvido especificamente para esse propósito. O PDU deve possuir tomadas suficientes para conectar todos os equipamentos usados com algumas tomadas de reserva para necessidades futuras. Prefira usar PDUs com um medidor do consumo de energia, já que eles reduzem erros humanos, como sobrecarga acidental resultando em queda da carga.

Para a seleção correta do modelo de Nobreak apropriado, atingindo o nível de energia, redundância, tensão e autonomia necessárias, o processo é simplificado ao usar um seletor de Nobreaks, como o seletor de Nobreaks da APC em http://www.apcc.com/template/size/apc/. Este sistema disponibiliza dados atualizados de consumo de energia para os switches, servidores e dispositivos de armazenamento mais usados no mercado, evitando a necessidade de coletar esses dados. Em sistemas como este, a escolha de configurar um Nobreak vai fornecer várias opções de tomadas.

Para assegurar uma operação contínua dos equipamentos na sala de Telecom sem qualquer interrupção, as questões de resfriamento devem ser identificadas e consideradas. A dissipação de energia na sala deve ser calculada para decidir a melhor maneira com custo adequado para resolver o problema (veja Tabela 1). É importante observar que os equipamentos envolvidos podem ter um alto consumo de energia, entretanto isso não significa que eles consomem toda essa energia na sala. Por exemplo, os servidores podem drenar 1.800 W, mas podem estar consumindo apenas de 200 a 500 W na sala. A energia restante está sendo fornecida através da rede aos vários Telefones IP espalhados, e consumida por toda a área do complexo regulador do SAMU.

Item	Dados Necessários	Cálculo da Dissip. de Saída	Subtotal da Dissip. de Saída
Switches sem energia In-Line, outros equipamentos de TI (exceto unidades de energia externas)	Soma da energia de entrada em Watts	Mesma que o total da carga de energia de TI em watts	_____ Watts
Switches PoE	Energia de entrada em Watts	0.6 x energia de entrada	_____ Watts
Unidades de energia externas Servidores, Storages, gateways	Energia de entrada em Watts	0.6 x energia de entrada	_____ Watts
Iluminação	Energia de entrada da iluminação permanente ligada em Watts	Taxa de energia	_____ Watts
	Taxa de energia no (não a carga) em Watts	0.09 x taxa de energia do Nobreak	_____ Watts
Total	Subtotais acima	Soma dos subtotais acima	_____ Watts

Tabela 1 *– Tabela de cálculo da dissipação de calor num rack de Telefonia IP*

Uma vez que a energia dissipada na sala de Telecom seja calculada, siga o guia descrito na Tabela 2.

Carga de Calor Total no Rack	Condição	Análise	Ação
< 100 W	O prédio possui um ambiente uniformemente	A condução pelas paredes e a infiltração de ar será suficiente.	Nenhuma.
< 100 W	O prédio possui um espaço hostil, sem sistema de ar-condicionado.	O ar de fora da sala não pode ser considerado seguro para uso devido à temperatura ou contaminação.	Instale um condicionador de ar de precisão na sala e próximo aos Equipamentos.
100 – 500W	Existe sistema de ar-condicionado no forro falso (aéreo). O prédio possui um ambiente uniformemente condicionado.	O ar será suficiente se encaminhado para a sala, mas a porta pode bloquear o fluxo de ar. Traga o ar para dentro da sala pela porta e faça a exaustão para o retorno do condicionador de ar.	Coloque uma grelha de retorno para exaustão no teto da sala e uma grelha na parte inferior da porta da sala.

100 – 500W	Rack sem acesso a qualquer sistema HVAC O prédio possui um ambiente uniformemente condicionado.	O ar será suficiente se drenado para a sala, mas a porta pode bloquear o fluxo de ar. Traga o ar para dentro da sala pela parte inferior e a exaustão por cima da porta.	Coloque uma grelha de retorno para exaustão no topo e uma grelha para entrada de ar na parte inferior da porta da sala.
500 – 1000W	Existe sistema de ar-condicionado no forro falso (aéreo). O prédio possui um ambiente uniformemente condicionado.	O ar será suficiente se encaminhado para a sala, mas a porta pode bloquear o fluxo de ar. E um funcionamento contínuo de um ventilador é necessário e não confiável.	Coloque uma grelha com ventilação forçada para o retorno de exaustão no topo e uma abertura na parte inferior da porta da sala.
500 – 1000W	Rack sem acesso a qualquer sistema HVAC O prédio possui um ambiente uniformemente	O ar será suficiente se drenado continuamente para a sala, porém não há como captar o ar.	Coloque uma grelha com ventilação forçada para o retorno de exaustão no topo e uma abertura na parte inferior da porta da
> 1000W	Existe sistema de ar-condicionado no forro falso (aéreo) e está acessível. O prédio possui um ambiente uniformemente condicionado.	O ar será suficiente se drenado continua e diretamente através dos equipamentos e não houver ar quente da exaustão recirculando para a parte frontal dos equipamentos.	Coloque os equipamentos em um rack fechado com sistema de exaustão de ar quente e uma abertura na parte inferior da porta da sala.
> 1000W	Sem acesso a qualquer sistema de ar-condicionado. O prédio possui um ambiente uniformemente condicionado.	O movimento do ar através da porta não é suficiente. É necessário resfriamento local da exaustão de ar quente dos equipamentos.	Instale um condicionador de ar de precisão na sala e próximo aos equipamentos.

Tabela 2 – *Guia de soluções de resfriamento para salas de Telecom VoIP*

Por fim, o monitoramento ambiental (temperatura e umidade) para essas salas de Telecom é altamente recomendado, já que ajudarão na indicação de condições anormais, permitindo um tempo suficiente para tomar medidas proativas e evitar o tempo de parada dos equipamentos.

Diante de cálculos previamente realizados e quantidade de equipamentos da estruturação da NCPI, rede de telefonia e dados, servidores de telefonia IP e outros equipamentos chegamos

facilmente a uma carga maior que 1000W de potência, porém não excedendo os 10KW. Podemos classificar esse datacenter como de pequeno porte diante da carga de TI apresentada. Então devemos seguir a última orientação da tabela 2 em amarelo para a refrigeração do ambiente.

Refrigeração

A TC 9.9 da Sociedade Americana de Engenheiros de Aquecimento, Refrigeração e Ar-Condicionado (ASHRAE) publica as temperaturas de operação recomendadas e permitidas para equipamentos de TI. A intenção é fornecer uma melhor orientação para assegurar a confiabilidade e desempenho dos equipamentos, maximizando a eficiência do sistema de refrigeração. Esses valores das *Diretrizes Térmicas da ASHRAE* de 2011 para equipamentos classe 1 são fornecidos na **Tabela 3.**

Temperatura de operação	Faixa de Temperatura
Recomendada	**(18-27°C)**
Permitida	**(15-32°C)**

Tabela 3 – *Norma TC 9.9 da ASHRAE limites de temperatura de operação*

Energia

A alimentação para pequenos data centers consiste em um nobreak e a distribuição de energia. Os sistemas de nobreak para esta aplicação são geralmente de linha interativa para cargas de até 5 kVA e de dupla conversão para cargas acima de 5 kVA. Os sistemas de nobreak maiores que aproximadamente 6 kVA geralmente estão conectados fisicamente a partir de um painel elétrico. Orientações técnicas e definições sobre carga serão explanadas em sequência. Para o complexo regulador a proposta é de um nobreak online de dupla conversão de 6kVA.

Existem dois métodos básicos para distribuição desta energia:

1. Conectar os equipamentos de TI nas tomadas na parte traseira do nobreak.
2. Conectar os equipamentos de TI a um rack de distribuição de energia (PDU de rack), o qual é conectado ao nobreak. Este método requer que os equipamentos de TI sejam montados em um rack 19".

Quando utilizado com um rack, o gerenciamento de cabos de energia é mais fácil e mais organizado com PDUs de racks, uma vez que os cabos de energia não têm que se cruzar, conforme mostrado na **Figura 5.** Outra vantagem é que a parte traseira do rack permanece livre de cabos

de alimentação, o que melhora o fluxo de ar da frente para trás para a refrigeração dos equipamentos de TI. Nos casos em que o gerenciamento remoto das saídas é necessário, algumas PDUs de racks possuem medidores e saídas chaveadas que podem ser usadas para reinicializar remotamente os servidores.

Figura 5 *- Organização com PDU*

Sistemas de nobreak redundantes são recomendados para equipamentos críticos com dois cabos, tais como servidores, storages e networks. Certifique-se de que os cabos de alimentação redundantes estejam ligados a um nobreak ou a uma PDU de rack separados. A confiabilidade aumenta se cada nobreak estiver conectado a um circuito separado, onde cada circuito é alimentado a partir do seu próprio disjuntor. Recomenda-se os sistemas de nobreak com uma placa web de gerenciamento de rede integrada, pois permitem monitoramento remoto de nobreaks críticos, tais como carga baixa da bateria, bateria ruim, operação por bateria, sobrecarga, baixo tempo de execução, etc. Alarmes podem ser enviados por e-mail ou por um sistema de gerenciamento de rede NMS.

A mesma placa de gerenciamento pode ser utilizada para fornecer monitoramento ambiental. O ideal é que seja instalado pelo menos um sensor de temperatura do ar para controlar a temperatura de suprimento de ar na parte frontal do rack ou equipamento de TI. Sensores adicionais incluem um sensor único que mede tanto a temperatura quanto a umidade.

Nos casos em que a entrada na sala de servidores é necessária, um sensor de E/S de contato seco vai notificar os administradores quando a porta da sala do servidor for aberta. Outros sensores de contato seco incluem detecção de água. A **Figura 6** mostra um exemplo de um nobreak com estas características.

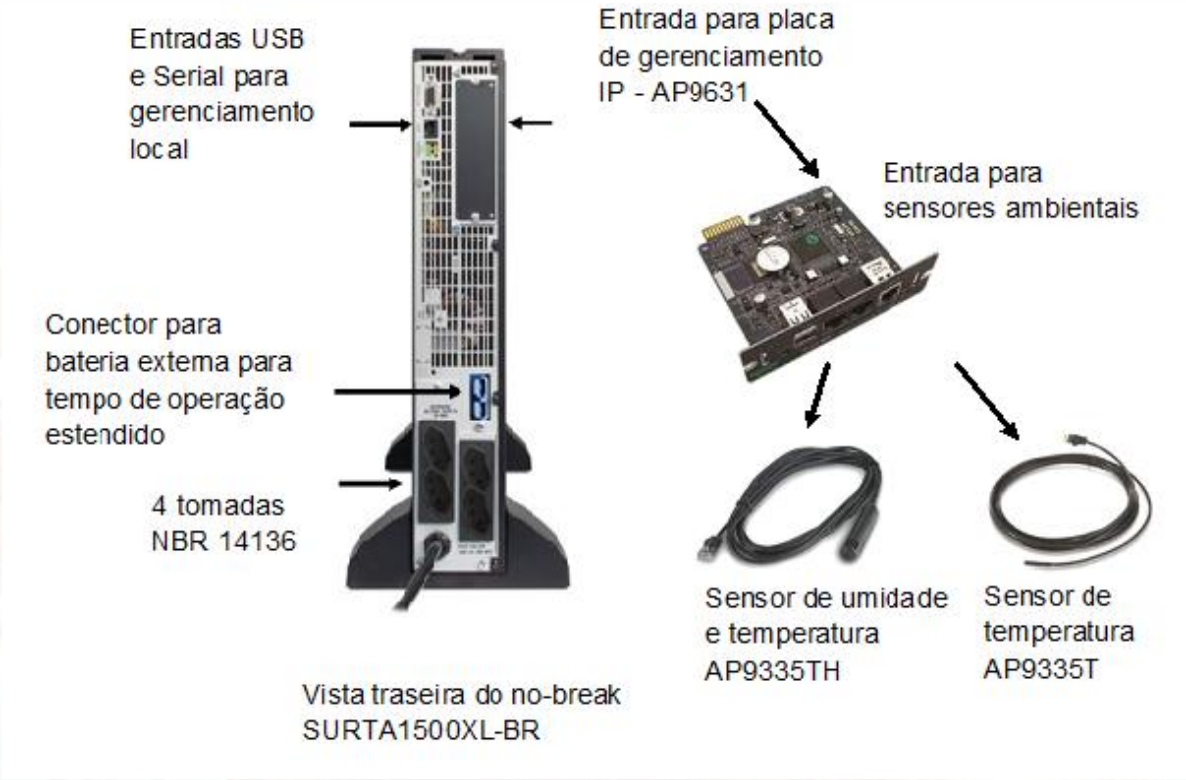


Figura 06 - *Nobreak tomadas padrão NBR 14136*

Segurança Física

Pessoas são essenciais às operações de TI, ainda que estudos mostrem consistentemente que pessoas são diretamente responsáveis por muito do tempo de inatividade, seja por acidentes ou por enganos — procedimentos inapropriados, equipamentos rotulados erroneamente, queda de substâncias e outros imprevistos.

Trancar uma sala de servidores ou gabinete de rack é fundamental caso o custo da paralisação for alto. Se um espaço de TI é considerado crítico, é recomendada a aplicação de câmeras de segurança. Algumas câmeras possuem sensores de ambiente integrados e portas

adicionais para vários tipos de sensores, incluindo contatos secos, detectores de fumaça, detectores de fluidos e interruptores da porta. Os sensores integrados deverão incluir detecção de temperatura, umidade e movimento.

Câmeras com detectores de movimento podem detectar e registrar movimentos automaticamente, permitindo que um registro visual seja combinado com um alerta de acesso ou ambiental, o que agiliza a análise da causa principal. Por exemplo, um administrador de TI pode ser alertado via SMS ou e-mail sobre o acesso por pessoas não autorizadas, através do interruptor da porta ou detecção de movimento. Câmeras irão permitir o acesso via smartphone para a exibição de imagens e dados do ambiente.

Figura 07 *– Câmera com visão noturna e gravação remota com detecção de movimento.*

Segundo a norma ANSI/TIA-942 a topologia do Data Center fica assim classificada:

- ***Entrace Room*** **(ER):** espaço de interconexão do cabeamento estruturado do Data Center e o cabeamento proveniente da telecomunicação.
- ***Main Distribution Area*** **(MDA):** local onde se encontra a conexão central do Data Center e de onde se distribui o cabeamento estruturado, incluindo roteadores e *backbone*.
- ***Horizontal Distribution Area*** **(HDA):** área utilizada para conexão com a área de equipamentos, incluindo o *cross conect* horizontal, equipamentos intermediários, LAN (*Local area network*), SAN (*Storage Area Networks*) e KVM (*Keyboard, Video, Mouse*) switches.
- ***Zone Distribution Area*** **(ZDA):** ponto de interconexão opcional do cabeamento horizontal. Fica entre HDA e o EDA, provê flexibilidade no Data Center.
- ***Equipment Distribution Area*** **(EDA):** área destinada para os equipamentos terminais (servidores, *storages*, unidades de fita), inclui também os *Racks*, gabinetes e equipamentos de comunicação de dados ou voz.

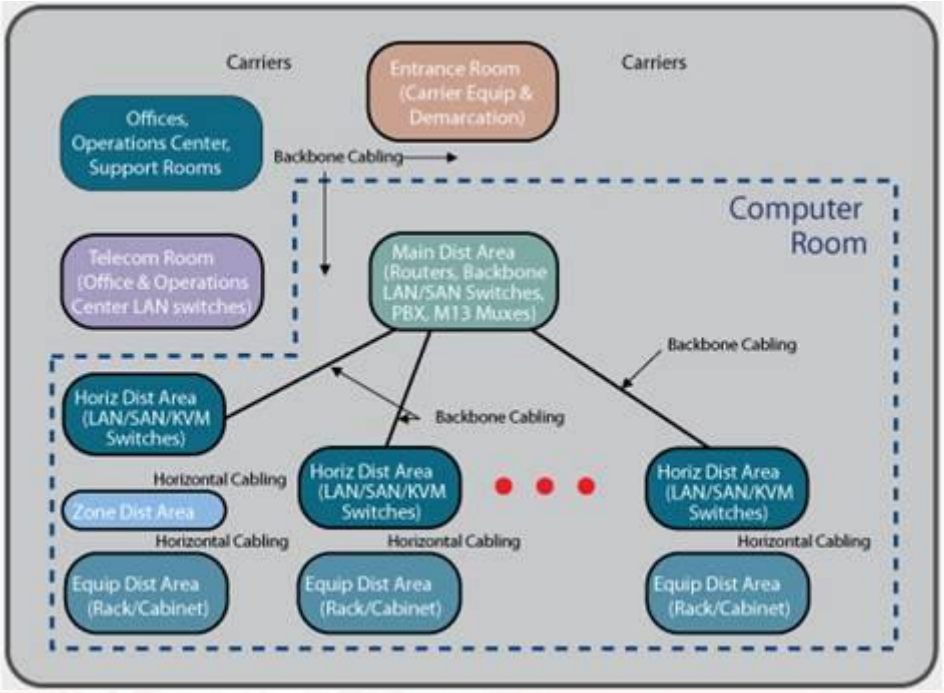


Figura 08 - *Diagrama Básico de um Data Center.*

Obedecendo a norma e suas classificações de disponibilidade de serviço temos um pequeno Data Center Tier 2 de carga de até 6kVA.

Tier 2 – Componentes Redundantes

De acordo com a Furukawa, no Tier 2 os equipamentos de telecomunicações do Data Center e os equipamentos da operadora de telecomunicação, assim como os comutadores LAN-SAN, devem ter os seus módulos redundantes. O cabeamento do *backbone* principal LAN e SAN das áreas de distribuição para os comutadores devem ter cabeamento redundante, par metálico ou fibra.

Devem ter duas caixas de acesso de telecomunicação e dois caminhos de entrada até a ER com no mínimo 20 metros.

No Tier 2 é necessário prover módulos UPS (*Uninterruptible Power Supply*) redundantes para N+1 e um sistema de gerador elétrico para suprir a carga, não é necessária redundância na entrada do serviço de distribuição de energia. O sistema de ar-condicionado deve ser projetado para ter o funcionamento contínuo de 24x7x365, com no mínimo a redundância de N+1.

Os possíveis pontos de falha dessa classificação são:

- Falhas no sistema de refrigeração ou de energia podem ocasionar falhas nos outros componentes do Data Center.

O Tier 2 possui uma disponibilidade de 99.749%, pode ter um *downtime* de 22 horas/ano e redundância parcial em energia e refrigeração. Em face de limitações estruturais das unidades e ou prédios onde os complexos reguladores do SAMU são implantados, uma classificação Tier 3 ou 4 se torna impossível ou muito onerosa.

MDF - Main Distribution Frame (Ambiente de Distribuição principal)

O MDF também é chamado de salas MERs (main equipment rooms – salas de equipamentos principais) ou POP (point of ping or presence – ponto de ping ou presença). Ele incorpora os equipamentos de Telefonia IP mais críticos, como roteadores da camada 3, switches e uma variedade de outros equipamentos de telecomunicações, TI e rede (Figura 9). As linhas E1 e conectividade IP de provedores, normalmente chegam no MDF e fornecem conectividade à espinha dorsal da internet e ao STFC (sistema de telefonia fixa comutada).

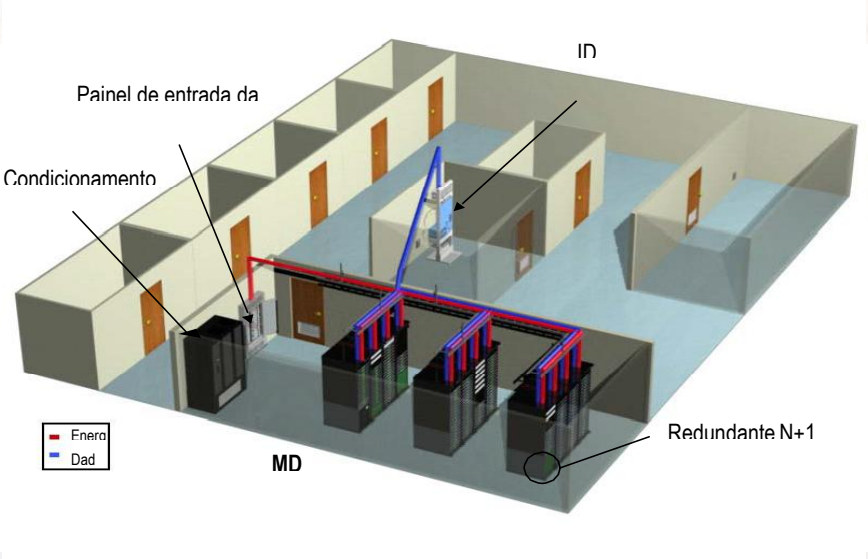


Figura 09 – *MDF.*

Ambiente

Os MDFs geralmente estão localizados no térreo ou primeiro andar, fornecendo a entrada de serviços do prédio. Um MDF típico pode ter de 4 a 12 racks de equipamentos e consumir de 4 kW a 40 kW de energia monofásica ou trifásica. Alguns equipamentos podem necessitar de energia –48VCC. A maioria dos racks em MDFs são abertos, usados para montar uma grande variedade de equipamentos de TI e Telefonia IP. Estes equipamentos podem ter diferentes padrões de ventilação; lado a lado, de frente para trás, etc., e podem ser de 19" ou 23". Entretanto, a maioria dos equipamentos de TI e Telefonia IP são de montagem em rack de 19".

Desafios

Alguns MDFs não tem um nobreak, muitos não têm tempo de autonomia adequado e muitas vezes podem não ter um sistema de ar refrigerado de precisão.

Melhores Práticas

Já que esses MDFs contém uma variedade de equipamentos de rede e telefonia IP críticos, eles devem ser tratados como um pequeno Data Center ou Sala de Servidores. Para obter aproximadamente cinco noves de disponibilidade de energia, um MDF deveria ser protegido por um Nobreak redundante e modular com by-pass interno e ao menos com trinta minutos de autonomia. Maiores autonomias e altos níveis de disponibilidade, como seis ou sete noves, podem ser alcançados com o uso de switches redundantes com fontes duplas, Nobreak redundante, e arquiteturas elétricas projetadas de modo concorrente e com gerador.

Os MDFs devem ter suas próprias unidades de condicionamento de ar de precisão com monitoramento ambiental. Unidades de condicionamento de ar redundantes, deveriam ser consideradas para aplicações críticas que necessitem de alta disponibilidade. Para racks com alta densidade de energia (> 3 kW/Rack), unidades adicionais de remoção e distribuição de ar devem ser usadas para evitar pontos quentes. Diferente de dispositivos de armazenamento e servidores, muitos switches têm o fluxo de ar lado a lado. Isso cria situações especiais numa instalação em um ambiente que usa racks anexos. Situação similar ao posicionamento dos racks adotados no croqui exemplo figura 3c.

Data Center ou Sala de Servidores

No Data Center ou Sala de Servidores (Figura 10) estão todos os servidores de aplicação para telefonia IP com seu software (Asterisk, Bilhetagem, BD etc.). Além disso, baseado na arquitetura de rede e no tamanho da organização, ele pode também armazenar os switches centrais (camada 3) e switches de distribuição (camada 2). Dependendo do seu tamanho (pequeno, médio ou grande), um Data Center ou Sala de Servidores pode conter de dezenas a centenas de racks, carregados com dezenas ou centenas de servidores e uma variedade de sistemas de computação e rede de TI rodando aplicações de negócios críticas como ERP, CRM, Firewalls e outros serviços Web.

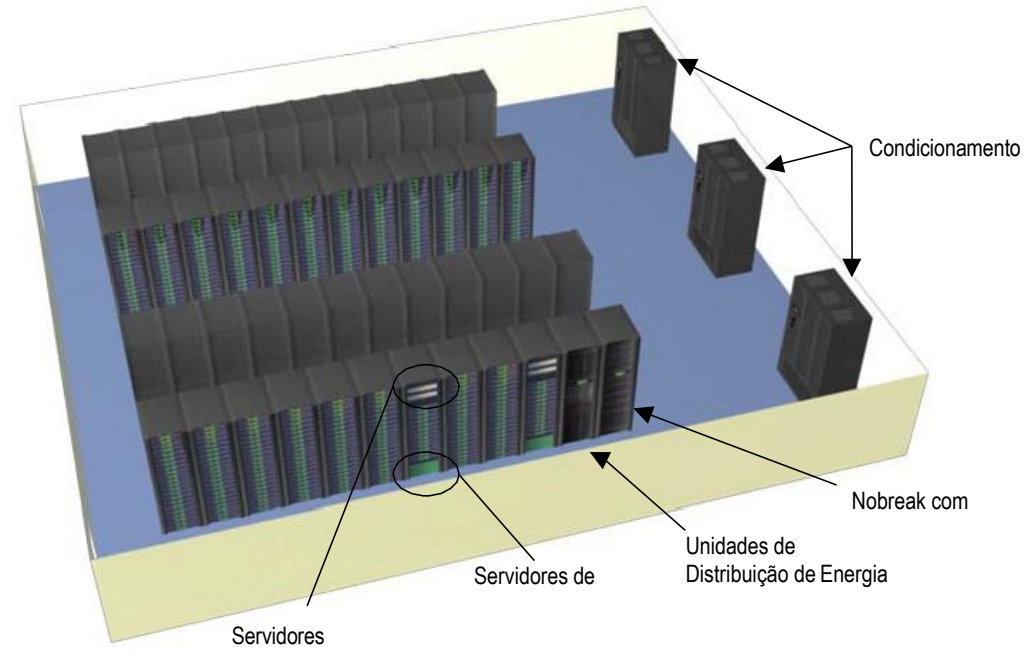


Figura 10 *– Data Center ou sala de servidores típico.*

Ambiente

Os Data Centers estão geralmente localizados no escritório corporativo drenando de 10 kW de energia monofásica ou trifásica a centenas de kilowatts de energia trifásica. Pode haver alguns pequenos requisitos de energia DC –48V para algumas cargas de telecomunicações, mas predominantemente todas as cargas serão de energia AC. A maioria dos Data Centers tem um Nobreak com bateria, gerador e unidades de condicionador de ar de precisão.

Desafios

Switches e servidores de Telefonia IP são basicamente carga incremental incidental ao Data Center, que podem exigir uma autonomia, redundância e disponibilidade maiores que outros equipamentos de rede e TI.

Melhores Práticas

Embora o Data Center possa ter seu próprio Nobreak ou gerador, muitas vezes pode ser apropriado implementar um Nobreak redundante separado com maior tempo de autonomia para o equipamento de Telefonia IP. O correto é identificar e agrupar os equipamentos de Telefonia IP que necessitem uma autonomia e uma disponibilidade maior em uma área separada, em racks separados dentro do Data Center. Após isso, é recomendado um Nobreak dedicado com uma

autonomia maior e uma disponibilidade N+1, N+2, conforme necessário. O conceito de "Disponibilidade Alvo" ajuda a aumentar a disponibilidade dos equipamentos críticos de telefonia IP para os negócios sem incorrer num gasto enorme de capital para o Data Center inteiro. Altos níveis de redundância como alimentações duplas, geradores redundantes e Nobreaks redundantes N+1 com caminhos de energia redundantes até o servidor e outros equipamentos críticos no rack podem ser considerados para redes e Data Centers com elevado nível de disponibilidade.

Deve ser assegurado, que o equipamento de ar-condicionado de precisão do Data Center tenha capacidade de resfriamento suficiente para a nova Central de Telefonia IP adicional. Unidades de condicionamento de ar redundante podem ser consideradas para maiores disponibilidades. Para racks de alta densidade (> 3kW/Rack), unidades de remoção de ar e distribuição de ar adicionais deveriam ser usadas para evitar pontos quentes. Erros que podem ser evitados e são cometidos rotineiramente ao instalar sistemas de resfriamento e racks em Data Centers ou salas de rede comprometem a disponibilidade e aumentam os custos.

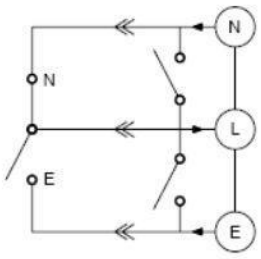
Considerações Finais

Na execução da implantação da estrutura tecnológica do complexo regulador do SAMU, tanto as normas para a NCPI quanto para o Data Center Tier 2, se misturam e se complementam em conceito e definições operacionais. Como a realidade das instalações físicas não permitem a plena implementação de tudo que foi exposto em projeto, é comum e aceitável que todos os layers da NCPI, como também a topologia da ANSI/TIA-942, se misturem em uma única sala, porém respeitando todas as diretrizes aqui esplanadas e definidas. O apêndice 1 fornece as devidas orientações como a configuração da alimentação concessionária, gerador e UPS devem estar dispostos a fim de garantir alimentação contínua às cargas de missão crítica (central de telefonia IP e sistemas de apoio) do complexo regulador.

Apêndice 1

É importante notar que, para as aplicações de suprimento de energia para cargas críticas, a Chave de Transferência Automática (ATS) deve ser dotada de by-pass com a finalidade de não comprometer a disponibilidade do sistema nos casos de manutenção ou reparo no quadro de transferência do grupo gerador **(figura 11).**

Preferencialmente, deve ser do tipo extraível, permitindo remoção e instalação rápidas, sem interrupção no suprimento de energia. Este item tem sido motivo de falhas que acarretaram paralisações prolongadas em muitas instalações, em consequência de servir como elemento de interrupção das fontes principal e de emergência.



N = Fonte principal (rede)

L = Carga

E = Emergência (gerador)

Figura 11 *– ATS com by-pass.*

As unidades UPS referenciadas como componentes de sistemas de energia segura, para os efeitos deste projeto, são as unidades padrão, de dupla conversão disponíveis no mercado, com a configuração básica a seguir. As opções de potências e características construtivas são ilimitadas. Cada fabricante pode disponibilizar modelos e configurações conforme suas conveniências e interesses do usuário final. (Figura 12).

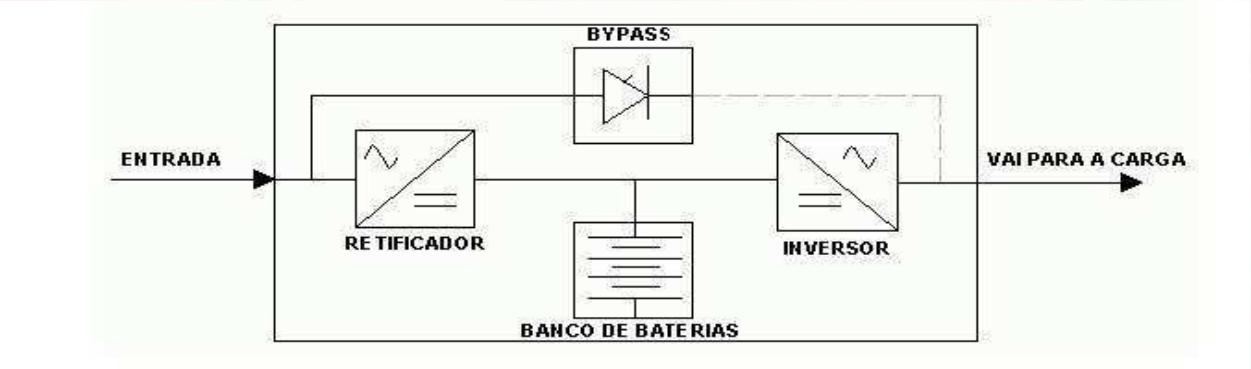


Figura 12 *- UPS CONFIGURAÇÃO PADRÃO.*

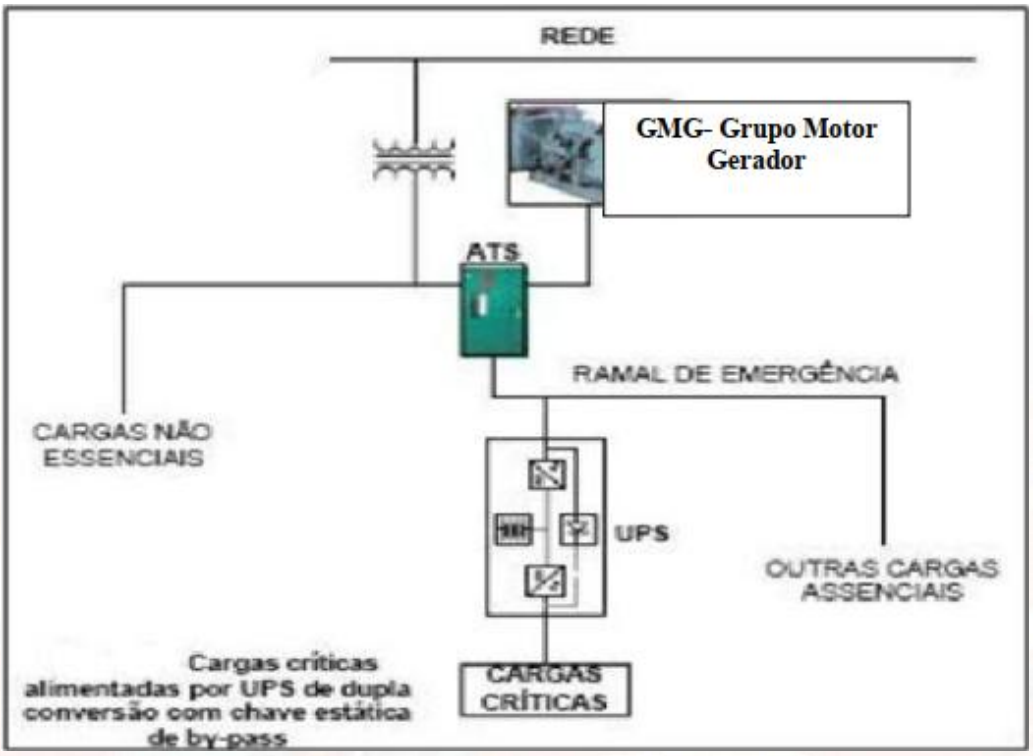


Figura 13 - *Conceito básico de suprimento de energia para cargas críticas*

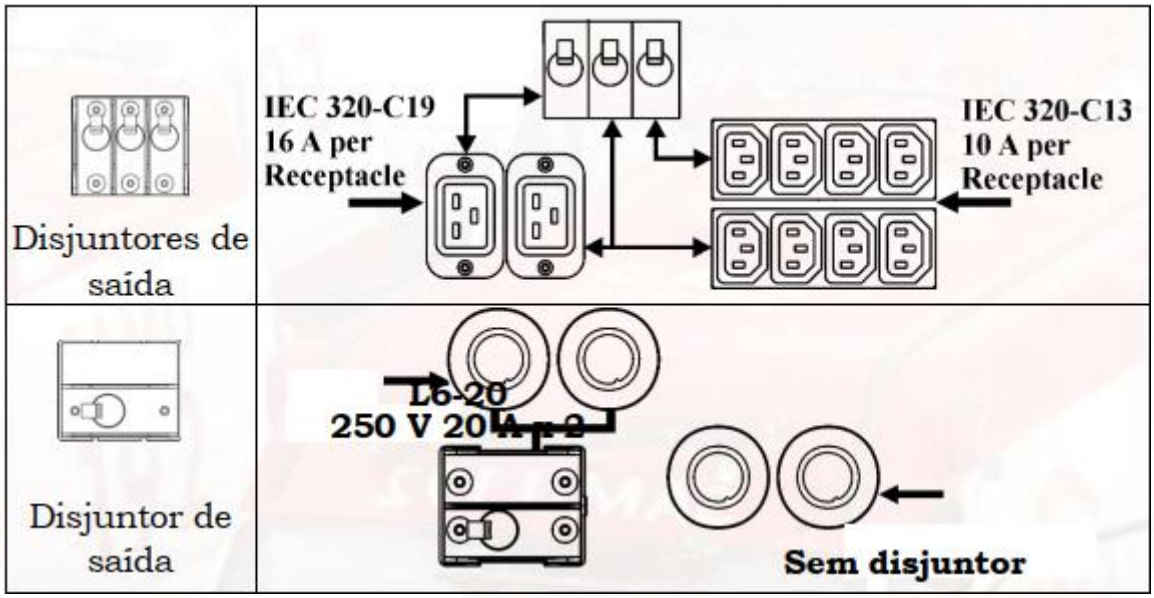
Atendendo aos dispositivos gerais de instalação do nobreak selecionado segundo o manual, temos:

Entrada

INSTRUÇÕES SOBRE CABEAMENTO:

- Cabeamento deve ser feito por um eletricista qualificado.
- Instale um disjuntor magnético de alta proteção de 30/32 A.
- Siga todas as normas e códigos de eletricidade nacionais e locais. NBR 5410
- Use cabo de bitola 10 AWG (5 mm²).

Saída



Aterramento Geral

A norma que rege este dimensionamento é a NBR-5410:2004. Deve ser seguida na confecção, teste e/ou aceitação do aterramento para implantação do projeto.

1.1.4. Segmentação da rede

Por questões de segurança, otimização da operação e resolução de problemas atendendo aos requisitos para uma NCPI, a rede foi dividida em 3 layers distintos, atendendo as disposições das normas descritas.

Como veia da informação, a rede, deve trafegar a mesma de forma segura, livre, sem gargalos e com o desempenho máximo permitido, garantindo a todos os componentes de sua estrutura de acesso rápido e sem perdas aos dados e a qualquer momento, 24 horas por dia, 365 dias no ano. Para permitir essa sustentabilidade, agilidade e confiabilidade sendo transparente as aplicações e se tornando altamente gerida por seus administradores, a rede deve seguir alguns conceitos.

Deve ser constituída por um sistema de cabos, fibras ou acesso sem fio que siga as normas IEEE 802.3 (última atualização 802.3-2022) (http://en.wikipedia.org/wiki/IEEE_802.3) e seus padrões subsequentes e as normas IEEE 802.1 (http://en.wikipedia.org/wiki/IEEE_802.1) e seus padrões subsequentes.

Sendo que para o padrão IEEE 802.3 que define o layer físico da rede, layer de link de dados, MAC de uma rede cabeada ethernet, temos um padrão equivalente ANSI/TIA/EIA.

O padrão de conexão física mais adotado e popularmente conhecido é o CAT 5E

(EIA/TIA-568-B) o qual deverá ser adotado em toda a confecção da infraestrutura, para se ter uma rede padronizada e normatizada podendo alcançar a velocidade de 100 Mbps como estabelece a norma para o padrão. Mas podendo ela atingir velocidade de até 1 Gbps, obedecendo os padrões IEEE 802.3ab para Gigabit Ethernet sobre rede de cabos de par trançado CAT 5, 5e e 6.

Deve seguir a topologia estrela ou malha e respeitar as normatizações para o protocolo TCP/ IP ver 4.0, além de ter suporte ao protocolo TCP/IP versão 6 que será usado no futuro, suporte ao protocolo de gestão de rede SNMP (Simple Network Management Protocol), suporte a QoS e Vlan e deve permitir aos gestores o controle de acesso de equipamentos a rede por MAC, IP ou regras semelhantes.

Todas essas características compõem o principal elemento de uma rede, a Switch LAYER 2 em algumas topologias mais simples e/ou Switches LAYER 3 em diante com topologias mais complexas.

A Switch é o elemento interligador da rede e une os elementos ativos em uma estrutura hierárquica, controlada e organizada seguindo o modelo OSI (Modelo de Sistema Aberto de Interconexão), subdividido em 7 níveis ou layers.

Os outros elementos como cabos, conectores e patch panels seguem a orientação do padrão ANSI/TIA/EIA 568-B e suas normativas correlatas para aterramento e estruturação do ambiente.

A justificativa para segmentação de rede é clara. Quando tratamos de um ambiente totalmente organizado e gerenciado, deparamos com dois conceitos bem distintos. A organização lógica: definição dos IPs, estrutura da árvore de diretórios, definição da lista de acesso e permissões, definição dos compartilhamentos, políticas de segurança, permissões de usuários, entre outros. A organização física: disposição dos equipamentos e dispositivos na rede, parametrização física dos Servidores e Firewalls que darão suporte a toda infraestrutura, definição do hardware de abrigo dos servidores, definição dos sistemas energéticos e de refrigeração entre outros.

Para que nosso objetivo não fique distanciado e para que possamos ter sucesso nessas colocações, faremos aqui algumas considerações pertinentes a esse desenvolvimento, porém dando abertura para que o executor do projeto escolha entre tantas opções, as que melhor se enquadrem em sua realidade. Vale lembrar que alguns pontos comuns devem ser respeitados e adotados para que o ambiente fique o mais próximo possível do que é aplicado hoje em dia.

1.1.4.1 Telefonia/ Suporte (NCPI)

Os IPS na rede Telefonia/ Suporte (NCPI) são os endereços de identificação de cada

equipamento de forma individual e servem para estabelecer um vínculo universal entre todos os elementos. Responsáveis também pela organização, seguem as definições do protocolo TCP/IP que diferente do OSI possui apenas 5 camadas.

Uma rede bem definida, deve ter a designação de seus IPS em uma tabela de acordo com o tamanho da rede e com a perspectiva de crescimento futuro. Então baseado no projeto, definimos uma rede com máscara /24 de 256 IPS distintos classe A, sendo servida pelo gateway router principal, através de protocolo DHCP. Esta rede alimentará todos os elementos principais da infraestrutura da NCPI Telefonia/Suporte, sendo eles, todos os telefones IP, servidores, gateways de comunicação, Storages de armazenamento, e etc., irá operar na Vlan 01 (Vlan default de rede) e será exclusiva ao funcionamento desse serviço, ficando isolada das outras redes. Abaixo segue exemplo de endereçamento:

FAIXA DE IP 10.0.1.0 MÁSCARA DE REDE 255.255.255.0 GW PADRÃO OU IP DO SERVIDOR 10.0.1.1.

1.1.4.2 Regulação (NCPI)

Os IPS na rede Regulação (NCPI) são os endereços de identificação de cada equipamento de forma individual e servem para estabelecer um vínculo universal entre todos os elementos. Responsáveis também pela organização, seguem as definições do protocolo TCP/IP que diferente do OSI possui apenas 5 camadas.

Uma rede bem definida, deve ter a designação de seus IPS em uma tabela de acordo com o tamanho da rede e com a perspectiva de crescimento futuro. Então baseado no projeto, definimos uma rede com máscara /24 de 256 IPS distintos classe C sendo servida pelo Firewall Regulação através de protocolo DHCP com endereçamento estático. Esta rede alimentará todos os elementos principais da infraestrutura da NCPI Regulação, sendo eles, todos os computadores e/ou elementos de apoio na regulação do SAMU, como servidores de softwares específicos, painéis de informação e etc., irá operar na Vlan 888 (Vlan específica de rede) e será exclusiva ao funcionamento desse serviço, ficando isolada das outras redes. Abaixo segue exemplo de endereçamento

FAIXA DE IP 192.168.1.0 MÁSCARA DE REDE 255.255.255.0 GW PADRÃO OU IP DO SERVIDOR 192.168.1.1

1.1.4.3. Administrativo

Os IPS na rede Administrativo são os endereços de identificação de cada equipamento de forma individual e servem para estabelecer um vínculo universal entre todos os elementos. Responsáveis também pela organização, seguem as definições do protocolo TCP/IP que diferente do OSI possui apenas 5 camadas.

Uma rede bem definida, deve ter a designação de seus IPS em uma tabela de acordo com o tamanho da rede e com a perspectiva de crescimento futuro. Então baseado no

projeto, definimos uma rede com máscara /24 de 256 IPS distintos classe C sendo servida pelo Firewall Administrativo através de protocolo DHCP com endereçamento estático. Esta rede alimentará todos os elementos principais da infraestrutura da rede Administrativo, sendo eles, todos os computadores e/ou elementos de apoio como servidores de softwares específicos, impressoras, servidores de compartilhamento, ERP, CRM e etc., irá operar na Vlan 889 (Vlan específica de rede) e será exclusiva ao funcionamento desse serviço, ficando isolada das outras redes. Abaixo segue modelo de endereçamento

FAIXA DE IP 192.168.2.0 MÁSCARA DE REDE 255.255.255.0 GW PADRÃO OU IP DO SERVIDOR 192.168.2.1.

Por se tratar de uma rede onde uma gama maior de serviços e sistemas irão funcionar, mesmo estes não sendo considerados críticos ao complexo regulador, cabe aqui uma atenção para alguns pontos de definição explanados abaixo:

1.1.4.4. Definições da Rede

COMPARTILHAMENTOS

Deve ser definido sob uma plataforma servidora, que será adotada no controle da rede e seus usuários para esse fim. No ambiente pode-se defini-lo com o uso do Windows Server 2022 x64 virtualizado, que nativamente possui suporte a todos esses recursos. Caso seja opção o uso do Linux como gestor, o serviço SAMBA poderá ser usado para compartilhamentos compatíveis com Windows e o NFS como compartilhamento nativo Linux. O compartilhamento de arquivos é uma prática comum nas redes administrativas e deve ser realizado com moderação e somente pelos gestores da infraestrutura. Compartilhamentos mal executados com permissões de acesso erradas, podem ocasionar vazamento de informações sigilosas da administração.

DOMÍNIO INTERNO

Deve ser definido em cima da plataforma servidora que será adotada no controle da rede e seus usuários para esse fim. No ambiente pode-se defini-lo com o uso do Windows Server 2022 x64 virtualizado, que nativamente possui suporte a todos esses recursos. O domínio interno é uma opção, mas que obrigatoriamente não precisa ser implantada. Muito usado caso a gestão opte pela implantação de um Diretório Ativo, no controle de acesso às máquinas administrativas do complexo regulador.

SERVIDOR DHCP

O servidor DHCP nessa rede Administrativa ficou a cargo do Firewall UTM, que será configurado para controle total da planta. Todas as requisições de IP e acesso a rede passam por ele. Mecanismos de controle serão aplicados para impedir o acesso indevido à rede.

SERVIDOR DE IMPRESSÃO

Deve ser definido em cima da plataforma servidora que será adotada no controle da rede e seus usuários para esse fim. No ambiente pode-se defini-lo com o uso do Windows Server 2022 x64 virtualizado, que nativamente possui suporte a todos esses recursos. Os servidores de impressão podem também ser substituídos pela combinação de uso dos recursos das impressoras em rede. Caso a impressora possua esse recurso, pode-se instalá-la exclusivamente para um ou outro departamento renunciando ao uso do servidor. Cabe a ressalva que, o uso de servidores de impressão melhora a gestão desse tipo de recurso e o monitoramento do uso e dos gastos é mais eficiente.

1.1.5. Segurança/Firewall

As políticas de segurança e bloqueio de acesso a conteúdo não permitido, bem como a proteção da integridade dos dados e sistemas são tarefas do Firewall. Um sistema de Firewall bem elaborado, juntamente com regras de utilização e controle bem definidas, permite ao gestor de TI e consequentemente ao SAMU, uma operação sem sustos. Livrando a rede de ataques e contaminações pelas diversas pragas eletrônicas, vírus, cavalos de Tróia, worms e outros.

O Firewall atualmente, não é somente uma ferramenta de defesa, mas sim uma arma de controle e gestão complexa, agregando diversos recursos como controle ativo de banda, relatórios de uso de recurso de rede, acesso diferenciado por classificação de usuário, balanceamento de links e demais funções usadas para uma ampla atuação na administração e controle do ambiente de TI. Seguindo essa tendência e aplicando as mais novas tecnologias de Firewall, será necessária uma solução virtualizada, sendo possível a adoção de diversas distribuições LINUX preparadas para este fim. Algumas sugestões vão desde soluções livres como IPCOP ou PFsense, até soluções comerciais de baixo custo de aquisição como Untangle e Sophos UTM.

As definições para implantação dessa tecnologia de segurança são baseadas no conceito de Firewall de Nova Geração (Next Generation Firewall - NGFW). Tanto o firewall da rede da Regulação (NCPI) e do Administrativo serão virtualizados e trabalharão em domínios broadcast diferentes separados por suas respectivas VLANS no atendimento aos seus clientes. A interfaces LAN às quais alimentam as redes internas estarão conectadas a switches camada três com tagueamento de pacotes para distinção das VLANS. As interfaces WAN dos dois firewalls serão alimentadas pelo router/ gateway principal que se encontra na rede Telefonia/ Suporte (NCPI).

Dessa maneira teremos uma tripla camada de segurança e gerência individual de cada rede. A virtualização da solução de segurança garante amplitude de recursos e opção de escolha, já que se pode trocar de soluções sem ter que desfazer do investimento em hardware.

1.1.6. Virtualização

O projeto de estruturação do ambiente de TI tem como premissa a virtualização de Servidores de Serviços e de Firewalls. A virtualização é hoje a principal ferramenta de desenvolvimento e implantação de novas estruturas. Permitindo fazer mais com menos e gerando uma economia significativa de energia, temos na virtualização o futuro de toda planta de TI.

Além de permitir mobilidade de seus ativos, segurança aprimorada e facilidade na manipulação dos recursos, a virtualização garante a total redundância de suas operações, uma vez que podemos mover qualquer servidor virtual entre os hospedeiros e manter o funcionamento da estrutura, já que as cópias de segurança são clones idênticos das máquinas em operação. Um servidor de virtualização permite o aumento dos recursos na rede, como mais servidores e aplicações virtuais sem aumentar ou adquirir hardware físico. Em muitos é possível uma relação de até 7 máquinas virtualizadas por núcleo de processador. Ficando o limite apenas na quantidade de memória RAM e disco da máquina hospedeira.

No mercado existem duas soluções líderes e concorrentes que atendem de forma satisfatória as necessidades de uma virtualização. Citrix Xen Server e VMware ESXi compõem a melhor relação custo-benefício se comparadas a tecnologias semelhantes. Suas soluções são livres de licença, gratuitas para uso em pequenos e médios empreendimentos.

Para virtualização, a definição dos parâmetros técnicos do Servidor hospedeiro deve ser realizada com cautela e entendimento. Listas de compatibilidade de hardware (HCLs) e outros requisitos dos softwares de virtualização, devem ser respeitados e seguidos. A máquina hospedeira ou Servidor Principal deve ter recursos de hardware suficientes para funcionar com uma folga mínima de 50% de sua capacidade, mantendo uma margem de segurança na operação. Deve ter recursos de redundância de disco e fonte para garantia de integridade dos dados das máquinas virtuais, possuir ferramentas embarcadas de gestão remota via console ou acesso a rede independente do compartilhado com os usuários. Esse acesso deve contemplar segurança e criptografia permitindo ao gestor acessar e diagnosticar qualquer eventual problema em sua estrutura.

O servidor de virtualização deverá permitir a criação de no mínimo 3 máquinas virtuais, sendo que duas delas deverão ter 4GB de RAM, duas interfaces de rede, 80 GB de disco e separação física entre as interfaces além de suporte a tag vlan. Essas máquinas serão os firewalls aqui citados. A terceira máquina deverá ter 4GB de RAM e 120 GB de disco para abrigar um servidor de serviço e suporte para gestão interna das redes.

A utilização da virtualização de servidores traz alguns benefícios para o projeto, dentre eles:

- Redução de downtime: Eliminação de paradas de ambiente de produção; Prevenção de perda de dados; Prevenção de downtimes não planejados.

- Automação e gerenciamento: Sistemas de gerenciamento centralizado de máquinas virtuais com interface amigável e intuitiva; Gerenciamento de ambiente de produção e homologação; Gerenciamento de implantação; Gerenciamento de atualização de versões de softwares e firmwares.
- Otimização da Infraestrutura: Pesquisas apontam que a utilização de servidores convencionais é em torno de 5 – 20%, através da virtualização essa taxa fica em torno de 65% - 90%; Maior ROI; Redução de até 40% de custo operacional; Com Virtualização de Servidores é obtido menor TCO de servidores; Melhor Gerenciamento; Otimização de infraestrutura, espaço físico e maximização da utilização de recursos; Redundância em caso de falha de Hardware, Virtualização de Servidores, o ambiente virtualizado migra as máquinas virtuais para os demais servidores virtualizados.

Todas as referências técnicas de projeto, podem ser consultadas nos sites dos criadores dos softwares de virtualização, bem como para consulta e comparação, podem ser obtidas através do endereço eletrônico. https://www.whatmatrix.com/comparison/Virtualization.

1.1.7. Integração

Umas das ferramentas de grande importância quando falamos de integração, é a possibilidade de unificar a comunicação com outras centrais de outros SAMUs. Essa integração tem a missão de permitir de forma transparente a comunicação entre elas, via rede segura e assim permitir a criação de uma rede universal de atendimento e colaboração.

A integração cria a rede de abrangência necessária e permite aos gestores de saúde uma comunicação direta com os complexos reguladores via rede privada de comunicação e torna possível a elaboração de arranjos operacionais amplos em caso de gestão de catástrofes. Um exemplo prático, uma determinada região do estado foi atingida por um fenômeno natural meteorológico e não possui mais comunicação telefônica. Neste ponto, a gestão central pode rearranjar outras centrais reguladoras em uma única operação conjunta integrada via rede segura e obter a gestão coordenada das ações. Para isso deve-se usar como ferramenta de integração, o protocolo de rede virtual privada baseado em openssl (openvpn) definido, gerido e configurado via hardware router/gateway de borda que se encontra na gestão da rede de Telefonia/Suporte (NCPI). A escolha do openvpn se dá pelas seguintes razões técnicas:

- Pode-se criar túnel de qualquer sub-rede IP ou adaptador Ethernet virtual através de uma única porta UDP ou TCP;
- Configurar um farm escalável, com balanceamento de carga VPN, servidor usando uma ou mais máquinas que podem lidar com milhares de ligações dinâmicas de clientes VPN de entrada.
- Usar todos os recursos de criptografia, autenticação e certificação da biblioteca OpenSSL para proteger o tráfego de rede privada, uma vez que transita pela internet.
- Usar qualquer cifra, tamanho da chave, ou HMAC digest (para verificação de integridade de datagrama) suportado pela biblioteca OpenSSL,

- Escolher entre criptografia convencional baseada em chave estática ou criptografia de chave pública baseada em certificado.
- Usar, chaves pré-compartilhadas estáticas ou troca de chave dinâmica baseada em TLS.
- Usar compressão adaptativa em tempo real de link e traffic shaping para gerir utilização de banda em link.
- Criar redes de túneis cujos terminais públicos são dinâmicos, como DHCP ou dial-in clientes.
- Criar redes de túneis através de firewalls stateful orientados a conexão sem ter que usar regras de firewall explícitas.
- Criar redes de túneis através de NAT.
- Criar pontes Ethernet seguras usando adaptadores virtuais (dispositivos TAP).
- Ter controle de OpenVPN usando uma GUI no Windows ou Mac OS X ou Linux.

1.2 CENTRAL TELEFÔNICA

1.2.1. Objetivo

Implantação e configuração de Central Telefônica IP (Internet Protocol) de alta disponibilidade baseado em PBX IP na plataforma ASTERISK. A opção por um sistema de telefonia baseado na plataforma ASTERISK justifica-se por ser um programa de código aberto que funciona no sistema operacional Linux, o que o torna flexível à medida que permite a sua constante evolução por profissionais de software livre, além de oferecer várias ferramentas livres.

O ASTERISK é um software que oferece vários recursos de comunicação e garante a expansão futura do sistema, sem a necessidade de troca da central de telefonia, podendo-se apenas efetuar a inclusão de novos ramais e configurá-los ao sistema, sem a necessidade de se obter novas licenças de software, para cada novo ramal disponibilizado. A tecnologia inclui funcionalidades avançadas de comunicações e, também, proporciona uma significativa liberdade, além da escalabilidade e robustez.

Além de todas essas vantagens, existe hoje no mercado várias empresas que prestam serviços utilizando esta plataforma, tornando assim a concorrência e a prestação de serviço bem mais ampla do que um sistema proprietário, além de uma vasta documentação disponível na internet, o que permite a capacitação de equipes multidisciplinares, permitindo o PCN - Plano de Continuidade do Negócio em conformidade com a ISO 22301.

1.2.2. O SISTEMA PBX IP

O termo PBX vem do inglês 'Private Branch Exchange' que significa a troca automática de ramais privados. Com a evolução tecnológica, os sistemas passaram a operar em plataformas de rede através do protocolo IP, pois todo o processo passou a ser controlado por sistemas operacionais e softwares, cuja o principal objetivo, era romper as barreiras da comunicação através das redes de dados ou da Internet. A partir deste princípio, as antigas centrais de comutação, ou

melhor, o PBX, evoluiu com o objetivo de utilizar essa rede, para integrar matriz e filiais com o menor custo. A plataforma de sistema PBX IP deve permitir o controle e o processamento da capacidade máxima de terminais SIP, gateways e troncos analógicos, digitais e GSM, conforme especificação e dimensionamento de hardware para o servidor.

O sistema PBX IP deverá ser capaz de realizar a bilhetagem total prevista no sistema; solução desenvolvida em SIP nativamente, denominado PBX IP, em conformidade com a RFC 3261 (Especificações do SIP: Session Initiation Protocol); realização de adaptação de protocolos para controle das chamadas SIP; possuir disponibilidade de uso de terminais SIP e gateways de qualquer fabricante, desde que suportem e atendam a RFC 3261; deve possuir estrutura de rede baseada em IP (Internet Protocol), TCP (Transmission Control Protocol) e UDP (User Datagram Protocol); utilização de sistemas de backup para recuperação da base de dados quando necessário, visando gestão de continuidade; o sistema PBX IP deve atuar como SIP Proxy Server e SIP Register Server, possibilitando o registro de ramais IP e gateways, além de controle do roteamento de chamadas de qualquer entidade SIP; suporte a gateways analógicos ATA utilizando protocolo SIP; suporte a sistemas de contingência para sinalização de troncos E1 de voz (RDSI/ISDN e R2); suporte a protocolos IAX 2, H.323, MGCP (Media Gateway Control Protocol), SCCP (Skinny Client Control Protocol); solução independente dos modelos dos dispositivos de rede, ou seja, garante as mesmas funcionalidades independente do fabricante dos ativos de rede, desde que a infraestrutura existente ofereça recursos mínimos de controle de qualidade de serviços - QoS (banda, jitter, delay e perda de pacotes); suporte a integrações com serviços de rede DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System), e NTP (Network Time Protocol); possibilidade de integração de múltiplos servidores para distribuição de carga, configuração de alta disponibilidade em dois servidores PBX IP, processamento e roteamento de voz entre localidades geográficas distintas; utilização de sistema operacional Open Source Linux.

Além dos requisitos básicos conforme parágrafo anterior, o sistema deverá conter gerenciamento completo do PBX IP em produção via Web, inclusive de novos servidores ASTERISK, através de plataforma única; Deverá ser implantada uma única plataforma WEB (Centralizada) capaz de gerenciar, alterar e configurar todo o servidor ASTERISK implantado dentro da rede do SAMU, permitindo a criação ou exclusão de ramais e a emissão de relatórios de tarifação centralizada; Disponibilidade de visualização completa do estado momentâneo (status) dos ramais mediante login e senha; Relógio de tempo real a fim de se manter o horário correto para serviços de despertador, hora certa, e bilhetagem; Numeração dos ramais programáveis para qualquer número; Proteção de programação: uso de memória flash; Siga-me interno e externo; Transferência e estacionamento das chamadas; Captura de chamadas de

grupo de captura ou ramal especifico; Desvio de chamadas não atendidas/ocupadas; Estacionamento de ligações; Chamada em espera; Limitador de duração de chamadas; Grupos de ramais; Voicemail (Correio de voz no e-mail e/ou telefone); Salas de Conferência; Codecs: G.711 fatores μ e A, G.729, G.722, ilbc, GSM; Habilitação de senha de utilização por usuário, possibilitando

a utilização de qualquer ramal interno e externo mediante utilização de senha pessoal; Identificador de chamadas (BINA – Sinalizações ISDN/R2 Digital); Supervisão de Chamadas / Monitoração de ramais (Escuta oculta sigilosa); Segmentação de Grupo de Chamadas (Local / DDD/ DDI/ Celular); Programação de DAC (Distribuidor Automático de Chamadas); Criação de agentes em filas de atendimento; Programação de Recebimento/Bloqueio de Chamadas Simultâneas; Capacidade de gerar relatório das chamadas efetuadas e recebidas; Gravação de Prompts (arquivos) personalizados de voz; Armazenamento de Informações em Banco de Dados baseado em Software Livre; DDR - Discagem Direta a Ramal; Linha executiva; Identificador de chamadas DTMF/FSK incorporado; Chamada de emergência; Música de espera (uma fonte externa e uma interna configuráveis); Blacklist (lista negra); Plano de numeração flexível; Acionamento externo; Transferência; Hora certa; Não perturbe; Hotline (interna e externa); Senha para os ramais; Cadeado; Bloqueio de ligações locais, DDD, DDI e celular; Bloqueio de ligações a cobrar; URA – Unidade de Resposta Audível com no mínimo 7 níveis/subníveis de atendimento; Gestão estratégica de condição de tempo (Time Condition); Agenda coletiva; Agenda individual; Soluções CTI; Rechamada interna; Rechamada externa; Chefe-secretária; Serviço noturno; Retenção de chamadas; Rota de menor custo; Seleção automática de linhas; Interface Ethernet; Ligações telefônicas IP (VoIP); Identificação e supressão do número chamador; Permitir integração da central de telefonia com aplicativos SIP disponibilizados em dispositivos móveis (smartphone, tablets); Toques distintos para chamadas internas e externas; restrição de chamadas de saída por código de acesso, com registro no bilhete; restrição de chamadas de saída por classes de serviço; rediscagem do último número de entrada e saída; auto provisionamento de dispositivos com ATA e Telefone IP.

O PBX IP deverá gerar sinalização para integração com dispositivos externos como ATA, Telefone IP, Softphone, Gateways e Aplicações, de forma a manter uma característica multiplataforma, utilizando assim recursos avançados destes dispositivos, permitindo o maior aproveitamento da tecnologia no processo de integração. Através do processo de sinalização, a plataforma deverá: Disponibilizar sinalização para diferenciação audível de novas chamadas enquanto usuário está com chamada ativa; Sinalização de segunda chamada para ramais ocupados; Sinalização avançada para atraso no toque de chamada, sem interferir na indicação visual; Sinalização para desvio de chamadas incondicional e em caso de ocupado, não atendimento, usuário inacessível; Sinalização para desvio de chamada com base no número chamador, horário e condições; Aplicação e Sinalização para desvio de chamadas para números diferentes, definidos para chamadas internas ou externas e conforme condição; Aplicação e Sinalização de chamadas para o correio de voz com indicação de mensagem (MWI – Message-Waiting Indicator); Aplicação e Sinalização avançada para ativação/desativação remota de desvios; Aplicação e Sinalização de ativação remota do desvio de chamadas incondicional; Sinalização para tratamento simultâneo de múltiplas chamadas; Sinalização para transferências de chamadas entre telefonistas; Sinalização para visualização do número chamador no visor do aparelho telefônico SIP; Sinalização para visualização do número do ramal chamador em aplicativo na estação de trabalho associada a ramal ATA através de CTI.

Além do processo de sinalização e aplicações internas, que são inerentes ao plano de discagem, a solução de PBX IP, como aplicações complementares e fundamentais para o provimento do serviço, deverá prover: Aplicação com disponibilidade de anúncio com número do ramal utilizado, para identificação do mesmo; Aplicação com Possibilidade de rechamada em caso de ocupado e não atendimento; Aplicação de sinalização do status das linhas; Aplicação avançada de reserva de linhas; Aplicação de serviços multilinhas; Aplicação de ativação remota do toque paralelo para busca do usuário; Aplicação de registro em qualquer telefone da rede através de usuário e senha; Aplicação de serviços para mesa de telefonista; Aplicação para acesso direto do chefe para a secretária e secretária para o chefe; Disponibilidade para acesso direto entre chefes; Aplicação avançada de visualização para a secretária com status da linha principal do chefe e de outra secretária; Aplicação de serviços de mobilidade; Aplicação de conferência com até 10 participantes, podendo se estender a partir da configuração do servidor PBX IP; Aplicação de serviço quality call (avaliação de qualidade do atendimento); Aplicação de ouvidoria (reclamações, sugestões); Aplicação de acesso a sala de conferência através de linha compartilhada com outros usuários; Aplicação de gravação de chamada (ramal, fila, número externo); Aplicação de call center (filas de atendimento); Aplicação de unidade de resposta audível (URA) com apresentação de informações por voz digitalizada sem a necessidade de atendentes, tratamento de tons DTMF, e com possibilidade de integração a banco de dados e a WebService externos; Aplicação de envio de mensagens de voz individuais ou campanha em massa para telefonia fixa e móvel, possibilitando ainda inserção de URA para intervenção de agentes de telefonia.

1.2.2.1. Recursos de Bilhetagem

Gerenciamento dos recursos de bilhetagem através dos parâmetros da administração web, no idioma português do Brasil, centralizado no servidor PBX IP; Visualização dos relatórios em português; Operação das estatísticas através das classes em sub menus; Os relatórios gerados podem ser enviados via e-mail ou impressos em qualquer impressora da rede; Processar o agendamento da geração de relatórios possibilitando exportar no formato PDF; Acesso a relatórios em formato CSV para exportação a ferramentas de terceiros; Acesso disponível, a partir de qualquer ponto da rede, a consulta de gráficos e relatórios via web browser e com uso de credenciais de acesso; O processamento e geração de bilhetagem devem ser centralizados no servidor no Cluster PBX IP; Gerenciamento e visualização de relatórios disponíveis para totalizações e sumarizações em vários níveis: por ramal; por tronco; por número discado; por data e hora; por centro de custo; estatística da central; tráfego telefônico, operadora de telefonia fixa ou móvel; Permitir coletar os bilhetes de todos os ramais do sistema de comunicação corporativo via rede IP; Classificar chamadas em local, celular, DDD, celular DDD, a Cobrar, ramal e serviços; Registrar e organizar todos os dados de chamadas de voz que venham a ser obtidos em toda a rede; O registro dos bilhetes deverá ser efetuado através da rede, de forma automática; Somente usuários com devido nível de acesso têm possibilidade e permissão para gerar relatórios; Possibilidade de exportação e integração de relatórios para gestão de custos em softwares de tarifação, não contemplado aqui, trazendo as quantidades de minutos por códigos de área e análise de melhores planos de tarifação.

1.2.2.2. Segurança

Gerenciamento dos mecanismos para segurança da estrutura visando garantir o acesso aos recursos do sistema de telefonia apenas a usuários com permissão garantida. Prever no mínimo as seguintes funcionalidades:

Complexidade de senha de ramais utilizando caracteres especiais; Utilização de senhas para os níveis de acesso e funcionalidades para administração web, dispositivos IP e aplicativos; Proteção contra ataques e serviços de defesa; Monitoramento do tráfego de entrada do sistema; Deve gerar alarmes quando mensagens são descartadas por ataques de negação de serviço (DoS - Denial of Service); Firewall interno: Deve permitir o bloqueio de endereço IP de origem e transferência do mesmo para uma lista negra após ultrapassar limiar pré-definido. Gerenciamento das regras, bloqueios, lista de exceções e tráfego; A política de segurança padrão para gerenciamento deve bloquear todas as portas exceto as portas utilizadas para gerenciamento e operação; Possibilidade de autenticação ou login na aplicação; Segurança em CLI (Command Line Interface): Deve possuir interface segura de Linha de Comando através de SSH (Secure Shell); Deve possuir interface segura de transferência de arquivos através de SFTP (Secure File Transfer Protocol); Possibilidade de upgrade (atualizações) para as devidas implementações de segurança; Disponibilizar no sistema de administração web, acesso com suas devidas restrições por usuário, para definir e/ou customizar seu perfil de uso; Gerenciamento das políticas de senhas e bloqueios para cada ramal pertencente a rede PBX-IP; Disponibilidade de políticas de senhas para acesso a gravações de áudio; Disponibilidade de políticas de senhas para exibição de relatórios gerenciais de telefonia; Disponibilidade de políticas de senhas para acesso ao sistema de Operação telefonista; Disponibilidade de políticas de senhas para acesso para administração web (níveis de acesso e operacionalidades); Permissão e controle gerenciável para acesso remoto de possíveis manutenções e suporte; Prevenção de desastre e plano de recuperação.

1.2.2.3. Conectividade e Roteamento

O sistema deve permitir conexão aos sistemas das concessionárias de serviços de telefonia a partir de protocolos padrão de mercado; conexão com circuito de E1 (R2 e RDSI/ISDN) e Troncos SIP; Suporte a interfaces ISDN PRI e R2; Suporte a interfaces GSM para ligações para a rede celular; Conexões em rede local: Telefonia em redes independentes, telefonia em redes compartilhadas, Suporte para manutenção utilizando acesso remoto;

Integração entre a Unidade do SAMU com as demais unidades dos SAMU localizadas no Estado de Minas Gerais via VoIP; Suporte a roteamento por transbordo, rota de menor custo, origem, destino, horário, dias da semana; Acesso à base atualizada de portabilidade BDR (Base de Dados Nacional de Referência) para serviços de telefonia fixa (STFC) e móvel pessoal (SMP) permitindo definição de roteamento por operadora de destino da chamada; Relatório de operadora de destino das ligações de telefonia fixa e móvel; Rota de acesso de longa distância; Suporte para o roteamento das sessões para o mesmo destino através de diferentes tipos de rotas, como grupo de troncos.

Além disso, em caso de rota indisponível, o transbordo também pode ser direcionado para diferentes tipos de rotas; Monitoramento dos troncos através da disponibilidade das operadoras; Gerenciamento da rota de menor custo para chamadas de longa distância, incluindo eventuais redes de dados, e chamadas celular, sem a necessidade de digitar um código de rota especifico; Gerenciamento das características de roteamento de menor custo (LCR) para os entroncamentos com as operadoras de telefonia através de uma tecla predefinida para as rotas já programadas; Gerenciamento de categorização nos ramais dos sistemas de voz; Gerenciamento dos troncos dos sistemas para interface com as operadoras de telefonia.

1.2.2.4. Recursos de Áudio

Recursos de áudio centralizados no próprio servidor PBX-IP; Suporte aos codecs G.711 e G.729; Utilização de codecs diferenciados para LAN e WAN; Suporte à reprodução de tons e anúncios; Suporte à reprodução de música em espera (MoH); Suporte à geração de tons DTMF; Suporte a recepção e tratamento de tons DTMF; Suporte à geração de anúncios pré-definidos conforme a funcionalidade acessada; Suporte à geração de anúncios relacionados à ativação e desativação de funcionalidades; Suporte, gerenciamento e centralização de recursos de áudio e gravação para chamada em espera, URA e caixa postal através de administrador web; Serviço de caixa postal e fax programado para envio de e-mail para o devido ramal programado; Suporte a gravações de ramais e filas; Suporte de áudio para inserção de arquivos com extensão mp3/wav para a devida operação dos recursos de URA (Unidade de Resposta Audível) e espera telefônica.

1.2.2.5. Padrões de mercado compatíveis com a solução de telefonia IP

RFC 1213: Management Information Base for Network Management of TCP/ IP- based internets: MIB-II (SNMP); RFC 1442: Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2); RFC 1443: Textual Conventions for Version2 of the Simple Network Management Protocol (SNMPv2); RFC 1889: RTP: A Transport Protocol for Real-Time Applications; RFC 1890: RTP Profile for Audio and Video Conferences with Minimal Control; RFC 2131: Dynamic Host Configuration Protocol; RFC 2234: Augmented BNF for Syntax Specifications: ABNF; RFC 2246: The TLS Protocol; RFC 2327: Session Description Protocol(SDP); RFC 2475: An Architecture for Differentiated Services; RFC 2597: Assured Forwarding PHB Group; RFC 2705: Media Gateway Control Protocol (MGCP); RFC 2780: IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers; RFC 2782: DNS SRV; RFC

2806: URLs for Telephone Calls; RFC 2833: RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals; RFC 2848: The PINT Service Protocol: Extensions to SIP and SDP for IP Access to Telephone Call Services; RFC 2865: Remote Authentication Dial In User Service (RADIUS); RFC 2976: SIP INFO Method; RFC 3016: RTP Payload Format forMPEG-4 Audio/Visual Streams; RFC 3047: RTP Payload Format for ITU-T Recommendation G.722.1; RFC 3168: The Addition of Explicit Congestion Notification (ECN) to IP; RFC 3204: MIME Type for ISUP and QSIG; RFC 3260: New

Terminology and Clarifications for Diffserv; RFC 3261: SIP: Session Initiation Protocol; RFC 3262: Reliability of Provisional Responses in SIP; RFC 3263: Session Initiation Protocol (SIP): Locating SIP Servers; RFC 3264: SDP Offer/Answer Model; RFC 3265: SIP-specific Event Notification; RFC 3267: Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs; RFC 3272: Overview and Principles of Internet Traffic Engineering; RFC 3288: Using the Simple Object Access Protocol (SOAP) in Blocks Extensible Exchange Protocol (BEEP); RFC 3311: SIP UPDATE Method; RFC 3323: SIP Privacy Mechanism; RFC 3515: SIP REFER Method; RFC 3605: Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP); RFC 3725: SIP Third Party Call Control; RFC 3761: The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM); RFC 3824: Using E.164 Numbers with SIP; RFC 3830: MIKEY: Multimedia Internet Keying; RFC 3842: SIP Message Waiting; RFC 3892: The Session Initiation Protocol (SIP) Referred-By Mechanism; RFC 3952: Real-time Transport Protocol (RTP) Payload Format for internet Low Bit Rate Codec (iLBC) Speech (SIM); RFC 3959: The Early Session Disposition Type for the Session Initiation Protocol (SIP); RFC 3960: Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP); RFC 4028: Session Timers in SIP; RFC 4049: Binary Time: An Alternate Format for Representing Date and Time in ASN.1; RFC 4235: An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP); RFC 4353: Framework for Conferencing with the Session Initiation Protocol (SIP); RFC 4568: Session Description Protocol (SDP) Security Descriptions for Media Streams; RFC 4575: A Session Initiation Protocol (SIP) Event Package for Conference State;

1.2.2.6. Alta Disponibilidade

Um sistema de Alta Disponibilidade é aquele que visa manter a disponibilidade dos serviços prestados por um sistema computacional replicando serviço e servidores através da redundância de hardware e reconfiguração de software. Adicionando-se mecanismos especializados de detecção, recuperação e mascaramento de falhas, pode-se aumentar a disponibilidade do sistema, de forma que este venha a se enquadrar na classe de Alta Disponibilidade. Nesta classe as máquinas tipicamente apresentam disponibilidade na faixa de 99,99% a 99,999%, podendo ficar indisponíveis por um período de pouco mais de 5 minutos até uma hora em um ano de operação. Nesta classe, se encaixam grande parte das aplicações comerciais de Alta Disponibilidade, como centrais telefônicas;

O seu funcionamento inclui a sincronização dos bancos de dados em ambas as máquinas, e a criação de um endereço IP virtual através do software heartbeat *(solução que monitora o status de dois ou mais nodos (servidores) em um ambiente, em caso de detecção de falha, redireciona o serviço para outro servidor de forma transparente para o usuário/aplicação)*, que aponta para o servidor primário. Em caso de falha dessa máquina, automaticamente o software heartbeat transfere o IP virtual para a máquina secundária, que continuará disponibilizando os serviços.

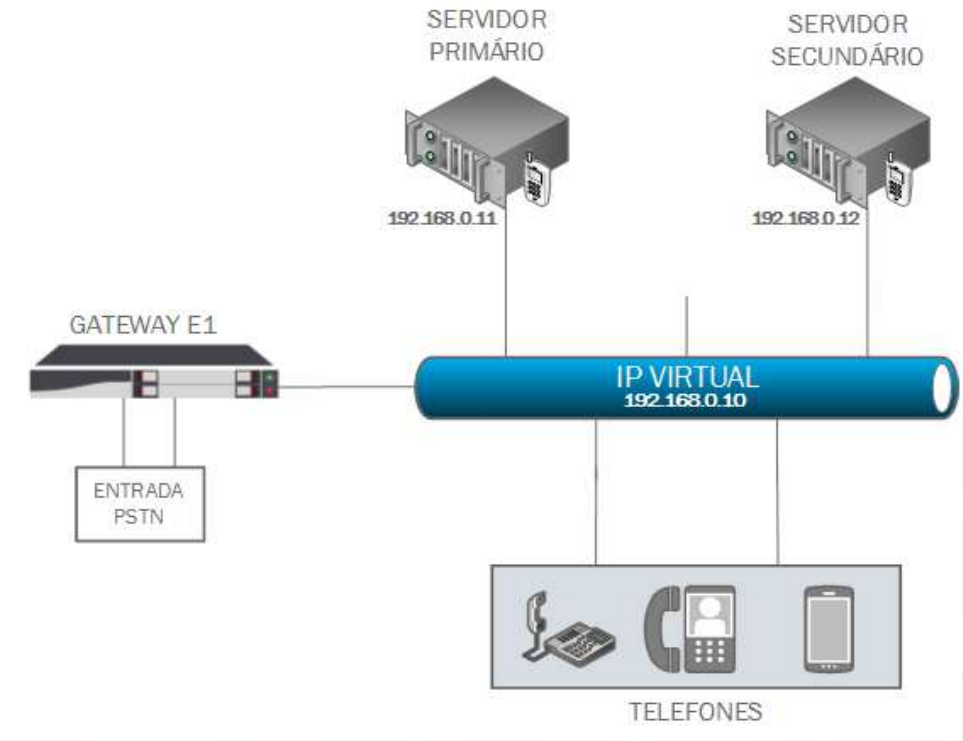


Figura 14 – *Exemplo de alta disponibilidade.*

Outro modelo de alta disponibilidade se dá através do sistema *Multi Master* onde os participantes do Cluster funcionam simultaneamente, executando todas as ações do PBX IP. Com esse cenário, a disponibilidade do ambiente tende a aumentar significativamente, provendo a continuidade do negócio sem pontos de interrupção. Neste caso, a distribuição das chamadas é realizada através de balanceamento de carga, com a utilização do protocolo DNS SRV, especificação da RFC 2782, não sendo necessário a configuração de um IP virtual através de um sistema de heartbeat. Desta forma, o Cluster é alcançado através do registro DNS, onde a pesquisa do host será respondida de acordo com peso e prioridade. Neste caso, os dispositivos Telefone IP, Gateways e ATA deverão ter a capacidade de consulta e comunicação do registro SIP reportado através dos servidores DNS.

O PBX IP deverá apresentar as duas formas de trabalho em alta disponibilidade supracitadas, obedecendo as melhores práticas de mercado, em conformidade com o PCN - Plano de Continuidade de Negócios da ISO 22301.

1.2.2.7. Integração com Sistemas

A plataforma de sistema PBX IP deve permitir integração com outros sistemas via CTI *(Computer Telephony Integration),* que é o processo pelo qual o PBX IP troca informações de uma chamada com um computador, permitindo o computador ou um indivíduo gerenciar melhor a chamada.

As funcionalidades que o PBX IP deve disponibilizar numa integração via CTI são: Exibir no computador as informações da chamada: Número chamador (ANI), número discado (DNIS) e preenchimento da tela no atendimento da chamada; Discagem automática e discagem controlada pelo computador: discagem rápida (fast dial), preview dial e discagem preditiva (predictive dial); Controle do telefone: atender (answer), desligar (hang up), colocar em espera (hold), fazer conferência (conference); notificar trabalho após o término da chamada (after-call work), gerar logs da chamada; Controle do status do atendente, por exemplo, se o trabalho após o término da chamada passar de um tempo determinado, o status do atendente volta para "pronto para tratar chamadas"; Controle de chamadas para monitoramento da qualidade e / ou por softwares de gravação das chamadas.

1.2.2.8. Backup de Dados

Todas as informações presentes no PBX IP tais como as presentes no banco de dados, arquivos de configuração e gravações telefônicas, deverão todas ser salvas em dispositivos de backup (storage), para que haja segurança de armazenamento dos dados. O Storage é um hardware que contém slots para vários discos, ligado aos servidores através de ISCSI, NFS ou fibra ótica, é uma peça altamente redundante e cumpre com louvor a sua missão, que é armazenar os dados com segurança.

O storage pode aceitar diversas conexões de servidores diferentes, ao mesmo tempo. Então a sua matriz RAID, além de segura, ficará altamente portável. A estrutura de backup deverá conter critérios para o sistema de prevenção de desastre, com a finalidade de recuperação do sistema em até 1 hora.

2.2.2.9. Gravações Telefônicas

O sistema de gravação de chamadas incorporado ao PBX IP permite a gravação digital das chamadas e o armazenamento em dispositivos de backup (storage). A gravação das chamadas é essencial para o monitoramento de atendimento, controle de conversas não profissionais, escuta telefônica, gravação de diálogos para procedimentos de segurança, negociações verbais, auditorias, etc.

Características: Permitir configurar a gravação por ramal, fila de atendimento, número de telefone, opção de URA, etc.; Permitir o gerenciamento centralizado das gravações, restrito a usuários previamente autorizados; Possibilitar a programação e recuperação remota das gravações; Possuir filtros de busca por data, hora, duração, ramal, fila de atendimento, número de origem, número de destino; Suportar formatos de gravação como MP3, WAV, GSM, etc.; Gravar simultaneamente as ligações telefônicas de todos os canais; Gravação de linhas e ramais analógicos, digitais, E1; Reprodução de gravações telefônicas em software cliente local ou remoto; Sistema de arquivamento com pastas por canal, data e hora.

2.2.2.10. Aplicativo para Chamadas de Emergência SAMU 192 via VoIP

O sistema de PBX IP deve possuir um aplicativo gratuito compatível com dispositivos Android e iOS, desempenhando um papel crucial: permitir chamadas de emergência para o SAMU 192 via VoIP (Voz sobre IP). Esta capacidade se torna especialmente vital em regiões com cobertura móvel limitada ou durante falhas nas redes de telefonia fixa ou móvel, garantindo um acesso rápido ao serviço de urgência e emergência quando mais necessário.

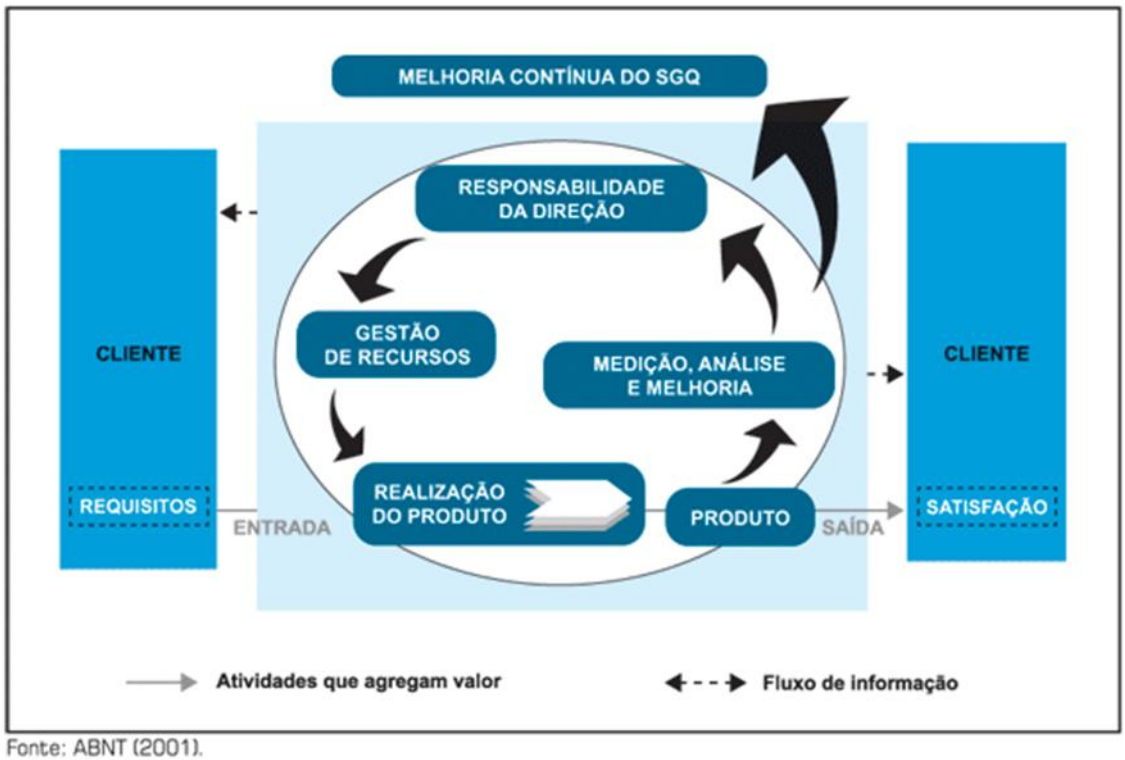
O aplicativo deve oferecer diversas opções para estabelecer comunicação com o SAMU 192, seja através de conexões Wi-Fi ou utilizando os dados da operadora móvel, como o 4G, por exemplo. Além disso, é essencial que os usuários possam cadastrar antecipadamente o município de origem das chamadas de emergência, facilitando um acionamento rápido dos serviços de socorro. Outra funcionalidade importante é o uso do GPS do dispositivo ao iniciar uma chamada. Essa função permite que o aplicativo identifique automaticamente o município de origem, mesmo se o usuário estiver em um local diferente do cadastrado. Essa capacidade é fundamental para direcionar a ligação para a Central de Regulação do SAMU responsável por aquele município específico, garantindo uma resposta mais eficiente e adequada às necessidades do usuário.

Esses recursos são fundamentais, especialmente em áreas remotas ou com cobertura móvel irregular. A capacidade de realizar chamadas de emergência por meio de redes Wi-Fi disponíveis pode ser a diferença entre salvar uma vida ou enfrentar uma situação de risco prolongada e potencialmente fatal. Assim, a incorporação dessas funcionalidades em uma solução de PABX-IP é essencial para garantir a segurança e o bem-estar dos usuários em uma variedade de circunstâncias desafiadoras.

2.3 - SERVIÇOS

2.3.1. Objetivo

Os serviços continuados, tem por propósito a melhoria na qualidade do que é oferecido ao cliente final, como premissa para toda a operação de serviços no complexo regulador do SAMU. Essa atividade tem por fim manter em pleno funcionamento toda a estrutura tecnológica implantada e promover de forma ativa, soluções e melhorias baseadas nas necessidades detectadas. O suporte continuado, o monitoramento de ativos e serviços, bem como a implantação de conectividade de internet, deve seguir as normas básicas de SGQ (Sistema de Gestão da Qualidade), referenciado na ISO:9001:2000. O processo mostrado abaixo classifica essa atuação. O produto oferecido é o serviço em questão e o cliente são as pessoas, processos e diretrizes internas do complexo regulador.



Fonte: ABNT (2001).

Figura 15 – *Atuação do SQG.*

2.3.2. Suporte

O ambiente proposto necessita de suporte técnico especializado no que se referem à infraestrutura da rede de dados, voz, seus dispositivos e periféricos e usuários. O suporte técnico é uma parte indispensável do projeto. Ele deve participar de toda a operação (instalação e homologação do projeto), além de prestar manutenção e assistência pós-implantação, aderindo a um conceito de Melhoria Continuada – processo fundamental para potencializar todas as funcionalidades do produto, identificar possibilidades de melhoramento da ferramenta ou ainda de novas necessidades de expansão do projeto. Para a unidade do SAMU, o suporte técnico também deve ficar responsável pelo monitoramento e assistência técnica de toda a infraestrutura e processos pertinentes ao ambiente do local, incluindo suporte e apoio ao usuário.

2.3.2.1. Predefinições:

- **Central de Serviços**: Ponto Único de Contato, composta por uma equipe responsável por lidar frequentemente com uma variedade de eventos de serviço.
- **Chamados (Ordens de Serviço)**: Requisições de Serviços e/ou Incidentes registrados pelos usuários ou detectados automaticamente pela central de monitoramento de eventos.
- **Tipificação**: Tipificar um chamado significa atribuir a ele uma classificação dentro do escopo de tratamento para incidentes e requisições de serviços declarados, para identificar o tipo exato do evento que está sendo registrado.

- **Requisição de Serviço**: Solicitações que demandem alterações no ambiente, objetivadas a atender uma nova realidade ou necessidade da operação ou negócio, tais como:
    - **Mudança/melhorias no ambiente**: Referem-se às requisições de serviço que venham ser realizadas para melhorar a qualidade dos serviços prestados, bem como implantação de mudanças rotineiras do ambiente;
    - **Condição para a operação do negócio**: Referem-se às requisições de serviço que se não implantadas, inviabilizam ou podem vir a inviabilizar a operação.
- **Incidente**: Todo e qualquer evento que não faz parte da operação normal de um serviço e que cause ou venha causar uma interrupção, ou redução da qualidade de serviço, tais como:
    - **Produção Parada**: Incidente que torna um ou mais serviço(s) indisponível(eis) inviabilizando as operações ou sem desempenhar seu papel previsto;
    - **Produção Impactada**: Incidente que torna um ou mais serviço(s) degradado(s), mas em funcionamento, permitindo a operação.

2.3.2.2. Níveis de suporte

O setor de suporte técnico deve ser dotado de capacidade de atendimento no primeiro nível (Equipe de TI local ou Suporte *In Loco)*, segundo nível (Equipe de Service Desk e especialistas), além do acionamento e acompanhamento do terceiro nível (Especialistas e Analista Sênior). O processo de suporte deve atender a um modelo de atendimento padrão, conforme o fluxograma a seguir:

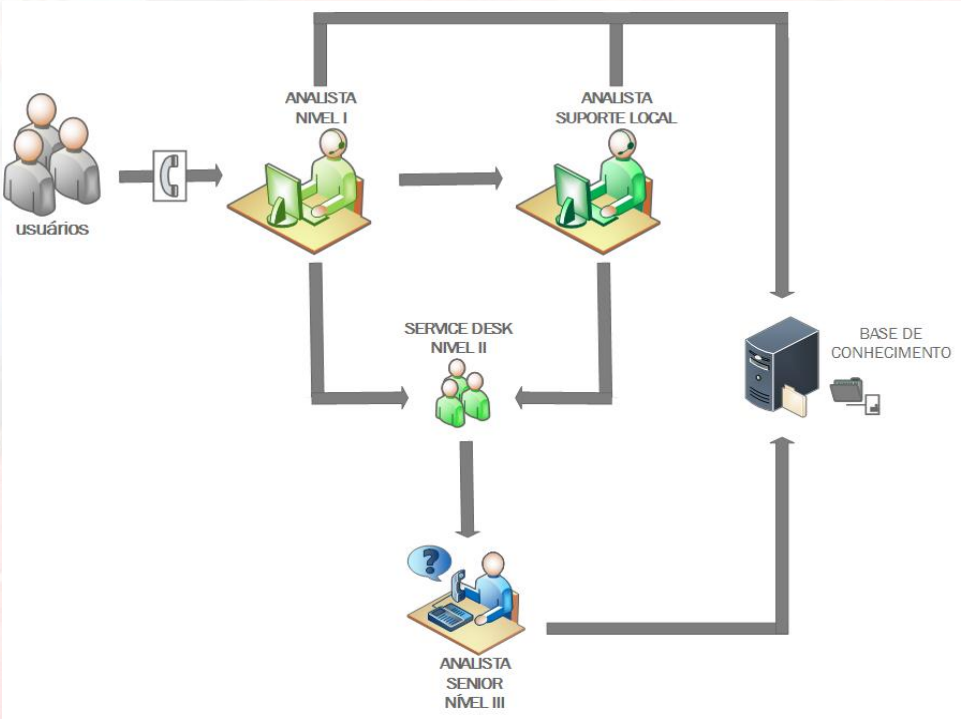


Figura 16 – *Ação dos níveis de Suporte.*

Suporte técnico in loco (primeiro nível) é a prestação de serviços de TI no local em que o problema ocorre ou que se faça necessário um suporte específico. Para o local em questão, ele se faz necessário devido à complexidade da infraestrutura do local, para auxílio na resolução de possíveis incidentes e eventos em relação ao projeto, bem como na assistência técnica, seja intelectual (conhecimentos) ou tecnológica (manutenção: revisões, regulagens, calibrações, reparos/consertos, requisições pertinentes à área, atualizações de software etc.) para todo o ambiente de TI do local, com a finalidade de solucionar problemas técnicos relacionados a produtos e soluções tecnológicas, tais como: redes (dados e voz), telefonia, computadores, softwares e afins. Para atender a Unidade do SAMU, o Suporte in loco deve possuir disponibilidade de 14 horas por dia, em dias úteis, distribuindo a carga horária entre dois técnicos capacitados e, fora deste, a prestadora de serviços deve disponibilizar pessoal capacitado para eventuais demandas de suporte.

O Suporte Especializado (Segundo e terceiro níveis) deste serviço, deve ter por objetivo resolver os eventos de serviço (chamados) da Central de Serviços, sendo eles: Requisições de Serviços e Incidentes provenientes de chamados ou de alertas de ferramentas de monitoramento, devendo ser considerado uma janela de cobertura 24x7 (24 horas por dia, 7 dias por semana). Nesses níveis, se abrangem a identificação, o gerenciamento e a resolução de incidentes ou eventos de maior criticidade e/ou complexidade e que demandem um nível de conhecimento superior acerca dos sistemas e soluções implantadas, além de atender solicitações de nível gerencial.

2.3.2.3. Sistemática para atendimento e prestação de serviços/abertura de chamados/ resolução de incidentes

O Suporte Técnico deve possuir um portal ou ferramenta de Service Desk, além de ramais ou números de telefone dedicados ao atendimento remoto, abertura e documentação de chamados, bem como o feedback das solicitações. O processo de abertura de chamados e resolução de incidentes deve seguir as seguintes premissas:

- **Identificação e Registro de Incidentes:**
  - Os incidentes/eventos devem ser registrados oriundos dos diversos meios disponibilizados, tais como: telefone, e-mail, ferramenta de Service Desk ou registro manual de alarmes de eventos procedentes de ferramentas de monitoramento;
  - Todos os incidentes que ocorrem na infraestrutura e nos serviços devem ser registrados;
  - As informações relevantes para o tratamento do chamado devem ser registradas, mantendo-as sempre atualizadas a cada alteração, para que a resolução do incidente e o tratamento da requisição de serviço possam ocorrer de maneira adequada.
- **Categorização:**
  - Esta atividade compreende tanto a categorização de eventos que serão registrados como incidente, tanto quanto aqueles que devem ser encaminhados para o processo de requisição de serviços.

- Categorizar um incidente significa atribuir a ele uma classificação dentro do escopo de atividades do serviço, além de permitir o dimensionamento da quantidade de horas ou esforço técnico a ser consumido com o atendimento daquele incidente.

- **Priorização:**

  - A priorização dos incidentes deve ser realizada através da atribuição da Urgência (quão rápido o incidente precisa ser solucionado) e do dimensionamento do Impacto (extensão do dano no ambiente) que incidente registrado possa vir a causar.

- **Pesquisa e Diagnóstico:**

  - Após registrar, categorizar e priorizar o incidente, o atendente do chamado deverá prover o suporte inicial utilizando-se de scripts de atendimento e da base de erros conhecidos existente. Se, na pesquisa da Base de Conhecimento, o incidente for encontrado, deve-se verificar se existe uma solução de contorno e se a Central de Serviços pode aplicá-la;
  - Caso a solução não seja possível de aplicar dentro do escopo de serviços do atendimento, o chamado deve ser direcionado para grupo solucionador de especialistas, de acordo com as regras definidas e cadastradas no sistema da Central de Serviços do Suporte Técnico.

- **Encerramento do Chamado:**

  - Após a aplicação da solução de restauração ou contorno diretamente pela Central de Serviços ou após o retorno de chamados, o atendente deverá registrar de forma concisa e de fácil interpretação as ações tomadas para resolver o incidente/evento;
  - Além disso, a resolução e as ações tomadas devem ser informadas e confirmadas com o usuário;
  - O contato com o usuário para encerramento do chamado pode ser feito por telefone, podendo ser enviado e-mail, como método alternativo, caso não seja possível o contato;
  - Caso não exista resposta do usuário, seja ela por e-mail, telefone ou software de controle de chamados, o incidente registrado poderá ser automaticamente encerrado em até três dias úteis.

- **Encaminhamento de Chamados a Terceiros:**

  - Caso, durante o processo de atendimento, seja identificado que o chamado deverá resultar no acionamento de um subcontratado da Unidade do SAMU, caberá à Central de Serviços encaminhar o chamado e acompanhar sua resolução, monitorando os níveis de serviços prestados;
  - A Central de Serviços deverá gerir os chamados encaminhados aos subcontratados, bem como os níveis de serviços contratados, calculando as penalidades cabíveis por descumprimento desses serviços.

2.3.2.4. Catálogo de serviços

Item	Atividade do serviço	Descrição do serviço
1	Análise, configuração e manutenção de microcomputadores e notebooks.	Essa atividade consiste em identificar problemas nos microcomputadores ou notebooks, sejam eles físicos ou lógicos, reportando a solução e/ou posteriormente fazendo a correção dos mesmos, sendo documentada qualquer alteração na configuração dos dispositivos. Também consiste na configuração dos mesmos para o uso na rede e na instalação de softwares específicos nas máquinas correspondentes.
2	Análise, configuração, correção e ou instalação em equipamentos ativos de rede classe 1 e afins (Modem, switches e roteadores).	Essa atividade consiste em configurar, implantar e controlar as conexões dos diversos segmentos de rede no ambiente de TI interno e externo da Unidade do SAMU. Isso inclui a análise e correção dos switches e gateways existentes no ambiente, onde também se encontram recursos de roteamento, VLAN, VPNs, etc.
3	Análise e correção de problemas de segurança com antivírus.	Esse serviço inclui análise e correção de problemas de segurança que podem ser solucionados através do antivírus e/ou demais ferramentas de mercado.
4	Suporte e apoio ao usuário	Essa atividade consiste no auxílio e treinamento no uso de sistemas e equipamentos utilizados no ambiente de TI da Unidade do SAMU.
5	Instalação e Configuração de equipamentos	Esse serviço inclui a instalação, configuração e instrução de uso de equipamentos, de rede ou não, que sejam pertinentes ao ambiente de TI do local.
6	Análise, correção e atualização de firmwares de servidores do tipo torre, rack ou lâmina.	Essa atividade irá realizar uma análise de problemas relacionados ao servidor, bem como a possível solução, manutenção ou substituição do mesmo. Também inclui a atualização do firmware atual, se houver atualizações publicadas pelo fabricante, caso seja solicitado ou se faça necessário.

7	Análise, correção e atualização de componentes e serviços da central telefônica IPBX.	Esse serviço consiste na identificação de eventos e incidentes que possam ocorrer na central telefônica, bem como os componentes interligados diretamente na solução de telefonia, incluindo a manutenção corretiva/preventiva de tais incidentes/eventos e também o encaminhamento de chamados para terceiros, caso seja necessário.
8	Análise e solução de problemas de serviços em Windows Server	Esse serviço fornece uma análise dos problemas associados aos serviços do Windows server (File Server, Impressão, DHCP, SQL Server, etc.) e posteriormente a correção dos mesmos.
9	Análise e solução de problemas de ambientes virtuais VMware vSphere ESXI ou Citrix XenServer e outros.	Esse serviço fornece uma análise de todo ambiente virtual e posteriormente a correção dos mesmos. Inclui também o gerenciamento e configuração de máquinas virtuais.
10	Análise, configuração e correção de problemas em sistemas operacionais Linux e seus derivados.	Esse serviço fornece uma análise e posteriormente a correção de problemas em sistemas operacionais Linux e seus derivados, incluindo firewall, proxy, Apache, MySQL, Tomcat, FTP, OpenVPN, etc.
11	Assessoria para planejar e/ou definir melhorias no ambiente.	Discussão com um especialista sobre possíveis melhorias na infraestrutura local, políticas de TIC, bem como na utilização dos sistemas implantados.
12	Análise, configuração, e atualização de firmware de Nobreaks.	Essa atividade consiste em configurar, identificar incidentes e causas em Nobreaks gerenciáveis, para que se assegure o máximo de tempo do funcionamento do ambiente de TI no caso de surtos e falta de energia.
13	Análise, configuração, correção e gerenciamento de soluções de segurança de redes (Firewall).	Esse serviço inclui análise, configuração e correção de possíveis problemas causados por sistemas infectados por vírus, malwares ou spywares, no qual, o firewall deve ser utilizado como ferramenta de varredura, identificação e correção do problema na rede.

14	Elaboração de documentos finais	Esse serviço inclui confecção de documentações de apoio que poderão conter diagramas de rede e datacenter da infraestrutura de TI e mudanças ocorridas.
15	Serviço de Monitoramento Proativo da Infraestrutura.	Esse serviço inclui monitoramento proativo de toda a infraestrutura de TI, de acordo com o item 2.3.3 deste projeto.

2.3.2.5. Especificações dos serviços

Análise, configuração e manutenção de microcomputadores, notebooks e equipamentos; soluções antivírus e suporte ao usuário

- Manutenção corretiva/preventiva/limpeza de computadores e componentes;
- Formatação e instalação de sistemas operacionais Windows ou Linux;
- Instalação e configuração de softwares específicos em cada S.O, conforme necessidade;
- Configuração das interfaces de rede dos terminais;
- Configuração de compartilhamentos na rede, conforme necessidade;
- Instalação e configuração de impressoras e periféricos, de rede ou não;
- Configuração e atualização periódica de antivírus nos computadores e escaneamento periódico nos computadores;
- Remoção de vírus, malwares e spywares dos computadores;
- Apoio a usuário na utilização de sistemas e funcionalidades pertinentes ao trabalho do mesmo;
- Treinamento e apoio ao usuário na utilização de telefones IP e seus derivados, bem como na utilização das funcionalidades do sistema de telefonia pertinentes à cada área;
- Identificação de problemas físicos na infraestrutura de TI;
- Backup e restaurações de configurações e dados.

Serviços em equipamentos ativos de rede classe 1 e afins (Modem, switches e roteadores)

- Instalação, configuração, atualizações de firmwares de roteadores e switches;
- Implantação, configuração e gerenciamento de roteamentos dinâmicos, estáticos ou trunking, conforme necessidade;
- Gerenciamento de redes sem fio e cabeadas;
- Inclusão, exclusão e gerenciamento de Vlans de modo tagged ou untagged, nas Switches, de acordo com a necessidade;
- Configuração de interfaces, endereçamento e serviços de rede;
- Implantação, configuração e gerenciamento de interconexões através de VPN's, MPLS, etc., conforme necessidade e disponibilidade dos serviços;
- Backup e restauração de configurações dos equipamentos.

Serviços de segurança de redes, configuração, manutenção e gerenciamento de firewalls

- Criação, configuração e gerenciamento de redes lógicas, faixas de IP, perfis usuários;
- Inclusão e exclusão de dispositivos nas faixas de IP e perfis correspondentes;
- Atualização periódica da solução de segurança (firewall) conforme a disponibilidade;
- Criação, configuração e gerenciamento de políticas de segurança, regras de acesso e bloqueios necessários para o bom funcionamento da rede e para segurança dos dados trafegados;
- Análise de conformidade/aderência a políticas e normas de segurança. Esta atividade inclui a elaboração de relatórios técnicos indicando práticas a serem aplicadas em cada serviço para atender às normas de segurança;
- Elaboração de relatórios analíticos de acessos e estatísticas de tráfego de rede;
- Backup e restauração de configurações.

Instalação, configuração, atualização e manutenção em servidores

- Atualizações de firmwares;
- Configuração de sistema, tipos de particionamento e tipos de RAID a serem utilizados nos servidores;
- Instalação e configuração de Sistemas Operacionais (Windows servers, Linux ou seus derivados), além das configurações de rede e serviços dos mesmos;
- Backup e restauração de configurações.

Análise, manutenção, atualização e gerenciamento da Central Telefônica

- Gerenciamento de entroncamentos SIP, gateways e troncos analógicos, digitais e GSM; bem como análise de possíveis problemas decorrentes dos mesmos e resolução de incidentes junto aos provedores destes serviços;
- Manutenção corretiva/preventiva/limpeza dos servidores IPBX;
- Atualizações de firmware ou do sistema Asterisk, bem como do banco de dados, DAHDI ou outras ferramentas necessárias para o funcionamento da solução. Este serviço, por padrão, só deve ser feito caso exista necessidade comprovada pelo setor de suporte;
- Provimento, configuração e gerenciamento de todas as funcionalidades da Central Telefônica PBX IP, conforme descrito no item 2.2.2 deste projeto; além de manutenção e resolução de incidentes pertinentes às mesmas;
- Análise, configuração, atualização de firmwares e correção nos Storages que compõem a solução de telefonia, caso se faça necessário;
- Análise, configuração, atualização de firmwares e correção nos Gateways SIP/GSM que compõem a solução de telefonia, caso se faça necessário;
- Backup e restauração de dados e configurações.

Serviços em ambientes virtuais (VMware vSphere ESXI ou Citrix XenServer e outros)

- Instalação, configuração e resolução de problemas no software de virtualização da VMware e Citrix Xenserver;
- Inclusão e exclusão de máquinas virtuais, conforme necessidade;
- Gerenciamento de memória, discos e CPU's das MV's, alterando as configurações das mesmas, caso seja necessário, para o bom funcionamento do ambiente virtual;
- Instalação, configuração e manutenção de softwares de gerência de virtualização correspondentes;
- Conversão de servidores físicos para virtuais, caso se faça necessário(P2V);
- Backup e restauração de configurações.

Serviços de análise, identificação de incidentes e soluções relacionados a Nobreaks

- Identificação de possíveis surtos, falta de energia ou tensão de entrada inferior à aceitável;
- Identificação da autonomia das baterias;
- Contato junto ao prestador de serviços de eletricidade do local e reporte aos usuários e à Central de Serviços sobre detalhes do problema;
- Desligamento preventivo de equipamentos que possam ser impactados caso o nobreak descarregue completamente;

Elaboração de documentos técnicos

- Elaboração de documentos contendo todos os dispositivos existentes no ambiente de TI do local e informações que possam vir a ser necessárias no auxílio de resoluções de eventos ou incidentes;
- Criação de diagramas de rede;
- Criação de diagramas de rack contendo informações dos servidores e equipamentos;
- Atualização da base de conhecimento sobre os problemas e soluções relacionados.

Serviço de Monitoramento Proativo da Infraestrutura

- Consiste no monitoramento proativo de toda a infraestrutura de rede acordo com o item 2.3.4 deste projeto.

OBS.: O escopo dos serviços a serem contratados está segmentado por áreas de conhecimento, e devidamente especificado. Esta especificação foi baseada no parque computacional descrito nos **itens 2.1 e 2.2** deste projeto. Cabe ressaltar que a infraestrutura de TI sofre processo contínuo de atualização tecnológica, podendo se fazer necessário outros tipos de serviços pertinentes não inclusos neste escopo, mas, no entanto, pertinentes às áreas de conhecimento abordadas nas especificações. Deve o Suporte Técnico, portanto, prover a alocação de recursos especializados e adequados à prestação dos serviços aqui especificados.

2.3.3. Monitoramento

A rede de dados é composta de vários dispositivos e/ou serviços que precisam estar interligados, para que haja o compartilhamento de informações e recursos disponíveis dos ativos de rede, agilizando os processos das organizações. Por este motivo, se faz necessário o monitoramento, que através do NMS (*Network Management Station* ou Estação de Gerenciamento de Redes) e de protocolos/agentes presentes nos dispositivos, permite monitorar diversos estados e/ou serviços dos equipamentos que a rede oferece, facilitando assim o suporte proativo de problemas.

É de extrema importância o gerenciamento, para que se obtenha um bom fluxo no tráfego das informações, garantindo que os recursos sejam corretamente utilizados e visualizados

não sobrecarregando no transporte de dados, trazendo confiabilidade e segurança da estrutura.

O monitoramento, deve ser feito de forma remota, 24 horas por dia, através de uma central, com o objetivo de detectar atividades em tempo real, que porventura ocasionará futuras falhas, assim agindo de forma antecipada corrigindo-as em um curto espaço de tempo, prevenindo paradas e prejuízo ao processo operacional do SAMU.

Todos os eventos críticos na rede devem ser documentados, a partir de sistemas de help desk, com o objetivo criar um histórico para futuras consultas por relatórios gerenciais para análises de desempenho da infraestrutura.

A equipe de suporte é responsável pelo monitoramento da rede, porém, deve possuir capacidades específicas na área de informática, com conhecimento de especificações de hardware e software dos servidores, roteadores, switches, storage's, nobreaks, dentre outros dispositivos ou serviços que estarão conectados à rede e estações de trabalho.

Para o monitoramento da rede na unidade do SAMU, será necessário a utilização do protocolo SNMP (Simple Network Management Protocol) em conjunto com o RMON (Remote Network Monitoring) presente nos equipamentos, ou agentes próprios do sistema NMS, como uma ferramenta de monitoramento. O SNMP e o RMON foram criados para atender a necessidade de um padrão, de gerenciar dispositivos IP, além de fornecer aos usuários um conjunto simples de operações que permitem o gerenciamento remoto de dispositivos associados a esse protocolo, como roteadores, switches, servidores, storages e dentre outros equipamentos da rede, que contenham este protocolo embarcado.

Deve ser monitorada proativamente toda a infraestrutura cadastrada nesta solução, que abrange ativos de rede tais como: servidores (físicos), sistemas operacionais, Switches, Storages, Roteadores, Virtualizadores, Nobreaks, Gateways, Telefones IP, Links de internet, VPN's, dentre outros, e além disso, serviços do banco de dados, central telefônica, HTTP e FTP, que variam de acordo com a necessidade de informações disponibilizada pelos dispositivos e/ou sistemas.

O Monitoramento proativo da infraestrutura, deverá compreender os seguintes serviços:

- Instalação e configuração dos agentes de monitoramento nos servidores e clientes;
- Configurar os protocolos de monitoramento nos demais equipamentos que não suportam agentes (Agentless);
- Inclusão dos clientes na solução de monitoramento;
- Configurar os limites desejados para o bom funcionamento da infraestrutura e, com base nos valores individuais, gerar alertas programados quando eles apresentarem incidentes ou falhas;
- Configurar envio de alertas por e-mail;
- Configurar a geração de relatórios customizados de disponibilidade e informações específicas de equipamentos conforme o mesmo que, devidamente configurado, a disponibilize;
- O monitoramento deverá funcionar em regime 24x7 (24 horas por dia, 7 dias por semana).

Neste serviço, deverão ser atendidas as seguintes diretrizes de monitoramento, para que atinja um grau de informação desejado:

Ativo de TI	O que precisa ser monitorado	Protocolos padrão*
Sistemas operacionais dos servidores	Interfaces ethernet (Status UP/DOWN, consumo de rede), Carga de CPU, Memória RAM (total, livre e utilizada), Espaço em disco total e livre, Terminal services, banco de dados, Asterisk, HTTP, FTP.	- Agente próprio do sistema NMS - SNMP
Servidores	Interfaces ethernet (Status UP/DOWN, consumo de rede), Carga de CPU, Memória RAM (total, livre e utilizada), Espaço em disco total e livre.	- SNMP
Storage	Interfaces ethernet (Status UP/DOWN, consumo de rede), Carga de CPU, Espaço em disco total e livre.	- SNMP - Agente próprio do sistema NMS**
Roteadores	Interfaces ethernet (Status UP/DOWN, consumo de rede)	- SNMP - ICMP

Virtualizadores	Interfaces ethernet (Status UP/DOWN, consumo de rede), Carga de CPU, Espaço em disco total e livre, saúde da aplicação**	- SNMP - Agente próprio do sistema NMS**
Nobreaks	Interfaces ethernet (Status UP/DOWN, consumo de rede), Carga total, Carga Utilizada, Carga Restante, Temperatura, Tensão de entrada e saída, Tempo restante de baterias	- SNMP
Gateways	Interfaces ethernet (Status UP/DOWN, consumo de rede, tráfego), interfaces em uso, status das interfaces, status do dispositivo, status de VPN's	- SNMP - ICMP
Telefones IP	Interfaces ethernet (Status UP/DOWN, consumo de rede), status de conta registrada**	- ICMP - SNMP**
Links de internet	Status do link (UP/DOWN), Tráfego e latência	- ICMP

** Podem ser aplicados outros tipos de protocolos ou agentes, dependendo do modelo do dispositivo.*

*** Dependerá do dispositivo ou sistema suportar essa funcionalidade.*

2.3.4. E-mail

Deverá ser fornecida uma solução de e-mail hospedado com alta disponibilidade, com capacidade de 25gb por conta. O acesso deverá ser compatível com sistemas operacionais Windows, Linux, Mac OS, Android, IOS, navegadores Chrome, Internet Explorer, Firefox e Safari. O mesmo deverá possuir a possibilidade de sincronização das mensagens com clientes de e-mail, como Outlook, Mozilla Thunderbird ou algum outro, desde que este trabalhe com os protocolos IMAP e POP3.

2.3.5. Internet

Devido a vários serviços importantes que o SAMU utiliza sob a internet durante o dia, é necessário que sejam instalados links de internet que trabalhem em redundância na sede operacional, ou seja, caso o link principal pare, os secundários assumirão instantaneamente, garantindo uma maior segurança e confiabilidade no serviço. O link deverá apresentar as seguintes características:

2.3.5.1. Internet Setores Administrativo e Regulação

Link para acesso à rede mundial de computadores, INTERNET, de velocidade de 100 Mbps com garantia de banda de 80% sobre o valor nominal do link, que suporte aplicações TCP/IP e proveja o acesso à rede internet. Fornecimento de, no mínimo, 01 (um) endereço IPv4 público e válido na internet. O acesso deverá ser permanente (24 horas por dia e 07 dias por semana, a partir de sua ativação). Garantia e atendimento preferencial com SLA de no mínimo 97% (ou 10 dias parados em 365 dias do ano), sendo que não poderão ser dias consecutivos ou mais de dois dias no mesmo mês ou mês seguinte. Fornecimento de equipamentos para instalação do link, bem como para o funcionamento do mesmo. A tecnologia de acesso deverá ser através de fibra óptica ou par metálico. A entrega do link deverá ser feita com cabo de rede padrão categoria 5e e conectores RJ45 tipo 568B. O link deverá ser monitorado 24hs por dia.

2.3.5.2 Almoxarifado

Link para acesso à rede mundial de computadores, INTERNET, de velocidade de 50 Mbps com garantia de banda de 50% sobre o valor nominal do link. Garantia e atendimento preferencial com SLA de no mínimo 97% (ou 10 dias parados em 365 dias do ano), sendo que não poderão ser dias consecutivos ou mais de dois dias no mesmo mês ou mês seguinte. Fornecimento de equipamentos para instalação do link, bem como para o funcionamento do mesmo. A tecnologia de acesso deverá ser através de fibra óptica, par metálico ou rádio. A entrega do link deverá ser feita com cabo de rede padrão categoria 5e e conectores RJ45 tipo 568B. O link deverá ser monitorado 24hs por dia.

Fls. nº

ANEXO II

MODELO DE PROPOSTA COMERCIAL READEQUADA

PROCESSO LICITATÓRIO N.º 056/2025 - PREGÃO ELETRÔNICO N.º 031/2025

Razão Social: _____, **CNPJ:** __. ___. ___/____-__

Logradouro:_____, **nº** ____, **Bairro:** _____

Cidade: _____, **UF:** __, **CEP:** _____-___, **Telefone:** (__) _____-____

E-mail.: _____

A empresa acima se propõe **a executar o objeto, conforme discriminado no Termo de Referência e seus anexos**, pelos preços e condições assinalados na presente, obedecendo rigorosamente às disposições da legislação competente e conforme Ata de Julgamento.

Item	Descrição	Unid.	Quant.	Vlr. Unit.	Vlr. Total
1	Suporte técnico ao usuário (via telefone, e-mail, acesso remoto e presencial); manutenção preventiva e corretiva; suporte a serviços; monitoramento; gerência proativa; fornecimento e manutenção de solução de e-mail; atualização de softwares e firmware dos equipamentos, conforme especificações do Termo de Referência.	Mês	12		
2	Fornecimento e gerência de 05 (seis) links de Internet destinados aos setores Administrativo, Regulação e Almoxarifado	Mês	12		

Item	Descrição	Unid.	Quant.	Vlr. Unit.	Vlr. Total
3	Fornecimento e gerência de 01 (um) links de Internet destinados ao setor Almoxarifado	Mês	12		

OBS: Colocar na Planilha acima apenas os itens vencidos.

Declaro ter tomado conhecimento do instrumento convocatório relativo à licitação em referência, estar ciente dos critérios de julgamento do certame e da forma de pagamento estabelecidos para remunerar a execução do objeto licitado.

Declaro para os devidos fins que a proposta acima compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega desta proposta.

LOCAL/DATA

_____

Nome do Responsável

Fls. nº

ANEXO III - MINUTA DE CONTRATO

CONTRATO Nº _____/20__.

O Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul, inscrito no CNPJ nº 17.813.026/0001-51, com sede na Rua Coronel Vidal, nº 800, São Dimas, Juiz de Fora, MG, representado pelo Presidente, Exmo. Sr. Pedro Augusto Junqueira Ferraz a seguir denominado **CONTRATANTE** e o(a) empresa/autônomo(a) _____, inscrito(a) no CPF/CNPJ _____, situada na(o) _____, nº ____, Bairro _____, Cidade _____ - __, representada pelo(a) Sr.(a) _____, CPF nº _____, a seguir denominado(a) **CONTRATADO(A),** resolvem firmar o presente contrato, com fundamento no **Processo nº 056/2025 - Pregão Eletrônico nº 031/2025**, em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, aplicando-se a este instrumento suas disposições irrestrita e incondicionalmente, bem como pelas cláusulas e condições seguintes:

1 - CLÁUSULA PRIMEIRA: DO OBJETO

1.1 - Constitui objeto do presente instrumento a **Contratação de empresa especializada na prestação de SERVIÇOS TÉCNICOS na área de TECNOLOGIA DA INFORMAÇÃO E TELECOMUNICAÇÕES, para atender as necessidades do CISDESTE**, nos termos e condições especificadas no Termo de referência parte integrante e inseparável deste contrato.

1.2 - Objeto da contratação:

Item	Especificação	Unid.	Qntd.	Vlr. Unit.	Vlr. Total

1.3 - Integram este Contrato, como se nele estivessem transcritos, o Termo de referência, o estudo técnico preliminar, quando elaborado, o edital da licitação, Proposta Comercial apresentada pela

CONTRATADA, eventuais anexos dos documentos supracitados, ambos constantes deste Processo de Licitação.

2 - CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1 - O prazo de vigência da contratação será 12 (doze), contados da data de assinatura do contrato, podendo ser prorrogado por até 10 anos nos termos do art. 106 e 107 da Lei 14.133/21, desde que a autoridade competente ateste que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado ou a extinção contratual sem ônus para qualquer das partes, conforme Estudo Técnico Preliminar.

3 - CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS (art. 92, IV, VII e XVIII)

3.1 - O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

4 - CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1 - NÃO será admitida a subcontratação do objeto contratual.

5 - CLÁUSULA QUINTA - PREÇO

5.1 - O valor total da contratação será de R$ _____, conforme quadro acima.

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

6 - CLÁUSULA SEXTA - PAGAMENTO (art. 92, V e VI)

6.1 - O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

7 - CLÁUSULA SÉTIMA - REAJUSTE (art. 92, V)

7.1 - O reajuste e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

8 - CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE (art. 92, X, XI e XIV)

8.1 - São obrigações do Contratante:

8.2 - Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

8.3 - Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

8.4 - Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

8.5 - Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

8.6 - Comunicar a empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;

8.7 - Efetuar o pagamento ao Contratado do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

8.8 - Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

8.9 - Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

8.9.1 - A Administração terá o prazo de até 30 dias, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

8.10 - Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 30 dias, a contar da data do protocolo.

8.11 - Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

8.12 - A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

9 - CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO (art. 92, XIV, XVI e XVII)

9.1 - O Contratado deve cumprir todas as obrigações constantes deste Contrato e de seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

9.2 - Atender às determinações regulares emitidas pelo fiscal/gestor do contrato ou autoridade superior (art. 137, II);

9.3 - Alocar, quando for o caso, os empregados necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

9.4 - Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

9.5 - Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos;

9.6 - Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do fiscal ou gestor do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

9.7 - Quando não for possível a verificação da regularidade no Sistema de Cadastro utilizado pelo(a) Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul, o contratado deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos:

1) prova de regularidade relativa à Seguridade Social;

2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União;

3) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado;

4) Certidão de Regularidade do FGTS – CRF; e

5) Certidão Negativa de Débitos Trabalhistas – CNDT;

9.8 - Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante;

9.9 - Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.

9.10 - Prestar todo esclarecimento ou informação solicitada pelo Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.

9.11 - Paralisar, por determinação do Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

9.12 - Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato.

9.13 - Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.

9.14 - Submeter previamente, por escrito, ao Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.

9.15 - Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

9.16 - Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

9.17 - Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116);

9.18 - Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único);

9.19 - Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

9.20 - Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021;

9.21 - Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul;

9.22 - Se for o caso, realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul ou da nova empresa que continuará a execução dos serviços;

9.23 - Ceder ao Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul todos os direitos patrimoniais relativos ao objeto contratado, o qual poderá ser livremente utilizado e/ou alterado em outras ocasiões, sem necessidade de nova autorização do Contratado.

10 - CLÁUSULA DÉCIMA- OBRIGAÇÕES PERTINENTES À LGPD

10.1 - As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

10.2 - Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

10.3 - É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

10.4 - A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado, que possam impactar no cumprimento das obrigações relacionadas a LGPD.

10.5 - Quando for o caso, terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do contratado eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

10.6 - É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD, quando cabível.

10.7 - O Contratado deverá exigir de suboperadores e subcontratados, se houver, o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

10.8 - O Contratado deverá prestar, no prazo fixado pelo Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

10.9 - O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

11 - CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO (art. 92, XII e XIII)

11.1 - Eventual regra concernente a garantia de execução, encontra-se pormenorizada em tópico específico do Termo de Referência, parte integrante e inseparável deste instrumento de contrato.

12 - CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS (art. 92, XIV)

12.1. O(a) contratado(a) que descumprir o contrato, caracterizando qualquer das infrações previstas no art. 155 da Lei nº 14.133/2021 e no item 12.1 do edital, ficará sujeito às sanções previstas no art. 156, conforme detalhado no item 12.2 do edital, observados os procedimentos estabelecidos nos arts. 157 e 158 da referida lei.

12.1.1. As infrações e sanções administrativas encontram-se devidamente definidas no item 12 e seguintes do edital de licitação, parte integrante e inseparável deste contrato.

12.2. O(a) contratado(a) declara plena ciência das hipóteses de infrações e sanções previstas no item 12 e seguintes do edital de licitação.

13 - CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO CONTRATUAL (art. 92, XIX)

13.1 - O contrato se extingue quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

13.2 - Na hipótese de serviços contínuos, o contrato pode ser extinto antes do prazo nele fixado, sem ônus para o Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

13.3 - A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

13.4. Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

13.5 - O contrato pode ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

13.5.1 - Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

13.5.2 - A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a rescisão se não restringir sua capacidade de concluir o contrato.

13.5.2.1 - Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

13.6 - O termo de rescisão, sempre que possível, será precedido:

13.6.1 - Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

13.6.2 - Relação dos pagamentos já efetuados e ainda devidos;

13.6.3 - Indenizações e multas.

13.7 - A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, caput, da Lei n.º 14.133, de 2021).

14 - CLÁUSULA DÉCIMA QUARTA – DOTAÇÃO ORÇAMENTÁRIA (art. 92, VIII)

14.1 - As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento do Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul, para o exercício atual, na classificação abaixo:

3.3.90.39.00.1.02.01.10.302.0001.2.0003 1.633.000 RATEIO MACRO SUDESTE - GESTÃO DO CONSÓRCIO.

14.2 - A dotação relativa aos exercícios financeiros subsequentes, quando se tratar de serviços e fornecimento contínuos será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

15 - CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS (art. 92, III)

15.1 - Os casos omissos serão decididos pelo Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

16 - CLÁUSULA DÉCIMA SEXTA – ALTERAÇÕES

16.1 - Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

16.2 - O contratado será obrigado a aceitar, nas mesmas condições contratuais, acréscimos ou supressões de até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato que se fizerem nas obras, nos serviços ou nas compras, e, no caso de reforma de edifício ou de equipamento, o limite para os acréscimos será de 50% (cinquenta por cento), nos termos do art. 125 da Lei nº 14.133, de 2021.

16.3 - Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

17 - CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO

17.1 - Incumbirá ao Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94, salvo a exceção prevista no inciso III, c/c parágrafo único do art. 176, ambos da Lei nº 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em observância ao art. 8º, § 2º, da Lei nº 12.527, de 2011.

18 - CLÁUSULA DÉCIMA OITAVA– FORO (art. 92, §1º)

18.1 - Fica eleito o Foro da Comarca do município da licitante, para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21.

Para firmeza e validade do pactuado, o presente Termo de Contrato foi lavrado em duas (duas) vias de igual teor, que, depois de lido e achado em ordem, vai assinado pelos contraentes.

__Local__, __ de _____ de 20__.

_____

Pedro Augusto Junqueira Ferraz
Presidente

_____

Nome Representante Legal
Razão Social da Empresa

TESTEMUNHAS

1) Ass.:_____ **2) Ass.:**_____

Nome:_____ **Nome:**_____

CPF:_____ **CPF:**_____

ESTUDO TÉCNICO PRELIMINAR

1 - Informações Básicas

1.1 - Contratação de empresa especializada na prestação de SERVIÇOS TÉCNICOS na área de TECNOLOGIA DA INFORMAÇÃO E TELECOMUNICAÇÕES, para atender as necessidades do CISDESTE, conforme solução definida neste estudo técnico preliminar.

2 - Descrição da necessidade

2.1 - O Consórcio Intermunicipal de Saúde para Gerenciamento da Rede de Urgência e Emergência da Macro Sudeste e Leste do Sul - CISDESTE é entidade pública responsável pela operacionalização do Serviço de Atendimento Móvel de Urgência - SAMU 192 em 147 municípios das regiões Sudeste e Leste do Sul do Estado de Minas Gerais.

Para a adequada execução desse serviço essencial, torna-se indispensável uma infraestrutura robusta e continuamente operacional de Tecnologia da Informação e Telecomunicações, incluindo redes de dados, voz, telefonia IP, servidores, sistemas, links de Internet, estações de trabalho e demais recursos tecnológicos.

O projeto técnico que embasa a operação da Central de Regulação do CISDESTE foi estruturado com base em solução de telefonia IP utilizando Asterisk, software livre que atua como PABX IP, exigindo suporte especializado para sua correta administração, atualização e monitoramento.

Além da Central de Regulação, toda a infraestrutura administrativa - computadores, redes internas, segurança lógica, periféricos e equipamentos - necessita de suporte contínuo e profissional para manter níveis adequados de desempenho e disponibilidade.

Considerando que o serviço do SAMU opera 24 horas por dia, 7 dias por semana, e que a indisponibilidade de sistemas e comunicação pode comprometer diretamente o atendimento à população, a contratação de empresa especializada mostra-se imprescindível, garantindo:

- suporte técnico remoto e presencial;
- manutenção preventiva e corretiva;
- monitoramento proativo dos recursos de TI e Telecom;
- gestão dos links de Internet;
- resposta rápida a incidentes operacionais;
- continuidade e segurança dos serviços prestados.

Trata-se, portanto, de necessidade pública contínua, essencial ao funcionamento das atividades finalísticas do CISDESTE, enquadrando-se nas exigências de planejamento e motivação previstas na Lei nº 14.133/2021.

3 - Área(s) requisitante(s)

3.1 - Gerência Administrativa.

4 - Descrição dos Requisitos da Contratação

4.1 - Da natureza dos serviços

4.1.1 - A natureza do objeto deste ETP dadas suas características, enquadra-se em serviços comuns nos termos da Lei nº 14.133/2021, cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado, devendo, portanto, ser licitado por meio do **Pregão**, preferencialmente na forma **Eletrônica**.

4.2 - Da justificativa acerca da natureza continuada do serviço

4.2.1 - Os serviços prestados de forma contínua são aqueles que, pela sua essencialidade, visam a atender à necessidade pública de forma permanente e contínua, por mais de um exercício financeiro, assegurando a integridade do patrimônio público ou o funcionamento das atividades finalísticas do órgão, de modo que sua interrupção possa comprometer a prestação de um serviço público ou o cumprimento da missão institucional.

4.3 - Duração inicial do contrato de prestação de serviços de natureza continuada:

4.3.1 - O prazo de vigência da contratação será 12 (doze) contados da data de assinatura do contrato, podendo ser prorrogado por até 10 anos nos termos do art. 106 e 107 da Lei 14.133/21, desde que a autoridade competente ateste que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado ou a extinção contratual sem ônus para qualquer das partes.

4.4 - Sustentabilidade

4.4.1 - Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos:

4.4.1.1 - Observar os princípios de sustentabilidade contidos na Lei 14.133/2021, na Lei 12.305/10 (Política Nacional de Resíduos Sólidos) e demais legislações específicas, adotando ainda, na execução do objeto contratual, práticas de racionalização no uso de materiais e serviços quando cabível, com destaque:

a) utilização de materiais que sejam reciclados, reutilizáveis ou biodegradáveis, e que reduzam a necessidade de manutenção, conforme determina o Conselho Nacional do Meio Ambiente (CONAMA);d) redução de resíduos, reaproveitamento e destinação adequada dos materiais recicláveis;c) utilização de equipamentos com baixo consumo energético, de água e baixa emissão de ruído;d) observação das normas do INMETRO;e) racionalização do uso de substâncias potencialmente tóxicas/poluentes;f) fornecer e fiscalizar o uso de todos os equipamentos de proteção individual (EPI) para os seus empregados e equipamentos de proteção coletiva (EPC) necessários, de acordo com as normas da ABNT e Portaria nº 3.214/78 do Ministério do Trabalho.

5 - Levantamento de Mercado

5.1 - Realizou-se levantamento junto ao mercado e a contratações similares efetivadas por outros órgãos e entidades da Administração Pública, com o objetivo de identificar práticas, metodologias, modelos de execução e soluções aplicáveis ao atendimento da necessidade apresentada.

No entanto, não foram identificadas alternativas viáveis que substituam a contratação, na forma e extensão descritas neste Estudo Técnico Preliminar, dada a natureza crítica, contínua e especializada dos serviços de Tecnologia da Informação e Telecomunicações necessários ao CISDESTE.

Constatou-se que o modelo de contratação por empresa especializada, com disponibilidade contínua, suporte técnico remoto e presencial, administração de redes, telefonia IP, servidores, segurança, virtualização e monitoração ativa, é idêntico ao adotado por outros entes da Administração, demonstrando aderência às melhores práticas e à realidade operacional de ambientes que exigem alta disponibilidade, especialmente aqueles relacionados a serviços essenciais.

Ressalta-se, ainda, que este é o modelo atualmente adotado pelo CISDESTE, que atende de forma adequada às necessidades da Administração Pública, revelando-se tecnicamente justificado e alinhado às exigências de continuidade e eficiência previstas na Lei nº 14.133/2021.

6 - Descrição da solução como um todo

6.1 – A solução objeto desta contratação consiste na contratação de empresa especializada na prestação de serviços técnicos em Tecnologia da Informação e Telecomunicações, abrangendo suporte, administração, monitoramento, manutenção, configuração, ajustes, atualização e gestão de toda a infraestrutura tecnológica do CISDESTE, conforme condições, quantidades e requisitos estabelecidos neste documento e em seus anexos.

6.2 – Todas as especificações técnicas, requisitos funcionais, quantitativos e características operacionais dos serviços foram definidos por este setor demandante com base em parâmetros técnicos objetivos, de modo a garantir a adequada execução dos serviços e o atendimento ao interesse público. Tais especificações visam assegurar continuidade operacional, segurança lógica, eficiência e disponibilidade plena das soluções tecnológicas que sustentam o funcionamento do SAMU 192 e da estrutura administrativa do Consórcio.

6.3 – Síntese da Solução Adotada

Para fins de contextualização, apresenta-se a seguir breve resumo dos principais componentes tecnológicos abrangidos pela contratação.

6.3.1 – Infraestrutura de Rede e Ambiente Operacional

A infraestrutura de rede do CISDESTE encontra-se estruturada e segmentada em três redes principais, visando segurança, estabilidade e isolamento adequado de tráfegos distintos:

I – Rede de Telefonia/Suporte (NCPI): utilizada para operação de telefones IP, servidores de comunicação, gateways e dispositivos correlatos;

II – Rede da Central de Regulação: destinada às operações da Central de Regulação das Urgências;

III – Rede Administrativa: utilizada pelas rotinas administrativas, sistemas internos, estações de trabalho e periféricos.

A infraestrutura física compreende racks de telecomunicações, switches PoE de alto desempenho, cabeamento estruturado, dispositivos de rede e sistemas auxiliares, demandando ambiente com refrigeração adequada, alimentação elétrica estável e monitoramento contínuo devido à sua criticidade.

A segurança de rede é provida por firewalls de última geração (NGFW) operando em ambiente virtualizado, com políticas específicas para cada segmento, controle de banda, balanceamento de links, criptografia, inspeção de tráfego e registros detalhados de eventos.

O ambiente é predominantemente virtualizado, utilizando hipervisores como Citrix XenServer ou VMware ESXi, com gerenciamento centralizado, migração entre hosts, redundância, snapshots, políticas de contingência e capacidade ociosa para manutenção da alta disponibilidade.

A integração das unidades operacionais do CISDESTE utiliza OpenVPN, garantindo comunicação segura e criptografada, mesmo em cenários de rede adversos, contribuindo para a resiliência dos serviços.

6.3.2 – Central Telefônica IP – Asterisk

A solução de telefonia do CISDESTE é baseada no Asterisk, software livre que desempenha funções de PBX IP, com ampla capacidade de customização, integração e escalabilidade. Entre suas funcionalidades destacam-se:

- controle e bilhetagem de chamadas;
- compatibilidade com o protocolo SIP (RFC 3261);
- utilização de gateways analógicos, digitais e GSM;
- gravação de chamadas;
- atendimento automatizado (URA), DAC e filas;
- configuração de ramais, troncos e regras de discagem;
- conferências e serviços suplementares;
- integração com serviços de rede (DHCP, DNS, NTP);
- operação em alta disponibilidade.

A administração da central requer equipe especializada, apta a realizar ajustes, correções, atualizações, manutenção e monitoramento contínuo.

6.3.3 – Serviços Técnicos Abrangidos

Os serviços contemplados pela solução abrangem atividades constantes e altamente especializadas, essenciais ao pleno funcionamento das operações do CISDESTE, incluindo:

a) suporte técnico remoto e presencial aos usuários, abrangendo sistemas operacionais, periféricos, antivírus, impressoras e estações de trabalho;

b) administração e manutenção de rede, incluindo configuração de VLANs, Wi-Fi, roteamento, switches, roteadores, atualizações de firmware e trunking;

c) gestão de servidores e ambientes virtualizados, englobando criação, manutenção, migração e monitoramento de máquinas virtuais, backups e recuperação;

d) administração de sistemas de segurança e firewalls, com criação e ajuste de regras, análise de incidentes, relatórios e controles de acesso;

e) gestão da central telefônica Asterisk, com configuração e manutenção de troncos, ramais, gateways, filas, gravações e serviços suplementares;

f) monitoramento proativo de servidores, links, dispositivos e serviços críticos por meio de ferramenta NMS;

g) elaboração e manutenção de documentação técnica, incluindo diagramas, relatórios, inventários, registros e histórico de intervenções.

g) Documentação técnica, contemplando diagramas de rede, diagramas de rack, relatórios, registros de incidentes e histórico de manutenção.

6.4 – Remissão ao Anexo Técnico

Registra-se, por fim, que todas as especificações técnicas completas da Infraestrutura de Rede, Ambiente Operacional, Central Telefônica IP – Asterisk e Serviços Técnicos encontram-se integralmente detalhadas no ANEXO I – Descritivo Técnico da Infraestrutura e Serviços, cuja inclusão integral neste item seria redundante. O presente resumo tem finalidade meramente contextual, devendo o anexo ser consultado para fins de especificação técnica detalhada.

7 - Estimativa das Quantidades a serem contratadas

Item	Descrição	Unid.	Quant.
1	Suporte técnico ao usuário (via telefone, e-mail, acesso remoto e presencial); manutenção preventiva e corretiva; suporte a serviços; monitoramento; gerência proativa; fornecimento e manutenção de solução de e-mail; atualização de softwares e firmware dos equipamentos.	mês	12
2	Fornecimento e gerência de 05 (cinco) links de Internet destinados aos setores Administrativo e de Regulação.	mês	12
3	Fornecimento e gerência de 01 (um) link de Internet destinado ao setor de Almoxarifado.	mês	12

7.1 - Metodologia de cálculo dos quantitativos

7.1.1 - O dimensionamento do quantitativo foi obtido com base no histórico de serviço o qual o CISDESTE já possui contrato.

8 - Estimativa do Valor da Contratação

8.1 - O valor estimado da contratação é de R$ 256.902,24 (duzentos e cinquenta e seis mil, novecentos e dois reais e vinte e quatro centavos).

8.2 - O valor estimado da contratação foi elaborado seguindo as regras previstas no art. 23 da Lei Federal nº 14.133/2021, acompanhados dos preços unitários referenciais, das memórias de

cálculo e dos documentos que lhe dão suporte, com os parâmetros utilizados para a obtenção dos preços e para os respectivos cálculos, os quais foram utilizados para elaboração do orçamento estimativo.

9 - Justificativa para o Parcelamento ou não da Solução

9.1 - O objeto desta contratação, será licitado de forma GLOBAL OU POR GRUPO DE ITENS, nos termos do §3º, incisos I e II do art. 40 da Lei Federal nº 14.133/2021, por conta da interdependência dos serviços, causando desta forma uma espécie de unidade no todo. O desmembramento do objeto, nesse sentido, foi descartado, por inviabilidade técnica, operacional e por medida de segurança jurídica. Caso fossem contratadas duas empresas, haveria uma significativa dificuldade em determinar a responsabilidade em caso de falhas na execução do serviço, podendo comprometer a adoção das providências cabíveis.

9.1.1 - Ademais, impende ressaltar que ter uma única empresa responsável pelo objeto, torna o controle de fiscalização do objeto licitado muito mais eficaz por parte da contratante, melhora e facilita o acompanhamento de problemas e soluções, e sobretudo na verificação das obrigações e atribuições da contratada, reduzindo os riscos de falhas e insucesso.

9.1.2 - Ainda, corroborando a contratação por agrupamento de itens, ressalta-se a viabilidade da metodologia pleiteada e a disponibilidade de empresas para execução do objeto, ao passo que essa é a forma mais usual de contratação no mercado.

10 - Contratações Correlatas e/ou Interdependentes

10.1 - **Contratações correlatas** são aquelas que guardam relação com o objeto principal, interligando-se a essa prestação do serviço, mas que não precisam, necessariamente, ser contratadas para a completa prestação do objeto principal. **Já as contratações interdependentes** são aquelas que precisam ser contratadas juntamente com o objeto principal para sua completa prestação.

10.2 - Entendemos não haver para o objeto em questão a previsão de contratação correlata e nem interdependente.

11 - Demonstração da previsão da contratação no plano de contratações anual, quando elaborado

11.1 - A contratação pretendida está alinhada com o Planejamento previsto para o atual exercício, pelo(a) Consórcio Intermunicipal para Rede de Urgência e Emergência da Região Macro Sudeste e Macro Leste do Sul.

12 - Demonstrativo dos resultados pretendidos em termos de economicidade e de melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis;

12.1 - Pretende-se com esta contratação atingir os seguintes resultados:

12.1.1 A contratação de empresa especializada em serviços técnicos de Tecnologia da Informação e Telecomunicações visa assegurar a operacionalidade contínua e eficiente da infraestrutura tecnológica do CISDESTE, essencial à prestação ininterrupta do SAMU 192 em 147 municípios. A necessidade decorre da imprescindibilidade de suporte técnico qualificado para administração, atualização e monitoramento da solução de telefonia IP baseada em Asterisk, bem como da manutenção preventiva e corretiva dos sistemas, redes, servidores e demais equipamentos, garantindo a disponibilidade e segurança dos serviços essenciais à regulação e atendimento de urgência.

12.1.2 Espera-se, com a contratação, a redução de riscos de indisponibilidade dos sistemas críticos, a otimização do tempo de resposta a incidentes operacionais e a continuidade dos serviços 24 horas por dia, sete dias por semana, assegurando a qualidade e eficácia do atendimento à população. Ademais, a medida propiciará melhor aproveitamento dos recursos tecnológicos e humanos, promovendo a economicidade e eficiência na gestão dos ativos de TI e Telecomunicações, em consonância com os princípios e exigências da Lei 14.133/2021.

13 - Providências a Serem Adotadas

13.1 - Não há providências a serem adotadas pela administração previamente à celebração do contrato, visto que não há necessidade de capacitação de fiscais e/ou gestores de contrato ou de adequação do ambiente da organização.

14 - Possíveis Impactos Ambientais

14.1 - Não se vislumbra a ocorrência de possíveis impactos ambientais gerados pela contratação em estudo, contudo, a contratada deverá conduzir suas ações em conformidade com os requisitos legais e regulamentos aplicáveis, observando também a legislação ambiental para a prevenção de adversidades ao meio ambiente e a saúde dos trabalhadores e envolvidos na execução do objeto.

15 - Análise de Risco

15.1 - Conforme entendimento do TCU[1] "(...) o estudo técnico preliminar já serve, naturalmente, ao gerenciamento de riscos da futura contratação". Cada elemento do ETP permite de certa forma antecipar problemas e prever oportunidades, orientando a tomada de decisão na fase de elaboração dos demais documentos, especialmente o termo de referência.

15.2 - No entanto, no presente caso, foram identificados riscos relevantes que devem ser abordados de forma separada, sendo necessário elaborar o Mapa de Risco.

16 - Declaração de Viabilidade

16.1 - Declaro(amos) viável esta contratação.

16.1.1 - Justificativa da Viabilidade

16.1.1.1 - Pelo constatado nos estudos preliminares a contratação é viável e encontra-se dentro da previsão de despesas do setor requisitante. Além disso, a contratação permitirá ao setor a continuidade dos serviços de modo a não paralisar, retardar ou de alguma forma prejudicar o andamento dos serviços, desde que sejam adotadas as premissas e conclusões descritas neste documento.

Juiz de Fora, 16/12/2025.

Rafael Pontes Miranda
Gerente Administrativo

Luiz Fernandes Novais Oliveira
Assessor Técnico

Acxel Albrecht Araújo
Supervisor de Planejamento e Contratações Públicas

DESPACHO

Aprovo o Estudo Técnico Preliminar, considerando a importância da contratação, em face das justificativas técnica apresentadas.

Juiz de Fora, 16/12/2025.

Denys Arantes Carvalho
Secretário Executivo

ANEXO I – DESCRITIVO TÉCNICO DO PROJETO DE INFRAESTRUTURA E SERVIÇOS

1 - DESCRIÇÃO DO PROJETO

O projeto consiste em definir a melhor solução de Telecomunicações que atenda às necessidades atuais e futuras para o Serviço de Atendimento Móvel de Urgência (SAMU), onde será necessário a contratação de uma empresa, com capacidade de desenvolver, implantar e gerir o seu ambiente tecnológico, baseado na definição de projeto aqui colocada. A empresa deverá implantar e configurar a infraestrutura de Telecomunicações e TI, com enfoque na central de telefonia IP baseada no ASTERISK (O Asterisk é um software Livre, de código aberto, que implementa em software os recursos encontrados em um PABX convencional, utilizando tecnologia de telefonia IP) e seus componentes, fornecer suporte remoto e local na sede do SAMU, conforme descritivo técnico a seguir:

1.1 - REDE - INFRAESTRUTURA DE REDE FÍSICA (NCPI)

1.1.1. Definição

Para substituir sistemas convencionais de telecomunicações e centrais de PBX, a rede de telefonia IP e de dados terá que oferecer uma disponibilidade similar ou superior que irão se colocar a prova num campo onde o conceito de alta disponibilidade já é esperado. Um dos maiores motivos pelos quais os sistemas convencionais PBX possuem uma alta disponibilidade é o fato deles possuírem um sistema com bateria de backup de longa autonomia. Oferecer energia através da rede para o telefone IP (Power over Ethernet - PoE, energia através do cabo de rede IEEE 802.3af) terá que explorar em campo o conceito de fornecer energia para atingir a disponibilidade esperada. Por isso os racks de Telecom convencionais, que eram usados para armazenar dispositivos passivos como painéis de cabos e outros, agora vão precisar acomodar switches PoE de alta potência, roteadores, elementos de comutação ótica e Nobreaks com grande autonomia. A refrigeração e o fluxo de ar nessas salas de Telecom se tornarão importantes para garantir uma operação contínua.

A rede de Telefonia IP e de dados descrita é construída em camadas e cada camada é formada por componentes que residem em uma de suas 4 localizações físicas (Figura 1).

Necessidades de energia e refrigeração para essas quatro localidades variam de acordo com o descrito nas próximas seções e baseados em normas internacionais de operação.

Como tratamos de uma Infraestrutura Física de Rede Crítica (NCPI) que é o alicerce de todas as redes de alta disponibilidade, devemos levar em conta que esta deve ser sólida, escalável, altamente disponível, gerenciável e incluir:

1. Sistemas de energia como Nobreaks, unidades de distribuição de energia (PDUs) e geradores para fornecimento de energia e refrigeração para cargas críticas.
2. Sistemas de refrigeração para manter um ambiente ideal com regulação da temperatura e umidade.
3. Racks com equipamentos de redes críticas como switches L2 e L3, roteadores, gateways E1 e Internet, servidores, etc.
4. Sistemas de segurança física, virtual e proteção contra incêndio.
5. Cabeamento para interconexão dos equipamentos
6. Sistemas de gerenciamento que se comunicam local e remotamente, com serviços integrados para assegurar um funcionamento eficiente 24 horas por dia, 7 dias por semana. 365 dias por ano.
7. Serviços de suporte local, além de manutenção e diagnóstico

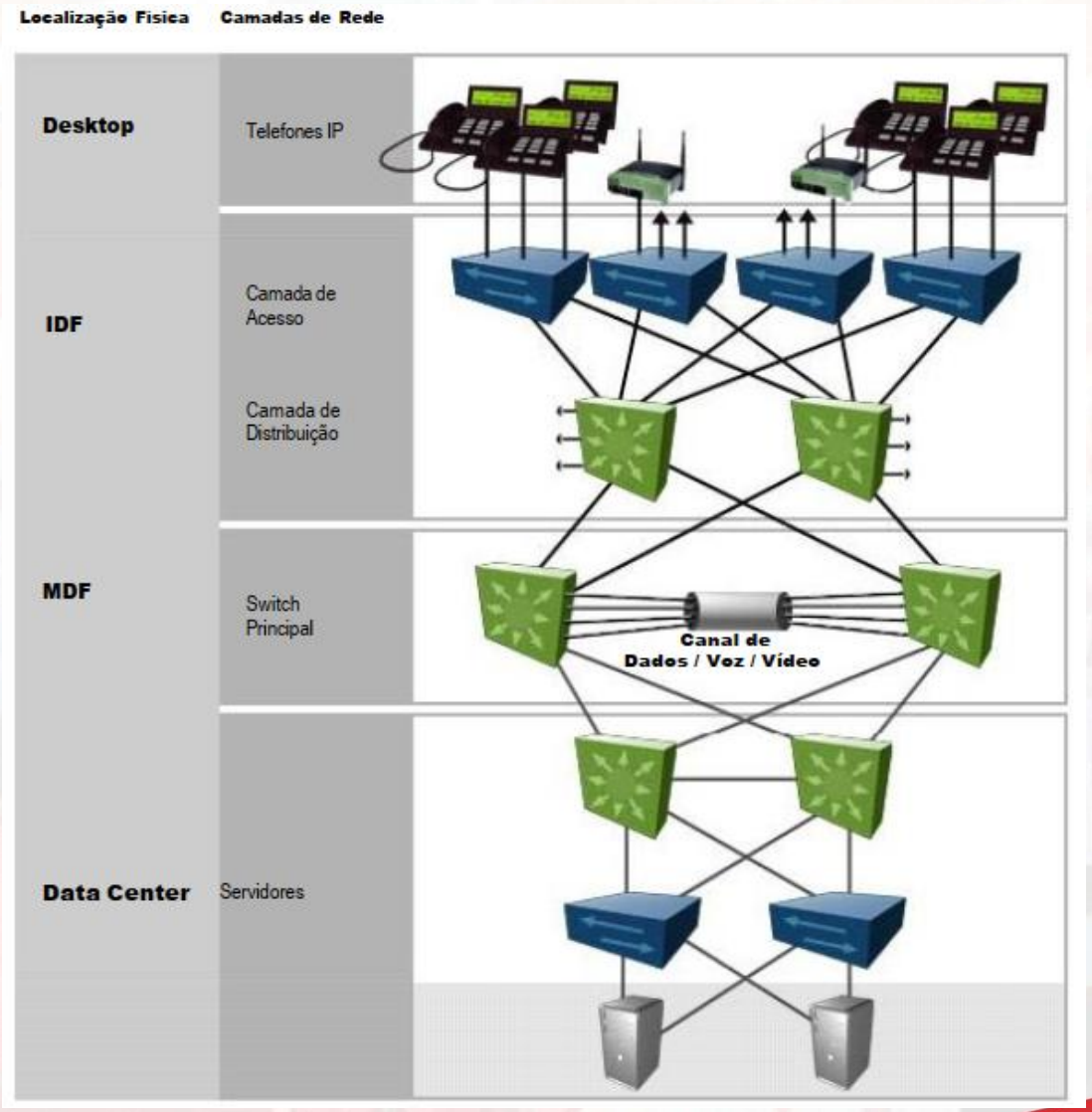


Figura 1 *– Camadas e localizações de uma rede de Telefonia IP Típica.*

1.1.2. Objetivo

Implantar e configurar a infraestrutura de rede, capaz de fornecer dados e telefonia IP para o complexo regulador do SAMU dentro dos padrões para NCPI (figura 1).

A rede terá as definições lógicas e de segurança segmentadas em três partes distintas. Telefonia/Suporte (NCPI) com faixa IP própria, roteador de comunicação e integração VPN com outras redes de emergência. Regulação NCPI com faixa IP própria e seu Firewall. Administrativo e uso geral com faixa IP própria e seu firewall.

1.1.3. Infraestrutura LocaL

Para a implantação deste projeto, foi definido condições mínimas de ambiente, cabeamento, energia e refrigeração que seguem abaixo:

Dispositivos de Comunicação

Os dispositivos de comunicação típicos na ponta, são telefones IP (Figura 2a), assim como computadores e dispositivos de rede sem fio (Figura 2b), oferecendo funções de telefonia e dados. O consumo típico dos telefones IP é de 6-7 Watts, porém alguns dispositivos podem consumir mais energia. A norma, IEEE 802.3af, limita a corrente média drenada por esses dispositivos com cabos CAT5 para 350mA e especifica os pinos através dos quais a energia pode ser transmitida. Com o cumprimento dessa nova norma, aproximadamente 15W de energia poderão ser fornecidos a uma distância de até 100m. Para o consumo de energia acima desta distância, os dispositivos de comunicação terão que contar com fontes externas.

Figura 2a *– Telefone IP.*

Figura 2b *– Roteador Wireless.*

Ambiente

Estes dispositivos localizam-se nos ambientes da regulação médica e setor administrativo, são montados nas baias das mesas da regulação ou usados no ambiente de escritório do administrativo. Para instalações novas ou atualizadas, eles poderão ser alimentados pela linha de dados. Entretanto, em alguns casos, poderão ser alimentados através das tomadas da rede elétrica.

Desafios

Os telefones IP precisam estar tão disponíveis quanto os telefones PBX que eles substituem. Aqui, o maior problema, é assegurar sua operação mesmo durante uma queda de energia prolongada.

Melhores Práticas

Enviar energia através da linha de dados para o telefone (chamada de energia In-Line) é a melhor maneira de resolver este problema. Desta maneira, o telefone é alimentado pelo switch da rede localizado na sala de Telecom suportado por um Nobreak com grande autonomia. Para os dispositivos alimentados pela tomada de rede elétrica (não usando energia In-Line), pode ser usado um Nobreak com um longo tempo de autonomia (quatro, seis, oito horas ou mais).

IDF - Intermediate Distribution Frame (Ambiente de Distribuição Intermediário)

O IDF incorpora as camadas de acesso 2 e 3, com a distribuição de switches, roteadores, painéis de cabos, Nobreaks, bem como qualquer outro equipamento de telecomunicação montado em um rack (Figura 3a e 3b). Os switches utilizados possuem a capacidade de fornecer energia através de linhas de dados para alimentar os dispositivos de comunicação. Para switches sem essa capacidade, uma fonte de energia externa apropriadamente dimensionada é usada para injetar a energia In-Line.

Figura 3a *– IDF (rack de Telecom).*

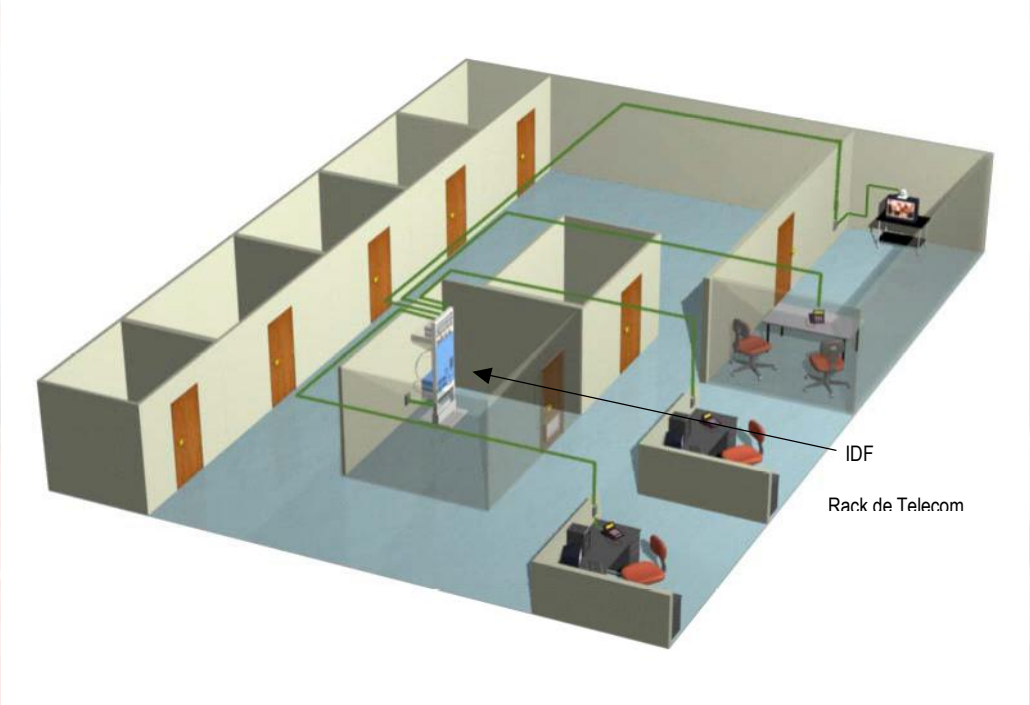


Figura 3b *– Layout Típico do IDF.*

Ambiente

Os IDFs para o projeto de rede do SAMU normalmente ficam na mesma sala dos MDFs e Data Center ou sala de servidores. Redes de telecomunicações convencionais normalmente usam esses racks para painéis de cabos e alguns switches de pequeno porte, porém os novos sistemas de Telefonia IP usam e dissipam consideravelmente mais energia. Estes novos Switches para Telefonia IP são geralmente montados em racks de 19" e tem um padrão de fluxo de ar que varia, dependendo do fabricante, por exemplo, lado a lado, de frente para trás, etc. Um IDF típico utilizará de 1 a 3 racks com equipamentos, e consumirá de 500 W a 4.000 W de energia CA monofásica ou bifásica. O croqui de exemplo é usado como referencial técnico. Nele todas as camadas NCPI são conjugadas.

O ambiente necessário para acomodações dos equipamentos, deverá possuir uma área útil de no mínimo 12m², uma das paredes deve possuir no mínimo 3,60m, sem obstáculos (porta, janela etc.) para instalação dos racks de telecomunicações, conforme figura 3c abaixo:

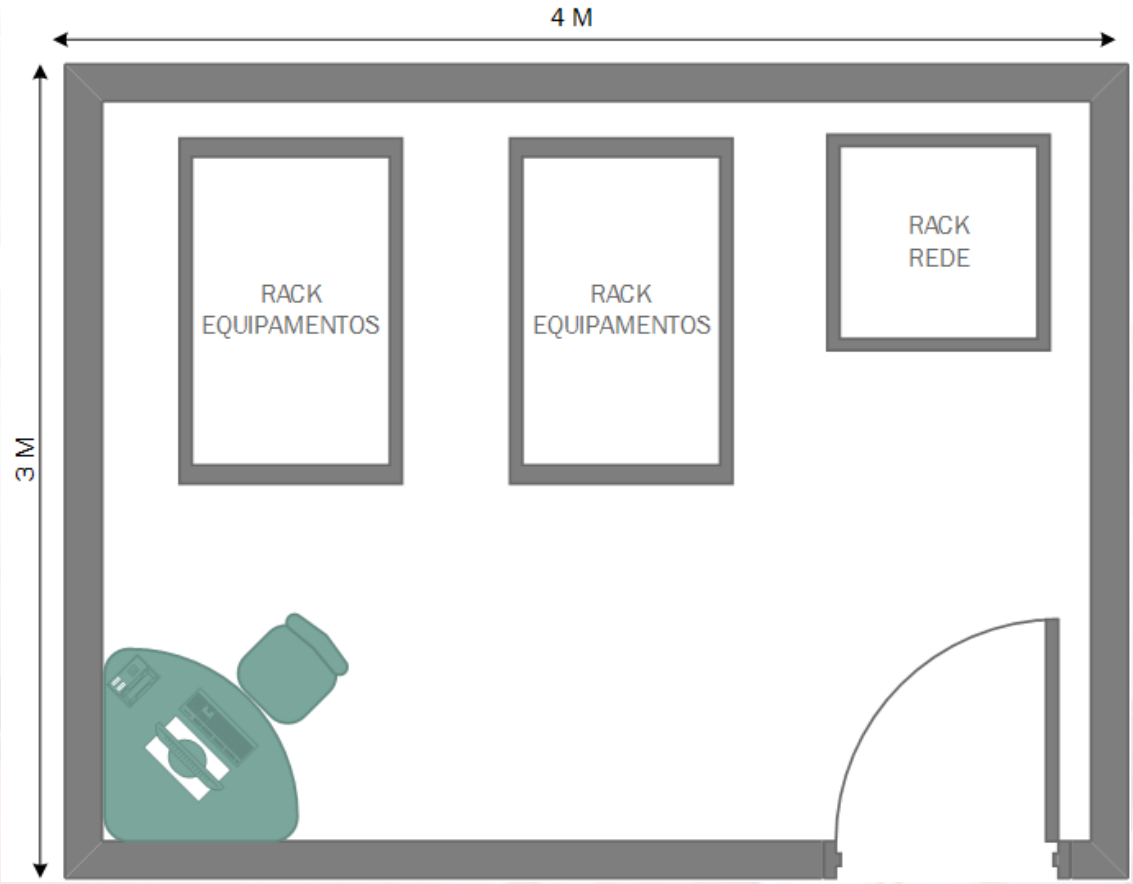


***Figura 3c**: Sala de Equipamentos.*

Desafios

Na implantação da Telefonia IP e rede de dados do SAMU, o IDF precisa do máximo de atenção para a energia e resfriamento. Com um consumo de 500 a 4.000 W, dependendo da arquitetura da rede e switch usado, a definição da tomada adequada, o consumo de energia com o disjuntor correto para os equipamentos de rede, Nobreak e PDUs em uma sala de Telecom é um desafio. O resfriamento e circulação do ar são geralmente um problema maior que não pode ser ignorado nesses ambientes.

Melhores Práticas

Todos os equipamentos no IDF devem ser protegidos por um Nobreak. A configuração do Nobreak é baseada em:

- Total de energia necessária em Watts;
- Autonomia necessária em minutos;
- Nível de redundância ou tolerância a falha desejada;
- Tensões e tomadas necessárias.

O Nobreak é dimensionado pela soma do consumo em Watt das cargas. Um Nobreak montado em rack como o da (Figura 4a) fornecerá aproximadamente quatro noves (99,99%) de disponibilidade de energia, enquanto um com redundância N+1 e by-pass embutido, como o da (Figura 4b), com uma hora de autonomia fornecerá aproximadamente cinco noves (99,999%), suficiente para a maior parte das aplicações.

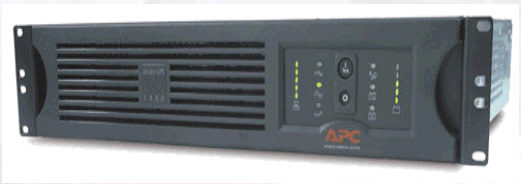


Figura 4a *– APC Smart-UPS.*

Figura 4b *– APC Symmetra RM.*

Nobreaks estão disponíveis com pacotes de baterias que fornecem diferentes tempos de autonomia. Os modelos apresentados nas Figuras 4a e 4b possuem pacotes de bateria opcionais, que podem ser usados para aumentar o tempo de autonomia para até 24 horas.

Mais altos níveis de disponibilidade, como seis ou sete noves, podem ser necessários para algumas aplicações críticas, tais como o SAMU. Tais requisitos podem ser atendidos com o uso de redundância de switches com fontes e cabos de alimentação duplos, Nobreaks redundantes, e arquiteturas elétricas concorrentes com gerador para backup. A empresa responsável pelo serviço deve avaliar essa disponibilidade e recomendar as infraestruturas com alta disponibilidade de energia para tais redes críticas.

Finalmente, identificar os plugs e tomadas necessárias para todos os equipamentos, incluindo o Nobreak da sala de telecom. O ideal é que todos os equipamentos estejam conectados diretamente no painel traseiro do Nobreak ou do transformador, devendo ser evitado o uso de réguas de tomadas adicionais ou PDUs para montagem em rack. Entretanto se existirem muitos equipamentos isso pode não ser prático e um PDU em Rack deve ser usado. Nesse caso, deve ser usado um PDU desenvolvido especificamente para esse propósito. O PDU deve possuir tomadas suficientes para conectar todos os equipamentos usados com algumas tomadas de reserva para necessidades futuras. Prefira usar PDUs com um medidor do consumo de energia, já que eles reduzem erros humanos, como sobrecarga acidental resultando em queda da carga.

Para a seleção correta do modelo de Nobreak apropriado, atingindo o nível de energia, redundância, tensão e autonomia necessárias, o processo é simplificado ao usar um seletor de Nobreaks, como o seletor de Nobreaks da APC em http://www.apcc.com/template/size/apc/. Este sistema disponibiliza dados atualizados de consumo de energia para os switches, servidores e dispositivos de armazenamento mais usados no mercado, evitando a necessidade de coletar esses dados. Em sistemas como este, a escolha de configurar um Nobreak vai fornecer várias opções de tomadas.

Para assegurar uma operação contínua dos equipamentos na sala de Telecom sem qualquer interrupção, as questões de resfriamento devem ser identificadas e consideradas. A dissipação de energia na sala deve ser calculada para decidir a melhor maneira com custo adequado para resolver o problema (veja Tabela 1). É importante observar que os equipamentos envolvidos podem ter um alto consumo de energia, entretanto isso não significa que eles consomem toda essa energia na sala. Por exemplo, os servidores podem drenar 1.800 W, mas podem estar consumindo apenas de 200 a 500 W na sala. A energia restante está sendo fornecida através da rede aos vários Telefones IP espalhados, e consumida por toda a área do complexo regulador do SAMU.

Item	Dados Necessários	Cálculo da Dissip. de Saída	Subtotal da Dissip. de Saída
Switches sem energia In-Line, outros equipamentos de TI (exceto unidades de energia externas)	Soma da energia de entrada em Watts	Mesma que o total da carga de energia de TI em watts	_____ Watts
Switches PoE	Energia de entrada em Watts	0.6 x energia de entrada	_____ Watts
Unidades de energia externas Servidores, Storages, gateways	Energia de entrada em Watts	0.6 x energia de entrada	_____ Watts
Iluminação	Energia de entrada da iluminação permanente ligada em Watts	Taxa de energia	_____ Watts
	Taxa de energia no (não a carga) em Watts	0.09 x taxa de energia do Nobreak	_____ Watts
Total	Subtotais acima	Soma dos subtotais acima	_____ Watts

Tabela 1 *– Tabela de cálculo da dissipação de calor num rack de Telefonia IP*

Uma vez que a energia dissipada na sala de Telecom seja calculada, siga o guia descrito na Tabela 2.

Carga de Calor Total no Rack	Condição	Análise	Ação
< 100 W	O prédio possui um ambiente uniformemente	A condução pelas paredes e a infiltração de ar será suficiente.	Nenhuma.
< 100 W	O prédio possui um espaço hostil, sem sistema de ar-condicionado.	O ar de fora da sala não pode ser considerado seguro para uso devido à temperatura ou contaminação.	Instale um condicionador de ar de precisão na sala e próximo aos Equipamentos.
100 – 500W	Existe sistema de ar-condicionado no forro falso (aéreo). O prédio possui um ambiente uniformemente condicionado.	O ar será suficiente se encaminhado para a sala, mas a porta pode bloquear o fluxo de ar. Traga o ar para dentro da sala pela porta e faça a exaustão para o retorno do condicionador de ar.	Coloque uma grelha de retorno para exaustão no teto da sala e uma grelha na parte inferior da porta da sala.

100 – 500W	Rack sem acesso a qualquer sistema HVAC O prédio possui um ambiente uniformemente condicionado.	O ar será suficiente se drenado para a sala, mas a porta pode bloquear o fluxo de ar. Traga o ar para dentro da sala pela parte inferior e a exaustão por cima da porta.	Coloque uma grelha de retorno para exaustão no topo e uma grelha para entrada de ar na parte inferior da porta da sala.
500 – 1000W	Existe sistema de ar-condicionado no forro falso (aéreo). O prédio possui um ambiente uniformemente condicionado.	O ar será suficiente se encaminhado para a sala, mas a porta pode bloquear o fluxo de ar. E um funcionamento contínuo de um ventilador é necessário e não confiável.	Coloque uma grelha com ventilação forçada para o retorno de exaustão no topo e uma abertura na parte inferior da porta da sala.
500 – 1000W	Rack sem acesso a qualquer sistema HVAC O prédio possui um ambiente uniformemente	O ar será suficiente se drenado continuamente para a sala, porém não há como captar o ar.	Coloque uma grelha com ventilação forçada para o retorno de exaustão no topo e uma abertura na parte inferior da porta da
> 1000W	Existe sistema de ar-condicionado no forro falso (aéreo) e está acessível. O prédio possui um ambiente uniformemente condicionado.	O ar será suficiente se drenado continua e diretamente através dos equipamentos e não houver ar quente da exaustão recirculando para a parte frontal dos equipamentos.	Coloque os equipamentos em um rack fechado com sistema de exaustão de ar quente e uma abertura na parte inferior da porta da sala.
> 1000W	Sem acesso a qualquer sistema de ar-condicionado. O prédio possui um ambiente uniformemente condicionado.	O movimento do ar através da porta não é suficiente. É necessário resfriamento local da exaustão de ar quente dos equipamentos.	Instale um condicionador de ar de precisão na sala e próximo aos equipamentos.

Tabela 2 – *Guia de soluções de resfriamento para salas de Telecom VoIP*

Por fim, o monitoramento ambiental (temperatura e umidade) para essas salas de Telecom é altamente recomendado, já que ajudarão na indicação de condições anormais, permitindo um tempo suficiente para tomar medidas proativas e evitar o tempo de parada dos equipamentos.

Diante de cálculos previamente realizados e quantidade de equipamentos da estruturação da NCPI, rede de telefonia e dados, servidores de telefonia IP e outros equipamentos chegamos

facilmente a uma carga maior que 1000W de potência, porém não excedendo os 10KW. Podemos classificar esse datacenter como de pequeno porte diante da carga de TI apresentada. Então devemos seguir a última orientação da tabela 2 em amarelo para a refrigeração do ambiente.

Refrigeração

A TC 9.9 da Sociedade Americana de Engenheiros de Aquecimento, Refrigeração e Ar-Condicionado (ASHRAE) publica as temperaturas de operação recomendadas e permitidas para equipamentos de TI. A intenção é fornecer uma melhor orientação para assegurar a confiabilidade e desempenho dos equipamentos, maximizando a eficiência do sistema de refrigeração. Esses valores das *Diretrizes Térmicas da ASHRAE* de 2011 para equipamentos classe 1 são fornecidos na **Tabela 3.**

Temperatura de operação	Faixa de Temperatura
Recomendada	**(18-27°C)**
Permitida	**(15-32°C)**

Tabela 3 – *Norma TC 9.9 da ASHRAE limites de temperatura de operação*

Energia

A alimentação para pequenos data centers consiste em um nobreak e a distribuição de energia. Os sistemas de nobreak para esta aplicação são geralmente de linha interativa para cargas de até 5 kVA e de dupla conversão para cargas acima de 5 kVA. Os sistemas de nobreak maiores que aproximadamente 6 kVA geralmente estão conectados fisicamente a partir de um painel elétrico. Orientações técnicas e definições sobre carga serão explanadas em sequência. Para o complexo regulador a proposta é de um nobreak online de dupla conversão de 6kVA.

Existem dois métodos básicos para distribuição desta energia:

1. Conectar os equipamentos de TI nas tomadas na parte traseira do nobreak.
2. Conectar os equipamentos de TI a um rack de distribuição de energia (PDU de rack), o qual é conectado ao nobreak. Este método requer que os equipamentos de TI sejam montados em um rack 19".

Quando utilizado com um rack, o gerenciamento de cabos de energia é mais fácil e mais organizado com PDUs de racks, uma vez que os cabos de energia não têm que se cruzar, conforme mostrado na **Figura 5.** Outra vantagem é que a parte traseira do rack permanece livre de cabos

de alimentação, o que melhora o fluxo de ar da frente para trás para a refrigeração dos equipamentos de TI. Nos casos em que o gerenciamento remoto das saídas é necessário, algumas PDUs de racks possuem medidores e saídas chaveadas que podem ser usadas para reinicializar remotamente os servidores.

Figura 5 *- Organização com PDU*

Sistemas de nobreak redundantes são recomendados para equipamentos críticos com dois cabos, tais como servidores, storages e networks. Certifique-se de que os cabos de alimentação redundantes estejam ligados a um nobreak ou a uma PDU de rack separados. A confiabilidade aumenta se cada nobreak estiver conectado a um circuito separado, onde cada circuito é alimentado a partir do seu próprio disjuntor. Recomenda-se os sistemas de nobreak com uma placa web de gerenciamento de rede integrada, pois permitem monitoramento remoto de nobreaks críticos, tais como carga baixa da bateria, bateria ruim, operação por bateria, sobrecarga, baixo tempo de execução, etc. Alarmes podem ser enviados por e-mail ou por um sistema de gerenciamento de rede NMS.

A mesma placa de gerenciamento pode ser utilizada para fornecer monitoramento ambiental. O ideal é que seja instalado pelo menos um sensor de temperatura do ar para controlar a temperatura de suprimento de ar na parte frontal do rack ou equipamento de TI. Sensores adicionais incluem um sensor único que mede tanto a temperatura quanto a umidade.

Nos casos em que a entrada na sala de servidores é necessária, um sensor de E/S de contato seco vai notificar os administradores quando a porta da sala do servidor for aberta. Outros sensores de contato seco incluem detecção de água. A **Figura 6** mostra um exemplo de um nobreak com estas características.

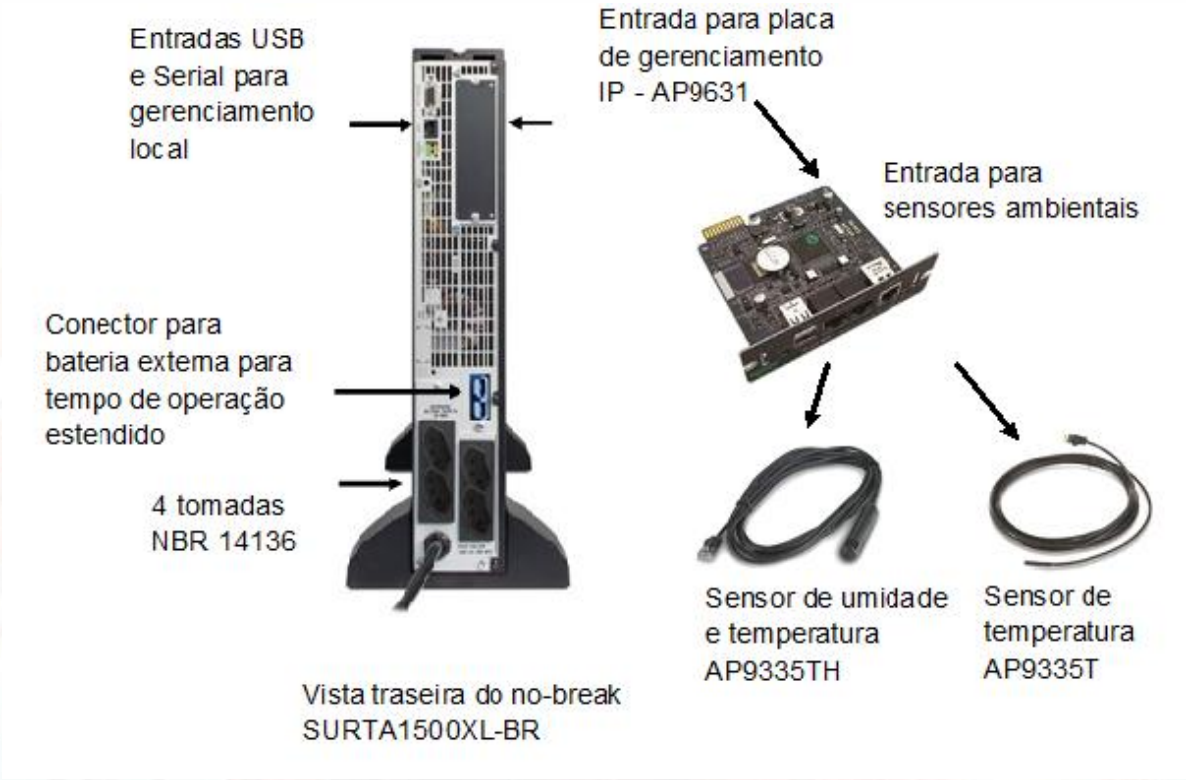


Figura 06 - *Nobreak tomadas padrão NBR 14136*

Segurança Física

Pessoas são essenciais às operações de TI, ainda que estudos mostrem consistentemente que pessoas são diretamente responsáveis por muito do tempo de inatividade, seja por acidentes ou por enganos — procedimentos inapropriados, equipamentos rotulados erroneamente, queda de substâncias e outros imprevistos.

Trancar uma sala de servidores ou gabinete de rack é fundamental caso o custo da paralisação for alto. Se um espaço de TI é considerado crítico, é recomendada a aplicação de câmeras de segurança. Algumas câmeras possuem sensores de ambiente integrados e portas

adicionais para vários tipos de sensores, incluindo contatos secos, detectores de fumaça, detectores de fluidos e interruptores da porta. Os sensores integrados deverão incluir detecção de temperatura, umidade e movimento.

Câmeras com detectores de movimento podem detectar e registrar movimentos automaticamente, permitindo que um registro visual seja combinado com um alerta de acesso ou ambiental, o que agiliza a análise da causa principal. Por exemplo, um administrador de TI pode ser alertado via SMS ou e-mail sobre o acesso por pessoas não autorizadas, através do interruptor da porta ou detecção de movimento. Câmeras irão permitir o acesso via smartphone para a exibição de imagens e dados do ambiente.

Figura 07 *– Câmera com visão noturna e gravação remota com detecção de movimento.*

Segundo a norma ANSI/TIA-942 a topologia do Data Center fica assim classificada:

- ***Entrace Room*** **(ER):** espaço de interconexão do cabeamento estruturado do Data Center e o cabeamento proveniente da telecomunicação.
- ***Main Distribution Area*** **(MDA):** local onde se encontra a conexão central do Data Center e de onde se distribui o cabeamento estruturado, incluindo roteadores e *backbone*.
- ***Horizontal Distribution Area*** **(HDA):** área utilizada para conexão com a área de equipamentos, incluindo o *cross conect* horizontal, equipamentos intermediários, LAN (*Local area network*), SAN (*Storage Area Networks*) e KVM (*Keyboard, Video, Mouse*) switches.
- ***Zone Distribution Area*** **(ZDA):** ponto de interconexão opcional do cabeamento horizontal. Fica entre HDA e o EDA, provê flexibilidade no Data Center.
- ***Equipment Distribution Area*** **(EDA):** área destinada para os equipamentos terminais (servidores, *storages*, unidades de fita), inclui também os *Racks*, gabinetes e equipamentos de comunicação de dados ou voz.

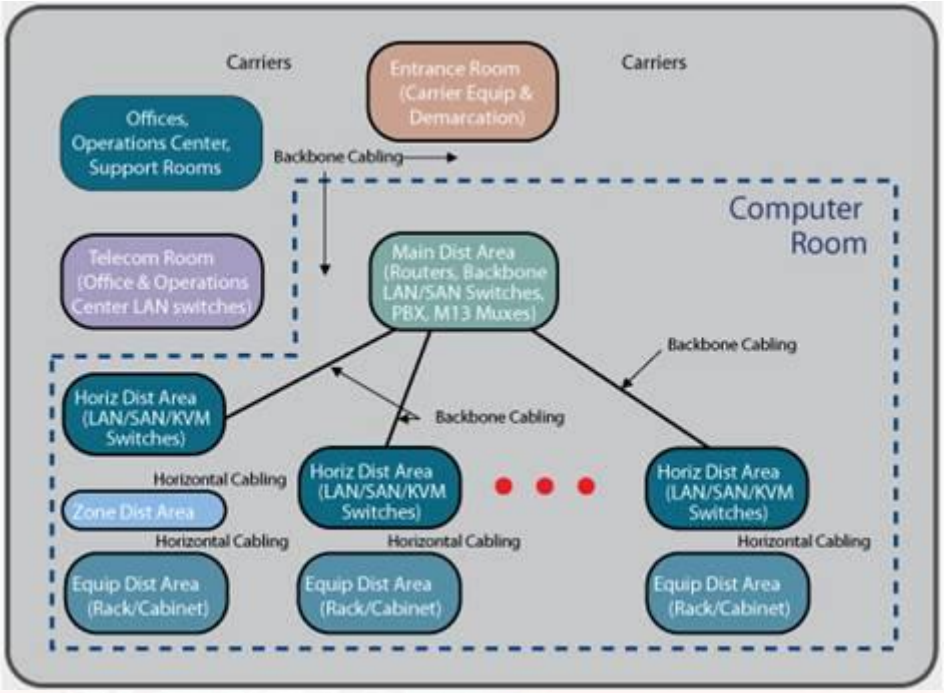


Figura 08 - *Diagrama Básico de um Data Center.*

Obedecendo a norma e suas classificações de disponibilidade de serviço temos um pequeno Data Center Tier 2 de carga de até 6kVA.

Tier 2 – Componentes Redundantes

De acordo com a Furukawa, no Tier 2 os equipamentos de telecomunicações do Data Center e os equipamentos da operadora de telecomunicação, assim como os comutadores LAN-SAN, devem ter os seus módulos redundantes. O cabeamento do *backbone* principal LAN e SAN das áreas de distribuição para os comutadores devem ter cabeamento redundante, par metálico ou fibra.

Devem ter duas caixas de acesso de telecomunicação e dois caminhos de entrada até a ER com no mínimo 20 metros.

No Tier 2 é necessário prover módulos UPS (*Uninterruptible Power Supply*) redundantes para N+1 e um sistema de gerador elétrico para suprir a carga, não é necessária redundância na entrada do serviço de distribuição de energia. O sistema de ar-condicionado deve ser projetado para ter o funcionamento contínuo de 24x7x365, com no mínimo a redundância de N+1.

Os possíveis pontos de falha dessa classificação são:

- Falhas no sistema de refrigeração ou de energia podem ocasionar falhas nos outros componentes do Data Center.

O Tier 2 possui uma disponibilidade de 99.749%, pode ter um *downtime* de 22 horas/ano e redundância parcial em energia e refrigeração. Em face de limitações estruturais das unidades e ou prédios onde os complexos reguladores do SAMU são implantados, uma classificação Tier 3 ou 4 se torna impossível ou muito onerosa.

MDF - Main Distribution Frame (Ambiente de Distribuição principal)

O MDF também é chamado de salas MERs (main equipment rooms – salas de equipamentos principais) ou POP (point of ping or presence – ponto de ping ou presença). Ele incorpora os equipamentos de Telefonia IP mais críticos, como roteadores da camada 3, switches e uma variedade de outros equipamentos de telecomunicações, TI e rede (Figura 9). As linhas E1 e conectividade IP de provedores, normalmente chegam no MDF e fornecem conectividade à espinha dorsal da internet e ao STFC (sistema de telefonia fixa comutada).

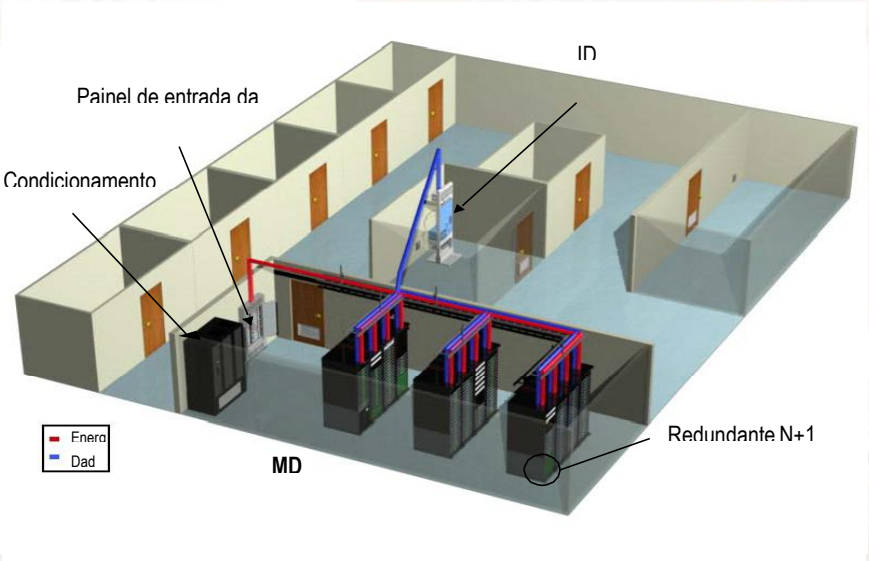


Figura 09 – *MDF.*

Ambiente

Os MDFs geralmente estão localizados no térreo ou primeiro andar, fornecendo a entrada de serviços do prédio. Um MDF típico pode ter de 4 a 12 racks de equipamentos e consumir de 4 kW a 40 kW de energia monofásica ou trifásica. Alguns equipamentos podem necessitar de energia –48VCC. A maioria dos racks em MDFs são abertos, usados para montar uma grande variedade de equipamentos de TI e Telefonia IP. Estes equipamentos podem ter diferentes padrões de ventilação; lado a lado, de frente para trás, etc., e podem ser de 19" ou 23". Entretanto, a maioria dos equipamentos de TI e Telefonia IP são de montagem em rack de 19".

Desafios

Alguns MDFs não tem um nobreak, muitos não têm tempo de autonomia adequado e muitas vezes podem não ter um sistema de ar refrigerado de precisão.

Melhores Práticas

Já que esses MDFs contém uma variedade de equipamentos de rede e telefonia IP críticos, eles devem ser tratados como um pequeno Data Center ou Sala de Servidores. Para obter aproximadamente cinco noves de disponibilidade de energia, um MDF deveria ser protegido por um Nobreak redundante e modular com by-pass interno e ao menos com trinta minutos de autonomia. Maiores autonomias e altos níveis de disponibilidade, como seis ou sete noves, podem ser alcançados com o uso de switches redundantes com fontes duplas, Nobreak redundante, e arquiteturas elétricas projetadas de modo concorrente e com gerador.

Os MDFs devem ter suas próprias unidades de condicionamento de ar de precisão com monitoramento ambiental. Unidades de condicionamento de ar redundantes, deveriam ser consideradas para aplicações críticas que necessitem de alta disponibilidade. Para racks com alta densidade de energia (> 3 kW/Rack), unidades adicionais de remoção e distribuição de ar devem ser usadas para evitar pontos quentes. Diferente de dispositivos de armazenamento e servidores, muitos switches têm o fluxo de ar lado a lado. Isso cria situações especiais numa instalação em um ambiente que usa racks anexos. Situação similar ao posicionamento dos racks adotados no croqui exemplo figura 3c.

Data Center ou Sala de Servidores

No Data Center ou Sala de Servidores (Figura 10) estão todos os servidores de aplicação para telefonia IP com seu software (Asterisk, Bilhetagem, BD etc.). Além disso, baseado na arquitetura de rede e no tamanho da organização, ele pode também armazenar os switches centrais (camada 3) e switches de distribuição (camada 2). Dependendo do seu tamanho (pequeno, médio ou grande), um Data Center ou Sala de Servidores pode conter de dezenas a centenas de racks, carregados com dezenas ou centenas de servidores e uma variedade de sistemas de computação e rede de TI rodando aplicações de negócios críticas como ERP, CRM, Firewalls e outros serviços Web.

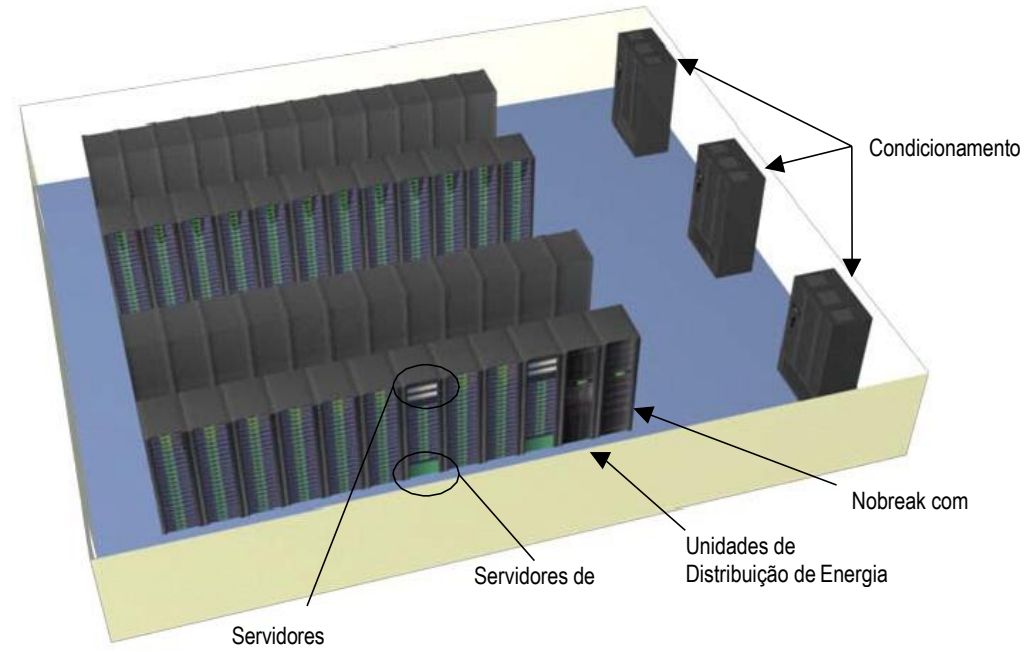


Figura 10 *– Data Center ou sala de servidores típico.*

Ambiente

Os Data Centers estão geralmente localizados no escritório corporativo drenando de 10 kW de energia monofásica ou trifásica a centenas de kilowatts de energia trifásica. Pode haver alguns pequenos requisitos de energia DC –48V para algumas cargas de telecomunicações, mas predominantemente todas as cargas serão de energia AC. A maioria dos Data Centers tem um Nobreak com bateria, gerador e unidades de condicionador de ar de precisão.

Desafios

Switches e servidores de Telefonia IP são basicamente carga incremental incidental ao Data Center, que podem exigir uma autonomia, redundância e disponibilidade maiores que outros equipamentos de rede e TI.

Melhores Práticas

Embora o Data Center possa ter seu próprio Nobreak ou gerador, muitas vezes pode ser apropriado implementar um Nobreak redundante separado com maior tempo de autonomia para o equipamento de Telefonia IP. O correto é identificar e agrupar os equipamentos de Telefonia IP que necessitem uma autonomia e uma disponibilidade maior em uma área separada, em racks separados dentro do Data Center. Após isso, é recomendado um Nobreak dedicado com uma

autonomia maior e uma disponibilidade N+1, N+2, conforme necessário. O conceito de "Disponibilidade Alvo" ajuda a aumentar a disponibilidade dos equipamentos críticos de telefonia IP para os negócios sem incorrer num gasto enorme de capital para o Data Center inteiro. Altos níveis de redundância como alimentações duplas, geradores redundantes e Nobreaks redundantes N+1 com caminhos de energia redundantes até o servidor e outros equipamentos críticos no rack podem ser considerados para redes e Data Centers com elevado nível de disponibilidade.

Deve ser assegurado, que o equipamento de ar-condicionado de precisão do Data Center tenha capacidade de resfriamento suficiente para a nova Central de Telefonia IP adicional. Unidades de condicionamento de ar redundante podem ser consideradas para maiores disponibilidades. Para racks de alta densidade (> 3kW/Rack), unidades de remoção de ar e distribuição de ar adicionais deveriam ser usadas para evitar pontos quentes. Erros que podem ser evitados e são cometidos rotineiramente ao instalar sistemas de resfriamento e racks em Data Centers ou salas de rede comprometem a disponibilidade e aumentam os custos.

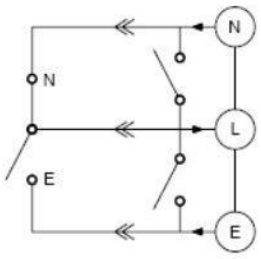
Considerações Finais

Na execução da implantação da estrutura tecnológica do complexo regulador do SAMU, tanto as normas para a NCPI quanto para o Data Center Tier 2, se misturam e se complementam em conceito e definições operacionais. Como a realidade das instalações físicas não permitem a plena implementação de tudo que foi exposto em projeto, é comum e aceitável que todos os layers da NCPI, como também a topologia da ANSI/TIA-942, se misturem em uma única sala, porém respeitando todas as diretrizes aqui esplanadas e definidas. O apêndice 1 fornece as devidas orientações como a configuração da alimentação concessionária, gerador e UPS devem estar dispostos a fim de garantir alimentação contínua às cargas de missão crítica (central de telefonia IP e sistemas de apoio) do complexo regulador.

Apêndice 1

É importante notar que, para as aplicações de suprimento de energia para cargas críticas, a Chave de Transferência Automática (ATS) deve ser dotada de by-pass com a finalidade de não comprometer a disponibilidade do sistema nos casos de manutenção ou reparo no quadro de transferência do grupo gerador **(figura 11).**

Preferencialmente, deve ser do tipo extraível, permitindo remoção e instalação rápidas, sem interrupção no suprimento de energia. Este item tem sido motivo de falhas que acarretaram paralisações prolongadas em muitas instalações, em consequência de servir como elemento de interrupção das fontes principal e de emergência.



N = Fonte principal (rede)

L = Carga

E = Emergência (gerador)

Figura 11 *– ATS com by-pass.*

As unidades UPS referenciadas como componentes de sistemas de energia segura, para os efeitos deste projeto, são as unidades padrão, de dupla conversão disponíveis no mercado, com a configuração básica a seguir. As opções de potências e características construtivas são ilimitadas. Cada fabricante pode disponibilizar modelos e configurações conforme suas conveniências e interesses do usuário final. (Figura 12).

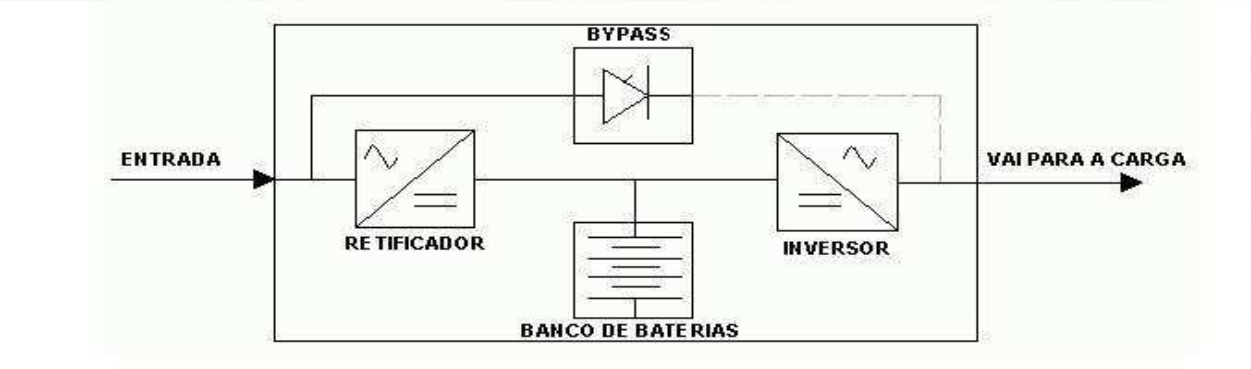


Figura 12 *- UPS CONFIGURAÇÃO PADRÃO.*

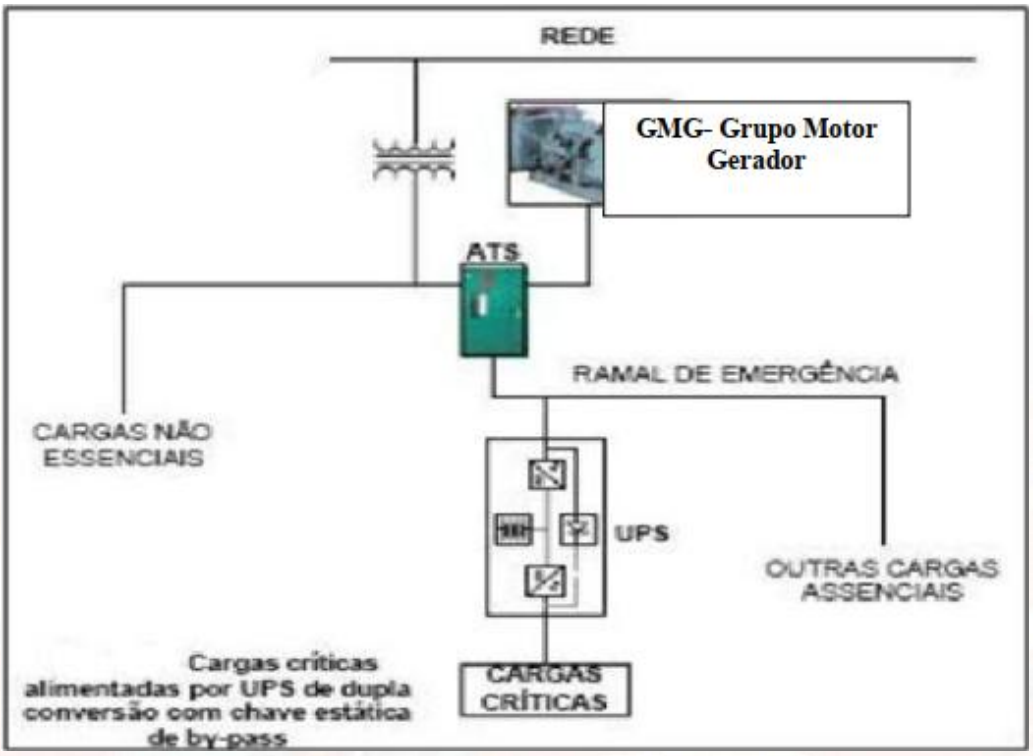


Figura 13 - *Conceito básico de suprimento de energia para cargas críticas*

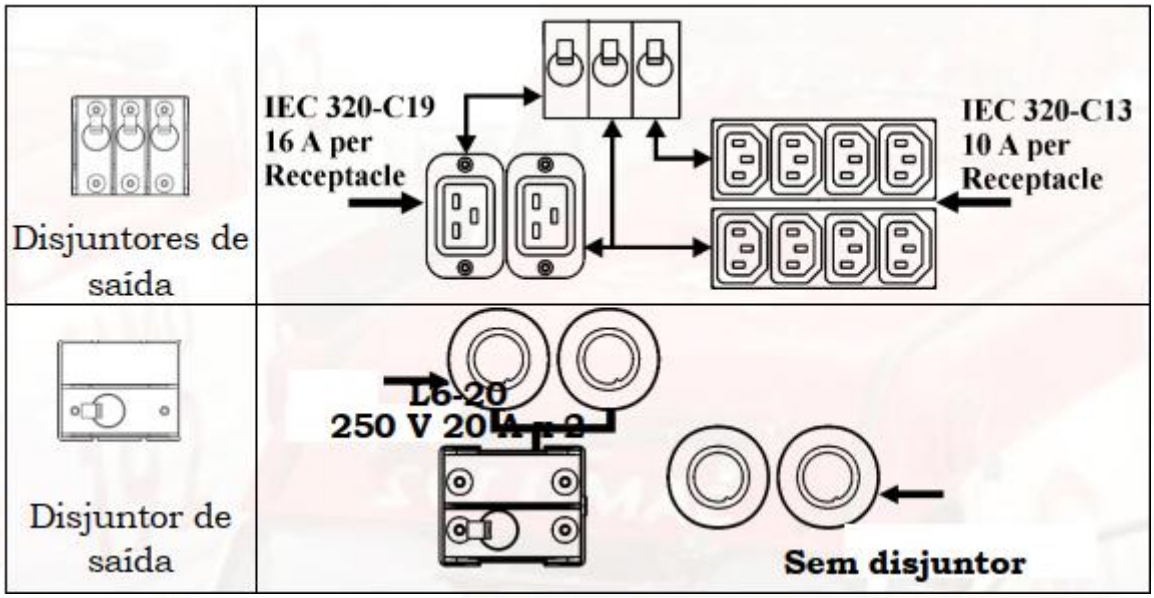
Atendendo aos dispositivos gerais de instalação do nobreak selecionado segundo o manual, temos:

Entrada

INSTRUÇÕES SOBRE CABEAMENTO:

- Cabeamento deve ser feito por um eletricista qualificado.
- Instale um disjuntor magnético de alta proteção de 30/32 A.
- Siga todas as normas e códigos de eletricidade nacionais e locais. NBR 5410
- Use cabo de bitola 10 AWG (5 mm²).

Saída



Aterramento Geral

A norma que rege este dimensionamento é a NBR-5410:2004. Deve ser seguida na confecção, teste e/ou aceitação do aterramento para implantação do projeto.

1.1.4. Segmentação da rede

Por questões de segurança, otimização da operação e resolução de problemas atendendo aos requisitos para uma NCPI, a rede foi dividida em 3 layers distintos, atendendo as disposições das normas descritas.

Como veia da informação, a rede, deve trafegar a mesma de forma segura, livre, sem gargalos e com o desempenho máximo permitido, garantindo a todos os componentes de sua estrutura de acesso rápido e sem perdas aos dados e a qualquer momento, 24 horas por dia, 365 dias no ano. Para permitir essa sustentabilidade, agilidade e confiabilidade sendo transparente as aplicações e se tornando altamente gerida por seus administradores, a rede deve seguir alguns conceitos.

Deve ser constituída por um sistema de cabos, fibras ou acesso sem fio que siga as normas IEEE 802.3 (última atualização 802.3-2022) (http://en.wikipedia.org/wiki/IEEE_802.3) e seus padrões subsequentes e as normas IEEE 802.1 (http://en.wikipedia.org/wiki/IEEE_802.1) e seus padrões subsequentes.

Sendo que para o padrão IEEE 802.3 que define o layer físico da rede, layer de link de dados, MAC de uma rede cabeada ethernet, temos um padrão equivalente ANSI/TIA/EIA.

O padrão de conexão física mais adotado e popularmente conhecido é o CAT 5E

(EIA/TIA-568-B) o qual deverá ser adotado em toda a confecção da infraestrutura, para se ter uma rede padronizada e normatizada podendo alcançar a velocidade de 100 Mbps como estabelece a norma para o padrão. Mas podendo ela atingir velocidade de até 1 Gbps, obedecendo os padrões IEEE 802.3ab para Gigabit Ethernet sobre rede de cabos de par trançado CAT 5, 5e e 6.

Deve seguir a topologia estrela ou malha e respeitar as normatizações para o protocolo TCP/ IP ver 4.0, além de ter suporte ao protocolo TCP/IP versão 6 que será usado no futuro, suporte ao protocolo de gestão de rede SNMP (Simple Network Management Protocol), suporte a QoS e Vlan e deve permitir aos gestores o controle de acesso de equipamentos a rede por MAC, IP ou regras semelhantes.

Todas essas características compõem o principal elemento de uma rede, a Switch LAYER 2 em algumas topologias mais simples e/ou Switches LAYER 3 em diante com topologias mais complexas.

A Switch é o elemento interligador da rede e une os elementos ativos em uma estrutura hierárquica, controlada e organizada seguindo o modelo OSI (Modelo de Sistema Aberto de Interconexão), subdividido em 7 níveis ou layers.

Os outros elementos como cabos, conectores e patch panels seguem a orientação do padrão ANSI/TIA/EIA 568-B e suas normativas correlatas para aterramento e estruturação do ambiente.

A justificativa para segmentação de rede é clara. Quando tratamos de um ambiente totalmente organizado e gerenciado, deparamos com dois conceitos bem distintos. A organização lógica: definição dos IPs, estrutura da árvore de diretórios, definição da lista de acesso e permissões, definição dos compartilhamentos, políticas de segurança, permissões de usuários, entre outros. A organização física: disposição dos equipamentos e dispositivos na rede, parametrização física dos Servidores e Firewalls que darão suporte a toda infraestrutura, definição do hardware de abrigo dos servidores, definição dos sistemas energéticos e de refrigeração entre outros.

Para que nosso objetivo não fique distanciado e para que possamos ter sucesso nessas colocações, faremos aqui algumas considerações pertinentes a esse desenvolvimento, porém dando abertura para que o executor do projeto escolha entre tantas opções, as que melhor se enquadrem em sua realidade. Vale lembrar que alguns pontos comuns devem ser respeitados e adotados para que o ambiente fique o mais próximo possível do que é aplicado hoje em dia.

1.1.4.1 Telefonia/ Suporte (NCPI)

Os IPS na rede Telefonia/ Suporte (NCPI) são os endereços de identificação de cada

equipamento de forma individual e servem para estabelecer um vínculo universal entre todos os elementos. Responsáveis também pela organização, seguem as definições do protocolo TCP/IP que diferente do OSI possui apenas 5 camadas.

Uma rede bem definida, deve ter a designação de seus IPS em uma tabela de acordo com o tamanho da rede e com a perspectiva de crescimento futuro. Então baseado no projeto, definimos uma rede com máscara /24 de 256 IPS distintos classe A, sendo servida pelo gateway router principal, através de protocolo DHCP. Esta rede alimentará todos os elementos principais da infraestrutura da NCPI Telefonia/Suporte, sendo eles, todos os telefones IP, servidores, gateways de comunicação, Storages de armazenamento, e etc., irá operar na Vlan 01 (Vlan default de rede) e será exclusiva ao funcionamento desse serviço, ficando isolada das outras redes. Abaixo segue exemplo de endereçamento:

FAIXA DE IP 10.0.1.0 MÁSCARA DE REDE 255.255.255.0 GW PADRÃO OU IP DO SERVIDOR 10.0.1.1.

1.1.4.2 Regulação (NCPI)

Os IPS na rede Regulação (NCPI) são os endereços de identificação de cada equipamento de forma individual e servem para estabelecer um vínculo universal entre todos os elementos. Responsáveis também pela organização, seguem as definições do protocolo TCP/IP que diferente do OSI possui apenas 5 camadas.

Uma rede bem definida, deve ter a designação de seus IPS em uma tabela de acordo com o tamanho da rede e com a perspectiva de crescimento futuro. Então baseado no projeto, definimos uma rede com máscara /24 de 256 IPS distintos classe C sendo servida pelo Firewall Regulação através de protocolo DHCP com endereçamento estático. Esta rede alimentará todos os elementos principais da infraestrutura da NCPI Regulação, sendo eles, todos os computadores e/ou elementos de apoio na regulação do SAMU, como servidores de softwares específicos, painéis de informação e etc., irá operar na Vlan 888 (Vlan específica de rede) e será exclusiva ao funcionamento desse serviço, ficando isolada das outras redes. Abaixo segue exemplo de endereçamento

FAIXA DE IP 192.168.1.0 MÁSCARA DE REDE 255.255.255.0 GW PADRÃO OU IP DO SERVIDOR 192.168.1.1

1.1.4.3. Administrativo

Os IPS na rede Administrativo são os endereços de identificação de cada equipamento de forma individual e servem para estabelecer um vínculo universal entre todos os elementos. Responsáveis também pela organização, seguem as definições do protocolo TCP/IP que diferente do OSI possui apenas 5 camadas.

Uma rede bem definida, deve ter a designação de seus IPS em uma tabela de acordo com o tamanho da rede e com a perspectiva de crescimento futuro. Então baseado no

projeto, definimos uma rede com máscara /24 de 256 IPS distintos classe C sendo servida pelo Firewall Administrativo através de protocolo DHCP com endereçamento estático. Esta rede alimentará todos os elementos principais da infraestrutura da rede Administrativo, sendo eles, todos os computadores e/ou elementos de apoio como servidores de softwares específicos, impressoras, servidores de compartilhamento, ERP, CRM e etc., irá operar na Vlan 889 (Vlan específica de rede) e será exclusiva ao funcionamento desse serviço, ficando isolada das outras redes. Abaixo segue modelo de endereçamento

FAIXA DE IP 192.168.2.0 MÁSCARA DE REDE 255.255.255.0 GW PADRÃO OU IP DO SERVIDOR 192.168.2.1.

Por se tratar de uma rede onde uma gama maior de serviços e sistemas irão funcionar, mesmo estes não sendo considerados críticos ao complexo regulador, cabe aqui uma atenção para alguns pontos de definição explanados abaixo:

1.1.4.4. Definições da Rede

COMPARTILHAMENTOS

Deve ser definido sob uma plataforma servidora, que será adotada no controle da rede e seus usuários para esse fim. No ambiente pode-se defini-lo com o uso do Windows Server 2022 x64 virtualizado, que nativamente possui suporte a todos esses recursos. Caso seja opção o uso do Linux como gestor, o serviço SAMBA poderá ser usado para compartilhamentos compatíveis com Windows e o NFS como compartilhamento nativo Linux. O compartilhamento de arquivos é uma prática comum nas redes administrativas e deve ser realizado com moderação e somente pelos gestores da infraestrutura. Compartilhamentos mal executados com permissões de acesso erradas, podem ocasionar vazamento de informações sigilosas da administração.

DOMÍNIO INTERNO

Deve ser definido em cima da plataforma servidora que será adotada no controle da rede e seus usuários para esse fim. No ambiente pode-se defini-lo com o uso do Windows Server 2022 x64 virtualizado, que nativamente possui suporte a todos esses recursos. O domínio interno é uma opção, mas que obrigatoriamente não precisa ser implantada. Muito usado caso a gestão opte pela implantação de um Diretório Ativo, no controle de acesso às máquinas administrativas do complexo regulador.

SERVIDOR DHCP

O servidor DHCP nessa rede Administrativa ficou a cargo do Firewall UTM, que será configurado para controle total da planta. Todas as requisições de IP e acesso a rede passam por ele. Mecanismos de controle serão aplicados para impedir o acesso indevido à rede.

SERVIDOR DE IMPRESSÃO

Deve ser definido em cima da plataforma servidora que será adotada no controle da rede e seus usuários para esse fim. No ambiente pode-se defini-lo com o uso do Windows Server 2022 x64 virtualizado, que nativamente possui suporte a todos esses recursos. Os servidores de impressão podem também ser substituídos pela combinação de uso dos recursos das impressoras em rede. Caso a impressora possua esse recurso, pode-se instalá-la exclusivamente para um ou outro departamento renunciando ao uso do servidor. Cabe a ressalva que, o uso de servidores de impressão melhora a gestão desse tipo de recurso e o monitoramento do uso e dos gastos é mais eficiente.

1.1.5. Segurança/Firewall

As políticas de segurança e bloqueio de acesso a conteúdo não permitido, bem como a proteção da integridade dos dados e sistemas são tarefas do Firewall. Um sistema de Firewall bem elaborado, juntamente com regras de utilização e controle bem definidas, permite ao gestor de TI e consequentemente ao SAMU, uma operação sem sustos. Livrando a rede de ataques e contaminações pelas diversas pragas eletrônicas, vírus, cavalos de Tróia, worms e outros.

O Firewall atualmente, não é somente uma ferramenta de defesa, mas sim uma arma de controle e gestão complexa, agregando diversos recursos como controle ativo de banda, relatórios de uso de recurso de rede, acesso diferenciado por classificação de usuário, balanceamento de links e demais funções usadas para uma ampla atuação na administração e controle do ambiente de TI. Seguindo essa tendência e aplicando as mais novas tecnologias de Firewall, será necessária uma solução virtualizada, sendo possível a adoção de diversas distribuições LINUX preparadas para este fim. Algumas sugestões vão desde soluções livres como IPCOP ou PFsense, até soluções comerciais de baixo custo de aquisição como Untangle e Sophos UTM.

As definições para implantação dessa tecnologia de segurança são baseadas no conceito de Firewall de Nova Geração (Next Generation Firewall - NGFW). Tanto o firewall da rede da Regulação (NCPI) e do Administrativo serão virtualizados e trabalharão em domínios broadcast diferentes separados por suas respectivas VLANS no atendimento aos seus clientes. A interfaces LAN às quais alimentam as redes internas estarão conectadas a switches camada três com tagueamento de pacotes para distinção das VLANS. As interfaces WAN dos dois firewalls serão alimentadas pelo router/ gateway principal que se encontra na rede Telefonia/ Suporte (NCPI).

Dessa maneira teremos uma tripla camada de segurança e gerência individual de cada rede. A virtualização da solução de segurança garante amplitude de recursos e opção de escolha, já que se pode trocar de soluções sem ter que desfazer do investimento em hardware.

1.1.6. Virtualização

O projeto de estruturação do ambiente de TI tem como premissa a virtualização de Servidores de Serviços e de Firewalls. A virtualização é hoje a principal ferramenta de desenvolvimento e implantação de novas estruturas. Permitindo fazer mais com menos e gerando uma economia significativa de energia, temos na virtualização o futuro de toda planta de TI.

Além de permitir mobilidade de seus ativos, segurança aprimorada e facilidade na manipulação dos recursos, a virtualização garante a total redundância de suas operações, uma vez que podemos mover qualquer servidor virtual entre os hospedeiros e manter o funcionamento da estrutura, já que as cópias de segurança são clones idênticos das máquinas em operação. Um servidor de virtualização permite o aumento dos recursos na rede, como mais servidores e aplicações virtuais sem aumentar ou adquirir hardware físico. Em muitos é possível uma relação de até 7 máquinas virtualizadas por núcleo de processador. Ficando o limite apenas na quantidade de memória RAM e disco da máquina hospedeira.

No mercado existem duas soluções líderes e concorrentes que atendem de forma satisfatória as necessidades de uma virtualização. Citrix Xen Server e VMware ESXi compõem a melhor relação custo-benefício se comparadas a tecnologias semelhantes. Suas soluções são livres de licença, gratuitas para uso em pequenos e médios empreendimentos.

Para virtualização, a definição dos parâmetros técnicos do Servidor hospedeiro deve ser realizada com cautela e entendimento. Listas de compatibilidade de hardware (HCLs) e outros requisitos dos softwares de virtualização, devem ser respeitados e seguidos. A máquina hospedeira ou Servidor Principal deve ter recursos de hardware suficientes para funcionar com uma folga mínima de 50% de sua capacidade, mantendo uma margem de segurança na operação. Deve ter recursos de redundância de disco e fonte para garantia de integridade dos dados das máquinas virtuais, possuir ferramentas embarcadas de gestão remota via console ou acesso a rede independente do compartilhado com os usuários. Esse acesso deve contemplar segurança e criptografia permitindo ao gestor acessar e diagnosticar qualquer eventual problema em sua estrutura.

O servidor de virtualização deverá permitir a criação de no mínimo 3 máquinas virtuais, sendo que duas delas deverão ter 4GB de RAM, duas interfaces de rede, 80 GB de disco e separação física entre as interfaces além de suporte a tag vlan. Essas máquinas serão os firewalls aqui citados. A terceira máquina deverá ter 4GB de RAM e 120 GB de disco para abrigar um servidor de serviço e suporte para gestão interna das redes.

A utilização da virtualização de servidores traz alguns benefícios para o projeto, dentre eles:

- Redução de downtime: Eliminação de paradas de ambiente de produção; Prevenção de perda de dados; Prevenção de downtimes não planejados.

- Automação e gerenciamento: Sistemas de gerenciamento centralizado de máquinas virtuais com interface amigável e intuitiva; Gerenciamento de ambiente de produção e homologação; Gerenciamento de implantação; Gerenciamento de atualização de versões de softwares e firmwares.
- Otimização da Infraestrutura: Pesquisas apontam que a utilização de servidores convencionais é em torno de 5 – 20%, através da virtualização essa taxa fica em torno de 65% - 90%; Maior ROI; Redução de até 40% de custo operacional; Com Virtualização de Servidores é obtido menor TCO de servidores; Melhor Gerenciamento; Otimização de infraestrutura, espaço físico e maximização da utilização de recursos; Redundância em caso de falha de Hardware, Virtualização de Servidores, o ambiente virtualizado migra as máquinas virtuais para os demais servidores virtualizados.

Todas as referências técnicas de projeto, podem ser consultadas nos sites dos criadores dos softwares de virtualização, bem como para consulta e comparação, podem ser obtidas através do endereço eletrônico. https://www.whatmatrix.com/comparison/Virtualization.

1.1.7. Integração

Umas das ferramentas de grande importância quando falamos de integração, é a possibilidade de unificar a comunicação com outras centrais de outros SAMUs. Essa integração tem a missão de permitir de forma transparente a comunicação entre elas, via rede segura e assim permitir a criação de uma rede universal de atendimento e colaboração.

A integração cria a rede de abrangência necessária e permite aos gestores de saúde uma comunicação direta com os complexos reguladores via rede privada de comunicação e torna possível a elaboração de arranjos operacionais amplos em caso de gestão de catástrofes. Um exemplo prático, uma determinada região do estado foi atingida por um fenômeno natural meteorológico e não possui mais comunicação telefônica. Neste ponto, a gestão central pode rearranjar outras centrais reguladoras em uma única operação conjunta integrada via rede segura e obter a gestão coordenada das ações. Para isso deve-se usar como ferramenta de integração, o protocolo de rede virtual privada baseado em openssl (openvpn) definido, gerido e configurado via hardware router/gateway de borda que se encontra na gestão da rede de Telefonia/Suporte (NCPI). A escolha do openvpn se dá pelas seguintes razões técnicas:

- Pode-se criar túnel de qualquer sub-rede IP ou adaptador Ethernet virtual através de uma única porta UDP ou TCP;
- Configurar um farm escalável, com balanceamento de carga VPN, servidor usando uma ou mais máquinas que podem lidar com milhares de ligações dinâmicas de clientes VPN de entrada.
- Usar todos os recursos de criptografia, autenticação e certificação da biblioteca OpenSSL para proteger o tráfego de rede privada, uma vez que transita pela internet.
- Usar qualquer cifra, tamanho da chave, ou HMAC digest (para verificação de integridade de datagrama) suportado pela biblioteca OpenSSL,

- Escolher entre criptografia convencional baseada em chave estática ou criptografia de chave pública baseada em certificado.
- Usar, chaves pré-compartilhadas estáticas ou troca de chave dinâmica baseada em TLS.
- Usar compressão adaptativa em tempo real de link e traffic shaping para gerir utilização de banda em link.
- Criar redes de túneis cujos terminais públicos são dinâmicos, como DHCP ou dial-in clientes.
- Criar redes de túneis através de firewalls stateful orientados a conexão sem ter que usar regras de firewall explícitas.
- Criar redes de túneis através de NAT.
- Criar pontes Ethernet seguras usando adaptadores virtuais (dispositivos TAP).
- Ter controle de OpenVPN usando uma GUI no Windows ou Mac OS X ou Linux.

1.2 CENTRAL TELEFÔNICA

1.2.1. Objetivo

Implantação e configuração de Central Telefônica IP (Internet Protocol) de alta disponibilidade baseado em PBX IP na plataforma ASTERISK. A opção por um sistema de telefonia baseado na plataforma ASTERISK justifica-se por ser um programa de código aberto que funciona no sistema operacional Linux, o que o torna flexível à medida que permite a sua constante evolução por profissionais de software livre, além de oferecer várias ferramentas livres.

O ASTERISK é um software que oferece vários recursos de comunicação e garante a expansão futura do sistema, sem a necessidade de troca da central de telefonia, podendo-se apenas efetuar a inclusão de novos ramais e configurá-los ao sistema, sem a necessidade de se obter novas licenças de software, para cada novo ramal disponibilizado. A tecnologia inclui funcionalidades avançadas de comunicações e, também, proporciona uma significativa liberdade, além da escalabilidade e robustez.

Além de todas essas vantagens, existe hoje no mercado várias empresas que prestam serviços utilizando esta plataforma, tornando assim a concorrência e a prestação de serviço bem mais ampla do que um sistema proprietário, além de uma vasta documentação disponível na internet, o que permite a capacitação de equipes multidisciplinares, permitindo o PCN - Plano de Continuidade do Negócio em conformidade com a ISO 22301.

1.2.2. O SISTEMA PBX IP

O termo PBX vem do inglês 'Private Branch Exchange' que significa a troca automática de ramais privados. Com a evolução tecnológica, os sistemas passaram a operar em plataformas de rede através do protocolo IP, pois todo o processo passou a ser controlado por sistemas operacionais e softwares, cuja o principal objetivo, era romper as barreiras da comunicação através das redes de dados ou da Internet. A partir deste princípio, as antigas centrais de comutação, ou

melhor, o PBX, evoluiu com o objetivo de utilizar essa rede, para integrar matriz e filiais com o menor custo. A plataforma de sistema PBX IP deve permitir o controle e o processamento da capacidade máxima de terminais SIP, gateways e troncos analógicos, digitais e GSM, conforme especificação e dimensionamento de hardware para o servidor.

O sistema PBX IP deverá ser capaz de realizar a bilhetagem total prevista no sistema; solução desenvolvida em SIP nativamente, denominado PBX IP, em conformidade com a RFC 3261 (Especificações do SIP: Session Initiation Protocol); realização de adaptação de protocolos para controle das chamadas SIP; possuir disponibilidade de uso de terminais SIP e gateways de qualquer fabricante, desde que suportem e atendam a RFC 3261; deve possuir estrutura de rede baseada em IP (Internet Protocol), TCP (Transmission Control Protocol) e UDP (User Datagram Protocol); utilização de sistemas de backup para recuperação da base de dados quando necessário, visando gestão de continuidade; o sistema PBX IP deve atuar como SIP Proxy Server e SIP Register Server, possibilitando o registro de ramais IP e gateways, além de controle do roteamento de chamadas de qualquer entidade SIP; suporte a gateways analógicos ATA utilizando protocolo SIP; suporte a sistemas de contingência para sinalização de troncos E1 de voz (RDSI/ISDN e R2); suporte a protocolos IAX 2, H.323, MGCP (Media Gateway Control Protocol), SCCP (Skinny Client Control Protocol); solução independente dos modelos dos dispositivos de rede, ou seja, garante as mesmas funcionalidades independente do fabricante dos ativos de rede, desde que a infraestrutura existente ofereça recursos mínimos de controle de qualidade de serviços - QoS (banda, jitter, delay e perda de pacotes); suporte a integrações com serviços de rede DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System), e NTP (Network Time Protocol); possibilidade de integração de múltiplos servidores para distribuição de carga, configuração de alta disponibilidade em dois servidores PBX IP, processamento e roteamento de voz entre localidades geográficas distintas; utilização de sistema operacional Open Source Linux.

Além dos requisitos básicos conforme parágrafo anterior, o sistema deverá conter gerenciamento completo do PBX IP em produção via Web, inclusive de novos servidores ASTERISK, através de plataforma única; Deverá ser implantada uma única plataforma WEB (Centralizada) capaz de gerenciar, alterar e configurar todo o servidor ASTERISK implantado dentro da rede do SAMU, permitindo a criação ou exclusão de ramais e a emissão de relatórios de tarifação centralizada; Disponibilidade de visualização completa do estado momentâneo (status) dos ramais mediante login e senha; Relógio de tempo real a fim de se manter o horário correto para serviços de despertador, hora certa, e bilhetagem; Numeração dos ramais programáveis para qualquer número; Proteção de programação: uso de memória flash; Siga-me interno e externo; Transferência e estacionamento das chamadas; Captura de chamadas de

grupo de captura ou ramal especifico; Desvio de chamadas não atendidas/ocupadas; Estacionamento de ligações; Chamada em espera; Limitador de duração de chamadas; Grupos de ramais; Voicemail (Correio de voz no e-mail e/ou telefone); Salas de Conferência; Codecs: G.711 fatores μ e A, G.729, G.722, ilbc, GSM; Habilitação de senha de utilização por usuário, possibilitando

a utilização de qualquer ramal interno e externo mediante utilização de senha pessoal; Identificador de chamadas (BINA – Sinalizações ISDN/R2 Digital); Supervisão de Chamadas / Monitoração de ramais (Escuta oculta sigilosa); Segmentação de Grupo de Chamadas (Local / DDD/ DDI/ Celular); Programação de DAC (Distribuidor Automático de Chamadas); Criação de agentes em filas de atendimento; Programação de Recebimento/Bloqueio de Chamadas Simultâneas; Capacidade de gerar relatório das chamadas efetuadas e recebidas; Gravação de Prompts (arquivos) personalizados de voz; Armazenamento de Informações em Banco de Dados baseado em Software Livre; DDR - Discagem Direta a Ramal; Linha executiva; Identificador de chamadas DTMF/FSK incorporado; Chamada de emergência; Música de espera (uma fonte externa e uma interna configuráveis); Blacklist (lista negra); Plano de numeração flexível; Acionamento externo; Transferência; Hora certa; Não perturbe; Hotline (interna e externa); Senha para os ramais; Cadeado; Bloqueio de ligações locais, DDD, DDI e celular; Bloqueio de ligações a cobrar; URA – Unidade de Resposta Audível com no mínimo 7 níveis/subníveis de atendimento; Gestão estratégica de condição de tempo (Time Condition); Agenda coletiva; Agenda individual; Soluções CTI; Rechamada interna; Rechamada externa; Chefe-secretária; Serviço noturno; Retenção de chamadas; Rota de menor custo; Seleção automática de linhas; Interface Ethernet; Ligações telefônicas IP (VoIP); Identificação e supressão do número chamador; Permitir integração da central de telefonia com aplicativos SIP disponibilizados em dispositivos móveis (smartphone, tablets); Toques distintos para chamadas internas e externas; restrição de chamadas de saída por código de acesso, com registro no bilhete; restrição de chamadas de saída por classes de serviço; rediscagem do último número de entrada e saída; auto provisionamento de dispositivos com ATA e Telefone IP.

O PBX IP deverá gerar sinalização para integração com dispositivos externos como ATA, Telefone IP, Softphone, Gateways e Aplicações, de forma a manter uma característica multiplataforma, utilizando assim recursos avançados destes dispositivos, permitindo o maior aproveitamento da tecnologia no processo de integração. Através do processo de sinalização, a plataforma deverá: Disponibilizar sinalização para diferenciação audível de novas chamadas enquanto usuário está com chamada ativa; Sinalização de segunda chamada para ramais ocupados; Sinalização avançada para atraso no toque de chamada, sem interferir na indicação visual; Sinalização para desvio de chamadas incondicional e em caso de ocupado, não atendimento, usuário inacessível; Sinalização para desvio de chamada com base no número chamador, horário e condições; Aplicação e Sinalização para desvio de chamadas para números diferentes, definidos para chamadas internas ou externas e conforme condição; Aplicação e Sinalização de chamadas para o correio de voz com indicação de mensagem (MWI – Message-Waiting Indicator); Aplicação e Sinalização avançada para ativação/desativação remota de desvios; Aplicação e Sinalização de ativação remota do desvio de chamadas incondicional; Sinalização para tratamento simultâneo de múltiplas chamadas; Sinalização para transferências de chamadas entre telefonistas; Sinalização para visualização do número chamador no visor do aparelho telefônico SIP; Sinalização para visualização do número do ramal chamador em aplicativo na estação de trabalho associada a ramal ATA através de CTI.

Além do processo de sinalização e aplicações internas, que são inerentes ao plano de discagem, a solução de PBX IP, como aplicações complementares e fundamentais para o provimento do serviço, deverá prover: Aplicação com disponibilidade de anúncio com número do ramal utilizado, para identificação do mesmo; Aplicação com Possibilidade de rechamada em caso de ocupado e não atendimento; Aplicação de sinalização do status das linhas; Aplicação avançada de reserva de linhas; Aplicação de serviços multilinhas; Aplicação de ativação remota do toque paralelo para busca do usuário; Aplicação de registro em qualquer telefone da rede através de usuário e senha; Aplicação de serviços para mesa de telefonista; Aplicação para acesso direto do chefe para a secretária e secretária para o chefe; Disponibilidade para acesso direto entre chefes; Aplicação avançada de visualização para a secretária com status da linha principal do chefe e de outra secretária; Aplicação de serviços de mobilidade; Aplicação de conferência com até 10 participantes, podendo se estender a partir da configuração do servidor PBX IP; Aplicação de serviço quality call (avaliação de qualidade do atendimento); Aplicação de ouvidoria (reclamações, sugestões); Aplicação de acesso a sala de conferência através de linha compartilhada com outros usuários; Aplicação de gravação de chamada (ramal, fila, número externo); Aplicação de call center (filas de atendimento); Aplicação de unidade de resposta audível (URA) com apresentação de informações por voz digitalizada sem a necessidade de atendentes, tratamento de tons DTMF, e com possibilidade de integração a banco de dados e a WebService externos; Aplicação de envio de mensagens de voz individuais ou campanha em massa para telefonia fixa e móvel, possibilitando ainda inserção de URA para intervenção de agentes de telefonia.

1.2.2.1. Recursos de Bilhetagem

Gerenciamento dos recursos de bilhetagem através dos parâmetros da administração web, no idioma português do Brasil, centralizado no servidor PBX IP; Visualização dos relatórios em português; Operação das estatísticas através das classes em sub menus; Os relatórios gerados podem ser enviados via e-mail ou impressos em qualquer impressora da rede; Processar o agendamento da geração de relatórios possibilitando exportar no formato PDF; Acesso a relatórios em formato CSV para exportação a ferramentas de terceiros; Acesso disponível, a partir de qualquer ponto da rede, a consulta de gráficos e relatórios via web browser e com uso de credenciais de acesso; O processamento e geração de bilhetagem devem ser centralizados no servidor no Cluster PBX IP; Gerenciamento e visualização de relatórios disponíveis para totalizações e sumarizações em vários níveis: por ramal; por tronco; por número discado; por data e hora; por centro de custo; estatística da central; tráfego telefônico, operadora de telefonia fixa ou móvel; Permitir coletar os bilhetes de todos os ramais do sistema de comunicação corporativo via rede IP; Classificar chamadas em local, celular, DDD, celular DDD, a Cobrar, ramal e serviços; Registrar e organizar todos os dados de chamadas de voz que venham a ser obtidos em toda a rede; O registro dos bilhetes deverá ser efetuado através da rede, de forma automática; Somente usuários com devido nível de acesso têm possibilidade e permissão para gerar relatórios; Possibilidade de exportação e integração de relatórios para gestão de custos em softwares de tarifação, não contemplado aqui, trazendo as quantidades de minutos por códigos de área e análise de melhores planos de tarifação.

1.2.2.2. Segurança

Gerenciamento dos mecanismos para segurança da estrutura visando garantir o acesso aos recursos do sistema de telefonia apenas a usuários com permissão garantida. Prever no mínimo as seguintes funcionalidades:

Complexidade de senha de ramais utilizando caracteres especiais; Utilização de senhas para os níveis de acesso e funcionalidades para administração web, dispositivos IP e aplicativos; Proteção contra ataques e serviços de defesa; Monitoramento do tráfego de entrada do sistema; Deve gerar alarmes quando mensagens são descartadas por ataques de negação de serviço (DoS - Denial of Service); Firewall interno: Deve permitir o bloqueio de endereço IP de origem e transferência do mesmo para uma lista negra após ultrapassar limiar pré-definido. Gerenciamento das regras, bloqueios, lista de exceções e tráfego; A política de segurança padrão para gerenciamento deve bloquear todas as portas exceto as portas utilizadas para gerenciamento e operação; Possibilidade de autenticação ou login na aplicação; Segurança em CLI (Command Line Interface): Deve possuir interface segura de Linha de Comando através de SSH (Secure Shell); Deve possuir interface segura de transferência de arquivos através de SFTP (Secure File Transfer Protocol); Possibilidade de upgrade (atualizações) para as devidas implementações de segurança; Disponibilizar no sistema de administração web, acesso com suas devidas restrições por usuário, para definir e/ou customizar seu perfil de uso; Gerenciamento das políticas de senhas e bloqueios para cada ramal pertencente a rede PBX-IP; Disponibilidade de políticas de senhas para acesso a gravações de áudio; Disponibilidade de políticas de senhas para exibição de relatórios gerenciais de telefonia; Disponibilidade de políticas de senhas para acesso ao sistema de Operação telefonista; Disponibilidade de políticas de senhas para acesso para administração web (níveis de acesso e operacionalidades); Permissão e controle gerenciável para acesso remoto de possíveis manutenções e suporte; Prevenção de desastre e plano de recuperação.

1.2.2.3. Conectividade e Roteamento

O sistema deve permitir conexão aos sistemas das concessionárias de serviços de telefonia a partir de protocolos padrão de mercado; conexão com circuito de E1 (R2 e RDSI/ISDN) e Troncos SIP; Suporte a interfaces ISDN PRI e R2; Suporte a interfaces GSM para ligações para a rede celular; Conexões em rede local: Telefonia em redes independentes, telefonia em redes compartilhadas, Suporte para manutenção utilizando acesso remoto;

Integração entre a Unidade do SAMU com as demais unidades dos SAMU localizadas no Estado de Minas Gerais via VoIP; Suporte a roteamento por transbordo, rota de menor custo, origem, destino, horário, dias da semana; Acesso à base atualizada de portabilidade BDR (Base de Dados Nacional de Referência) para serviços de telefonia fixa (STFC) e móvel pessoal (SMP) permitindo definição de roteamento por operadora de destino da chamada; Relatório de operadora de destino das ligações de telefonia fixa e móvel; Rota de acesso de longa distância; Suporte para o roteamento das sessões para o mesmo destino através de diferentes tipos de rotas, como grupo de troncos.

Além disso, em caso de rota indisponível, o transbordo também pode ser direcionado para diferentes tipos de rotas; Monitoramento dos troncos através da disponibilidade das operadoras; Gerenciamento da rota de menor custo para chamadas de longa distância, incluindo eventuais redes de dados, e chamadas celular, sem a necessidade de digitar um código de rota especifico; Gerenciamento das características de roteamento de menor custo (LCR) para os entroncamentos com as operadoras de telefonia através de uma tecla predefinida para as rotas já programadas; Gerenciamento de categorização nos ramais dos sistemas de voz; Gerenciamento dos troncos dos sistemas para interface com as operadoras de telefonia.

1.2.2.4. Recursos de Áudio

Recursos de áudio centralizados no próprio servidor PBX-IP; Suporte aos codecs G.711 e G.729; Utilização de codecs diferenciados para LAN e WAN; Suporte à reprodução de tons e anúncios; Suporte à reprodução de música em espera (MoH); Suporte à geração de tons DTMF; Suporte a recepção e tratamento de tons DTMF; Suporte à geração de anúncios pré-definidos conforme a funcionalidade acessada; Suporte à geração de anúncios relacionados à ativação e desativação de funcionalidades; Suporte, gerenciamento e centralização de recursos de áudio e gravação para chamada em espera, URA e caixa postal através de administrador web; Serviço de caixa postal e fax programado para envio de e-mail para o devido ramal programado; Suporte a gravações de ramais e filas; Suporte de áudio para inserção de arquivos com extensão mp3/wav para a devida operação dos recursos de URA (Unidade de Resposta Audível) e espera telefônica.

1.2.2.5. Padrões de mercado compatíveis com a solução de telefonia IP

RFC 1213: Management Information Base for Network Management of TCP/ IP- based internets: MIB-II (SNMP); RFC 1442: Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2); RFC 1443: Textual Conventions for Version2 of the Simple Network Management Protocol (SNMPv2); RFC 1889: RTP: A Transport Protocol for Real-Time Applications; RFC 1890: RTP Profile for Audio and Video Conferences with Minimal Control; RFC 2131: Dynamic Host Configuration Protocol; RFC 2234: Augmented BNF for Syntax Specifications: ABNF; RFC 2246: The TLS Protocol; RFC 2327: Session Description Protocol(SDP); RFC 2475: An Architecture for Differentiated Services; RFC 2597: Assured Forwarding PHB Group; RFC 2705: Media Gateway Control Protocol (MGCP); RFC 2780: IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers; RFC 2782: DNS SRV; RFC

2806: URLs for Telephone Calls; RFC 2833: RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals; RFC 2848: The PINT Service Protocol: Extensions to SIP and SDP for IP Access to Telephone Call Services; RFC 2865: Remote Authentication Dial In User Service (RADIUS); RFC 2976: SIP INFO Method; RFC 3016: RTP Payload Format forMPEG-4 Audio/Visual Streams; RFC 3047: RTP Payload Format for ITU-T Recommendation G.722.1; RFC 3168: The Addition of Explicit Congestion Notification (ECN) to IP; RFC 3204: MIME Type for ISUP and QSIG; RFC 3260: New

Terminology and Clarifications for Diffserv; RFC 3261: SIP: Session Initiation Protocol; RFC 3262: Reliability of Provisional Responses in SIP; RFC 3263: Session Initiation Protocol (SIP): Locating SIP Servers; RFC 3264: SDP Offer/Answer Model; RFC 3265: SIP-specific Event Notification; RFC 3267: Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs; RFC 3272: Overview and Principles of Internet Traffic Engineering; RFC 3288: Using the Simple Object Access Protocol (SOAP) in Blocks Extensible Exchange Protocol (BEEP); RFC 3311: SIP UPDATE Method; RFC 3323: SIP Privacy Mechanism; RFC 3515: SIP REFER Method; RFC 3605: Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP); RFC 3725: SIP Third Party Call Control; RFC 3761: The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM); RFC 3824: Using E.164 Numbers with SIP; RFC 3830: MIKEY: Multimedia Internet Keying; RFC 3842: SIP Message Waiting; RFC 3892: The Session Initiation Protocol (SIP) Referred-By Mechanism; RFC 3952: Real-time Transport Protocol (RTP) Payload Format for internet Low Bit Rate Codec (iLBC) Speech (SIM); RFC 3959: The Early Session Disposition Type for the Session Initiation Protocol (SIP); RFC 3960: Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP); RFC 4028: Session Timers in SIP; RFC 4049: Binary Time: An Alternate Format for Representing Date and Time in ASN.1; RFC 4235: An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP); RFC 4353: Framework for Conferencing with the Session Initiation Protocol (SIP); RFC 4568: Session Description Protocol (SDP) Security Descriptions for Media Streams; RFC 4575: A Session Initiation Protocol (SIP) Event Package for Conference State;

1.2.2.6. Alta Disponibilidade

Um sistema de Alta Disponibilidade é aquele que visa manter a disponibilidade dos serviços prestados por um sistema computacional replicando serviço e servidores através da redundância de hardware e reconfiguração de software. Adicionando-se mecanismos especializados de detecção, recuperação e mascaramento de falhas, pode-se aumentar a disponibilidade do sistema, de forma que este venha a se enquadrar na classe de Alta Disponibilidade. Nesta classe as máquinas tipicamente apresentam disponibilidade na faixa de 99,99% a 99,999%, podendo ficar indisponíveis por um período de pouco mais de 5 minutos até uma hora em um ano de operação. Nesta classe, se encaixam grande parte das aplicações comerciais de Alta Disponibilidade, como centrais telefônicas;

O seu funcionamento inclui a sincronização dos bancos de dados em ambas as máquinas, e a criação de um endereço IP virtual através do software heartbeat *(solução que monitora o status de dois ou mais nodos (servidores) em um ambiente, em caso de detecção de falha, redireciona o serviço para outro servidor de forma transparente para o usuário/aplicação)*, que aponta para o servidor primário. Em caso de falha dessa máquina, automaticamente o software heartbeat transfere o IP virtual para a máquina secundária, que continuará disponibilizando os serviços.

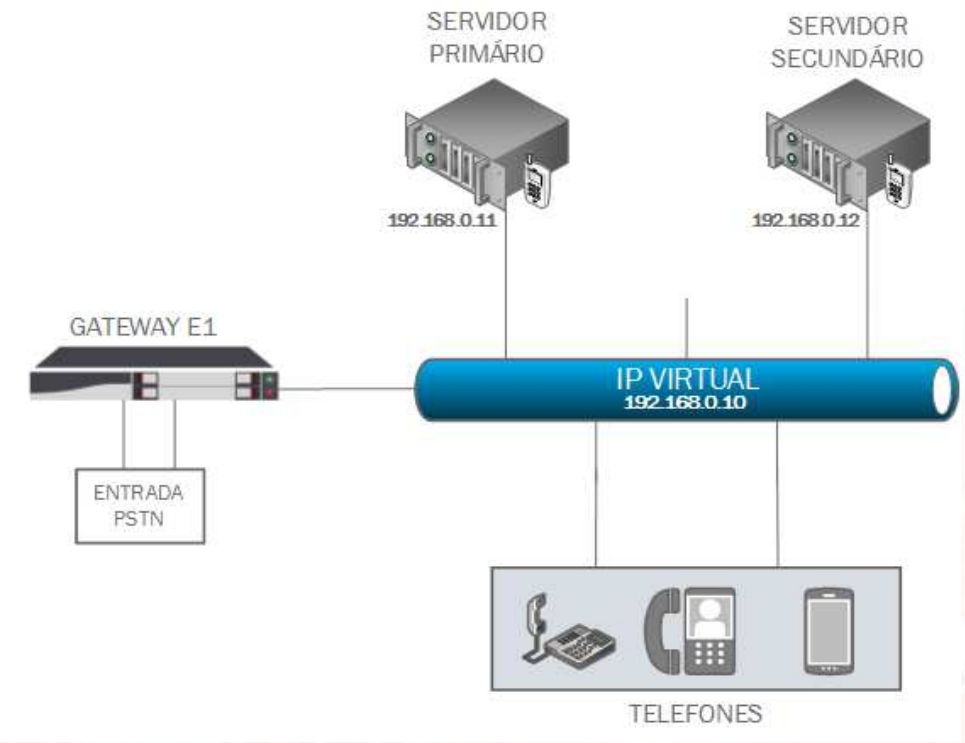


Figura 14 – *Exemplo de alta disponibilidade.*

Outro modelo de alta disponibilidade se dá através do sistema *Multi Master* onde os participantes do Cluster funcionam simultaneamente, executando todas as ações do PBX IP. Com esse cenário, a disponibilidade do ambiente tende a aumentar significativamente, provendo a continuidade do negócio sem pontos de interrupção. Neste caso, a distribuição das chamadas é realizada através de balanceamento de carga, com a utilização do protocolo DNS SRV, especificação da RFC 2782, não sendo necessário a configuração de um IP virtual através de um sistema de heartbeat. Desta forma, o Cluster é alcançado através do registro DNS, onde a pesquisa do host será respondida de acordo com peso e prioridade. Neste caso, os dispositivos Telefone IP, Gateways e ATA deverão ter a capacidade de consulta e comunicação do registro SIP reportado através dos servidores DNS.

O PBX IP deverá apresentar as duas formas de trabalho em alta disponibilidade supracitadas, obedecendo as melhores práticas de mercado, em conformidade com o PCN - Plano de Continuidade de Negócios da ISO 22301.

1.2.2.7. Integração com Sistemas

A plataforma de sistema PBX IP deve permitir integração com outros sistemas via CTI *(Computer Telephony Integration),* que é o processo pelo qual o PBX IP troca informações de uma chamada com um computador, permitindo o computador ou um indivíduo gerenciar melhor a chamada.

As funcionalidades que o PBX IP deve disponibilizar numa integração via CTI são: Exibir no computador as informações da chamada: Número chamador (ANI), número discado (DNIS) e preenchimento da tela no atendimento da chamada; Discagem automática e discagem controlada pelo computador: discagem rápida (fast dial), preview dial e discagem preditiva (predictive dial); Controle do telefone: atender (answer), desligar (hang up), colocar em espera (hold), fazer conferência (conference); notificar trabalho após o término da chamada (after-call work), gerar logs da chamada; Controle do status do atendente, por exemplo, se o trabalho após o término da chamada passar de um tempo determinado, o status do atendente volta para "pronto para tratar chamadas"; Controle de chamadas para monitoramento da qualidade e / ou por softwares de gravação das chamadas.

1.2.2.8. Backup de Dados

Todas as informações presentes no PBX IP tais como as presentes no banco de dados, arquivos de configuração e gravações telefônicas, deverão todas ser salvas em dispositivos de backup (storage), para que haja segurança de armazenamento dos dados. O Storage é um hardware que contém slots para vários discos, ligado aos servidores através de ISCSI, NFS ou fibra ótica, é uma peça altamente redundante e cumpre com louvor a sua missão, que é armazenar os dados com segurança.

O storage pode aceitar diversas conexões de servidores diferentes, ao mesmo tempo. Então a sua matriz RAID, além de segura, ficará altamente portável. A estrutura de backup deverá conter critérios para o sistema de prevenção de desastre, com a finalidade de recuperação do sistema em até 1 hora.

2.2.2.9. Gravações Telefônicas

O sistema de gravação de chamadas incorporado ao PBX IP permite a gravação digital das chamadas e o armazenamento em dispositivos de backup (storage). A gravação das chamadas é essencial para o monitoramento de atendimento, controle de conversas não profissionais, escuta telefônica, gravação de diálogos para procedimentos de segurança, negociações verbais, auditorias, etc.

Características: Permitir configurar a gravação por ramal, fila de atendimento, número de telefone, opção de URA, etc.; Permitir o gerenciamento centralizado das gravações, restrito a usuários previamente autorizados; Possibilitar a programação e recuperação remota das gravações; Possuir filtros de busca por data, hora, duração, ramal, fila de atendimento, número de origem, número de destino; Suportar formatos de gravação como MP3, WAV, GSM, etc.; Gravar simultaneamente as ligações telefônicas de todos os canais; Gravação de linhas e ramais analógicos, digitais, E1; Reprodução de gravações telefônicas em software cliente local ou remoto; Sistema de arquivamento com pastas por canal, data e hora.

2.2.2.10. Aplicativo para Chamadas de Emergência SAMU 192 via VoIP

O sistema de PBX IP deve possuir um aplicativo gratuito compatível com dispositivos Android e iOS, desempenhando um papel crucial: permitir chamadas de emergência para o SAMU 192 via VoIP (Voz sobre IP). Esta capacidade se torna especialmente vital em regiões com cobertura móvel limitada ou durante falhas nas redes de telefonia fixa ou móvel, garantindo um acesso rápido ao serviço de urgência e emergência quando mais necessário.

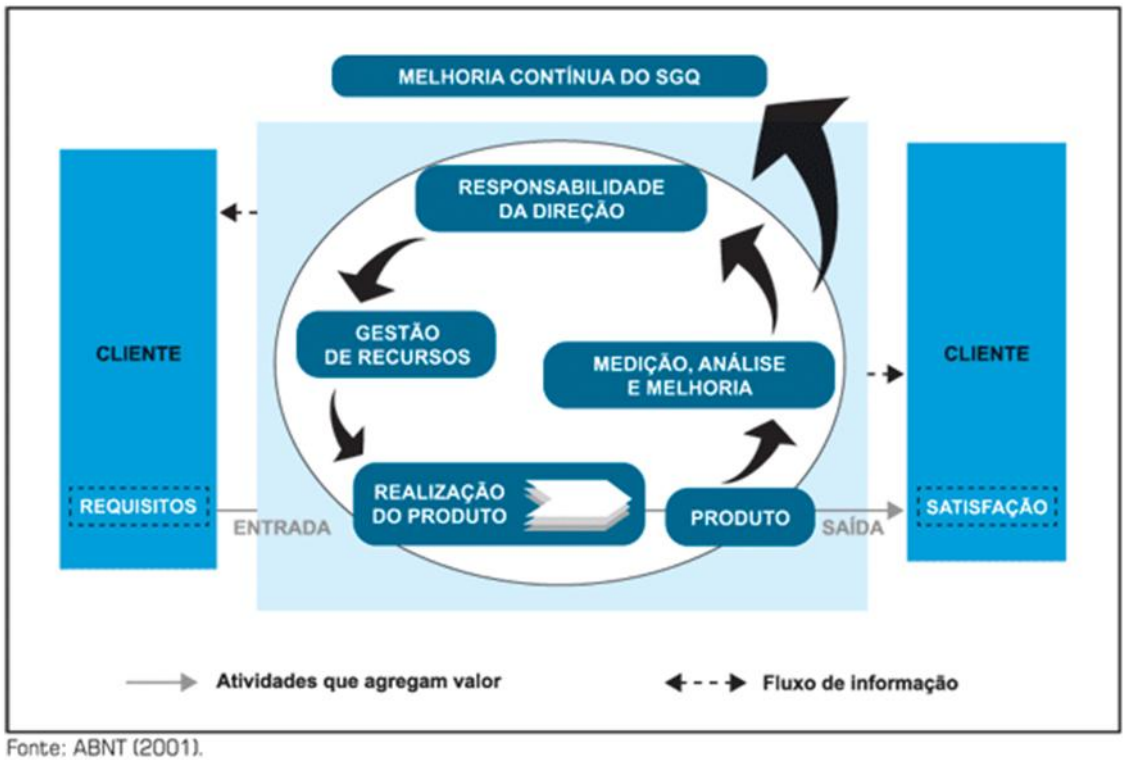
O aplicativo deve oferecer diversas opções para estabelecer comunicação com o SAMU 192, seja através de conexões Wi-Fi ou utilizando os dados da operadora móvel, como o 4G, por exemplo. Além disso, é essencial que os usuários possam cadastrar antecipadamente o município de origem das chamadas de emergência, facilitando um acionamento rápido dos serviços de socorro. Outra funcionalidade importante é o uso do GPS do dispositivo ao iniciar uma chamada. Essa função permite que o aplicativo identifique automaticamente o município de origem, mesmo se o usuário estiver em um local diferente do cadastrado. Essa capacidade é fundamental para direcionar a ligação para a Central de Regulação do SAMU responsável por aquele município específico, garantindo uma resposta mais eficiente e adequada às necessidades do usuário.

Esses recursos são fundamentais, especialmente em áreas remotas ou com cobertura móvel irregular. A capacidade de realizar chamadas de emergência por meio de redes Wi-Fi disponíveis pode ser a diferença entre salvar uma vida ou enfrentar uma situação de risco prolongada e potencialmente fatal. Assim, a incorporação dessas funcionalidades em uma solução de PABX-IP é essencial para garantir a segurança e o bem-estar dos usuários em uma variedade de circunstâncias desafiadoras.

2.3 - SERVIÇOS

2.3.1. Objetivo

Os serviços continuados, tem por propósito a melhoria na qualidade do que é oferecido ao cliente final, como premissa para toda a operação de serviços no complexo regulador do SAMU. Essa atividade tem por fim manter em pleno funcionamento toda a estrutura tecnológica implantada e promover de forma ativa, soluções e melhorias baseadas nas necessidades detectadas. O suporte continuado, o monitoramento de ativos e serviços, bem como a implantação de conectividade de internet, deve seguir as normas básicas de SGQ (Sistema de Gestão da Qualidade), referenciado na ISO:9001:2000. O processo mostrado abaixo classifica essa atuação. O produto oferecido é o serviço em questão e o cliente são as pessoas, processos e diretrizes internas do complexo regulador.



Fonte: ABNT (2001).

Figura 15 – *Atuação do SQG.*

2.3.2. Suporte

O ambiente proposto necessita de suporte técnico especializado no que se referem à infraestrutura da rede de dados, voz, seus dispositivos e periféricos e usuários. O suporte técnico é uma parte indispensável do projeto. Ele deve participar de toda a operação (instalação e homologação do projeto), além de prestar manutenção e assistência pós-implantação, aderindo a um conceito de Melhoria Continuada – processo fundamental para potencializar todas as funcionalidades do produto, identificar possibilidades de melhoramento da ferramenta ou ainda de novas necessidades de expansão do projeto. Para a unidade do SAMU, o suporte técnico também deve ficar responsável pelo monitoramento e assistência técnica de toda a infraestrutura e processos pertinentes ao ambiente do local, incluindo suporte e apoio ao usuário.

2.3.2.1. Predefinições:

- **Central de Serviços**: Ponto Único de Contato, composta por uma equipe responsável por lidar frequentemente com uma variedade de eventos de serviço.
- **Chamados (Ordens de Serviço)**: Requisições de Serviços e/ou Incidentes registrados pelos usuários ou detectados automaticamente pela central de monitoramento de eventos.
- **Tipificação**: Tipificar um chamado significa atribuir a ele uma classificação dentro do escopo de tratamento para incidentes e requisições de serviços declarados, para identificar o tipo exato do evento que está sendo registrado.

- **Requisição de Serviço**: Solicitações que demandem alterações no ambiente, objetivadas a atender uma nova realidade ou necessidade da operação ou negócio, tais como:
    - **Mudança/melhorias no ambiente**: Referem-se às requisições de serviço que venham ser realizadas para melhorar a qualidade dos serviços prestados, bem como implantação de mudanças rotineiras do ambiente;
    - **Condição para a operação do negócio**: Referem-se às requisições de serviço que se não implantadas, inviabilizam ou podem vir a inviabilizar a operação.
- **Incidente**: Todo e qualquer evento que não faz parte da operação normal de um serviço e que cause ou venha causar uma interrupção, ou redução da qualidade de serviço, tais como:
    - **Produção Parada**: Incidente que torna um ou mais serviço(s) indisponível(eis) inviabilizando as operações ou sem desempenhar seu papel previsto;
    - **Produção Impactada**: Incidente que torna um ou mais serviço(s) degradado(s), mas em funcionamento, permitindo a operação.

2.3.2.2. Níveis de suporte

O setor de suporte técnico deve ser dotado de capacidade de atendimento no primeiro nível (Equipe de TI local ou Suporte *In Loco)*, segundo nível (Equipe de Service Desk e especialistas), além do acionamento e acompanhamento do terceiro nível (Especialistas e Analista Sênior). O processo de suporte deve atender a um modelo de atendimento padrão, conforme o fluxograma a seguir:

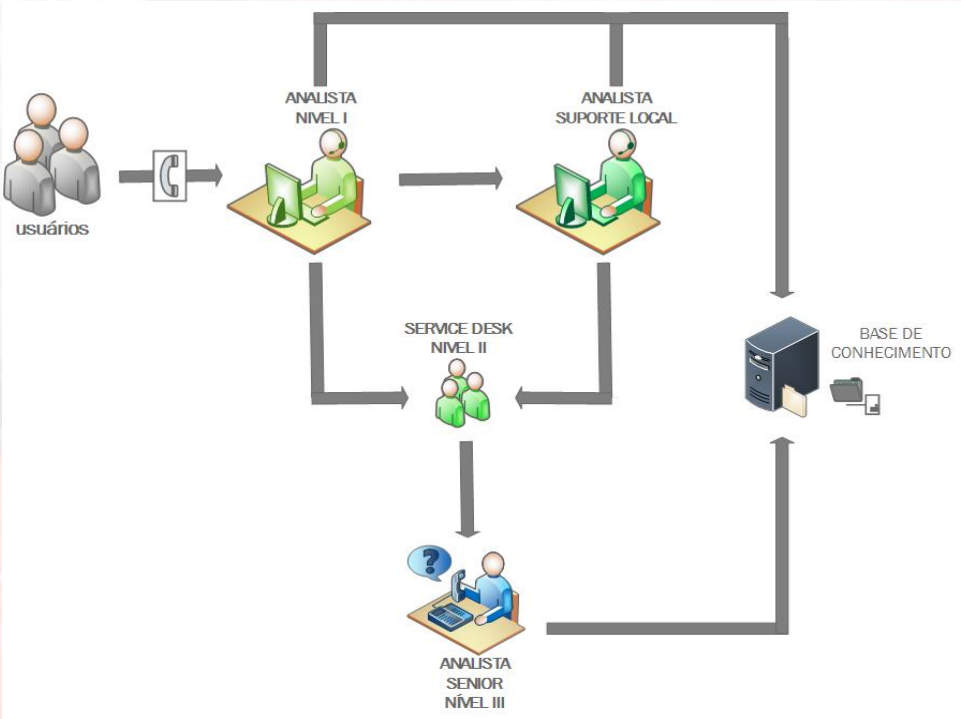


Figura 16 – *Ação dos níveis de Suporte.*

Suporte técnico in loco (primeiro nível) é a prestação de serviços de TI no local em que o problema ocorre ou que se faça necessário um suporte específico. Para o local em questão, ele se faz necessário devido à complexidade da infraestrutura do local, para auxílio na resolução de possíveis incidentes e eventos em relação ao projeto, bem como na assistência técnica, seja intelectual (conhecimentos) ou tecnológica (manutenção: revisões, regulagens, calibrações, reparos/consertos, requisições pertinentes à área, atualizações de software etc.) para todo o ambiente de TI do local, com a finalidade de solucionar problemas técnicos relacionados a produtos e soluções tecnológicas, tais como: redes (dados e voz), telefonia, computadores, softwares e afins. Para atender a Unidade do SAMU, o Suporte in loco deve possuir disponibilidade de 14 horas por dia, em dias úteis, distribuindo a carga horária entre dois técnicos capacitados e, fora deste, a prestadora de serviços deve disponibilizar pessoal capacitado para eventuais demandas de suporte.

O Suporte Especializado (Segundo e terceiro níveis) deste serviço, deve ter por objetivo resolver os eventos de serviço (chamados) da Central de Serviços, sendo eles: Requisições de Serviços e Incidentes provenientes de chamados ou de alertas de ferramentas de monitoramento, devendo ser considerado uma janela de cobertura 24x7 (24 horas por dia, 7 dias por semana). Nesses níveis, se abrangem a identificação, o gerenciamento e a resolução de incidentes ou eventos de maior criticidade e/ou complexidade e que demandem um nível de conhecimento superior acerca dos sistemas e soluções implantadas, além de atender solicitações de nível gerencial.

2.3.2.3. Sistemática para atendimento e prestação de serviços/abertura de chamados/ resolução de incidentes

O Suporte Técnico deve possuir um portal ou ferramenta de Service Desk, além de ramais ou números de telefone dedicados ao atendimento remoto, abertura e documentação de chamados, bem como o feedback das solicitações. O processo de abertura de chamados e resolução de incidentes deve seguir as seguintes premissas:

- **Identificação e Registro de Incidentes:**
  - Os incidentes/eventos devem ser registrados oriundos dos diversos meios disponibilizados, tais como: telefone, e-mail, ferramenta de Service Desk ou registro manual de alarmes de eventos procedentes de ferramentas de monitoramento;
  - Todos os incidentes que ocorrem na infraestrutura e nos serviços devem ser registrados;
  - As informações relevantes para o tratamento do chamado devem ser registradas, mantendo-as sempre atualizadas a cada alteração, para que a resolução do incidente e o tratamento da requisição de serviço possam ocorrer de maneira adequada.
- **Categorização:**
  - Esta atividade compreende tanto a categorização de eventos que serão registrados como incidente, tanto quanto aqueles que devem ser encaminhados para o processo de requisição de serviços.

- Categorizar um incidente significa atribuir a ele uma classificação dentro do escopo de atividades do serviço, além de permitir o dimensionamento da quantidade de horas ou esforço técnico a ser consumido com o atendimento daquele incidente.

- **Priorização:**

  - A priorização dos incidentes deve ser realizada através da atribuição da Urgência (quão rápido o incidente precisa ser solucionado) e do dimensionamento do Impacto (extensão do dano no ambiente) que incidente registrado possa vir a causar.

- **Pesquisa e Diagnóstico:**

  - Após registrar, categorizar e priorizar o incidente, o atendente do chamado deverá prover o suporte inicial utilizando-se de scripts de atendimento e da base de erros conhecidos existente. Se, na pesquisa da Base de Conhecimento, o incidente for encontrado, deve-se verificar se existe uma solução de contorno e se a Central de Serviços pode aplicá-la;
  - Caso a solução não seja possível de aplicar dentro do escopo de serviços do atendimento, o chamado deve ser direcionado para grupo solucionador de especialistas, de acordo com as regras definidas e cadastradas no sistema da Central de Serviços do Suporte Técnico.

- **Encerramento do Chamado:**

  - Após a aplicação da solução de restauração ou contorno diretamente pela Central de Serviços ou após o retorno de chamados, o atendente deverá registrar de forma concisa e de fácil interpretação as ações tomadas para resolver o incidente/evento;
  - Além disso, a resolução e as ações tomadas devem ser informadas e confirmadas com o usuário;
  - O contato com o usuário para encerramento do chamado pode ser feito por telefone, podendo ser enviado e-mail, como método alternativo, caso não seja possível o contato;
  - Caso não exista resposta do usuário, seja ela por e-mail, telefone ou software de controle de chamados, o incidente registrado poderá ser automaticamente encerrado em até três dias úteis.

- **Encaminhamento de Chamados a Terceiros:**

  - Caso, durante o processo de atendimento, seja identificado que o chamado deverá resultar no acionamento de um subcontratado da Unidade do SAMU, caberá à Central de Serviços encaminhar o chamado e acompanhar sua resolução, monitorando os níveis de serviços prestados;
  - A Central de Serviços deverá gerir os chamados encaminhados aos subcontratados, bem como os níveis de serviços contratados, calculando as penalidades cabíveis por descumprimento desses serviços.

2.3.2.4. Catálogo de serviços

Item	Atividade do serviço	Descrição do serviço
1	Análise, configuração e manutenção de microcomputadores e notebooks.	Essa atividade consiste em identificar problemas nos microcomputadores ou notebooks, sejam eles físicos ou lógicos, reportando a solução e/ou posteriormente fazendo a correção dos mesmos, sendo documentada qualquer alteração na configuração dos dispositivos. Também consiste na configuração dos mesmos para o uso na rede e na instalação de softwares específicos nas máquinas correspondentes.
2	Análise, configuração, correção e ou instalação em equipamentos ativos de rede classe 1 e afins (Modem, switches e roteadores).	Essa atividade consiste em configurar, implantar e controlar as conexões dos diversos segmentos de rede no ambiente de TI interno e externo da Unidade do SAMU. Isso inclui a análise e correção dos switches e gateways existentes no ambiente, onde também se encontram recursos de roteamento, VLAN, VPNs, etc.
3	Análise e correção de problemas de segurança com antivírus.	Esse serviço inclui análise e correção de problemas de segurança que podem ser solucionados através do antivírus e/ou demais ferramentas de mercado.
4	Suporte e apoio ao usuário	Essa atividade consiste no auxílio e treinamento no uso de sistemas e equipamentos utilizados no ambiente de TI da Unidade do SAMU.
5	Instalação e Configuração de equipamentos	Esse serviço inclui a instalação, configuração e instrução de uso de equipamentos, de rede ou não, que sejam pertinentes ao ambiente de TI do local.
6	Análise, correção e atualização de firmwares de servidores do tipo torre, rack ou lâmina.	Essa atividade irá realizar uma análise de problemas relacionados ao servidor, bem como a possível solução, manutenção ou substituição do mesmo. Também inclui a atualização do firmware atual, se houver atualizações publicadas pelo fabricante, caso seja solicitado ou se faça necessário.

7	Análise, correção e atualização de componentes e serviços da central telefônica IPBX.	Esse serviço consiste na identificação de eventos e incidentes que possam ocorrer na central telefônica, bem como os componentes interligados diretamente na solução de telefonia, incluindo a manutenção corretiva/preventiva de tais incidentes/eventos e também o encaminhamento de chamados para terceiros, caso seja necessário.
8	Análise e solução de problemas de serviços em Windows Server	Esse serviço fornece uma análise dos problemas associados aos serviços do Windows server (File Server, Impressão, DHCP, SQL Server, etc.) e posteriormente a correção dos mesmos.
9	Análise e solução de problemas de ambientes virtuais VMware vSphere ESXI ou Citrix XenServer e outros.	Esse serviço fornece uma análise de todo ambiente virtual e posteriormente a correção dos mesmos. Inclui também o gerenciamento e configuração de máquinas virtuais.
10	Análise, configuração e correção de problemas em sistemas operacionais Linux e seus derivados.	Esse serviço fornece uma análise e posteriormente a correção de problemas em sistemas operacionais Linux e seus derivados, incluindo firewall, proxy, Apache, MySQL, Tomcat, FTP, OpenVPN, etc.
11	Assessoria para planejar e/ou definir melhorias no ambiente.	Discussão com um especialista sobre possíveis melhorias na infraestrutura local, políticas de TIC, bem como na utilização dos sistemas implantados.
12	Análise, configuração, e atualização de firmware de Nobreaks.	Essa atividade consiste em configurar, identificar incidentes e causas em Nobreaks gerenciáveis, para que se assegure o máximo de tempo do funcionamento do ambiente de TI no caso de surtos e falta de energia.
13	Análise, configuração, correção e gerenciamento de soluções de segurança de redes (Firewall).	Esse serviço inclui análise, configuração e correção de possíveis problemas causados por sistemas infectados por vírus, malwares ou spywares, no qual, o firewall deve ser utilizado como ferramenta de varredura, identificação e correção do problema na rede.

14	Elaboração de documentos finais	Esse serviço inclui confecção de documentações de apoio que poderão conter diagramas de rede e datacenter da infraestrutura de TI e mudanças ocorridas.
15	Serviço de Monitoramento Proativo da Infraestrutura.	Esse serviço inclui monitoramento proativo de toda a infraestrutura de TI, de acordo com o item 2.3.3 deste projeto.

2.3.2.5. Especificações dos serviços

Análise, configuração e manutenção de microcomputadores, notebooks e equipamentos; soluções antivírus e suporte ao usuário

- Manutenção corretiva/preventiva/limpeza de computadores e componentes;
- Formatação e instalação de sistemas operacionais Windows ou Linux;
- Instalação e configuração de softwares específicos em cada S.O, conforme necessidade;
- Configuração das interfaces de rede dos terminais;
- Configuração de compartilhamentos na rede, conforme necessidade;
- Instalação e configuração de impressoras e periféricos, de rede ou não;
- Configuração e atualização periódica de antivírus nos computadores e escaneamento periódico nos computadores;
- Remoção de vírus, malwares e spywares dos computadores;
- Apoio a usuário na utilização de sistemas e funcionalidades pertinentes ao trabalho do mesmo;
- Treinamento e apoio ao usuário na utilização de telefones IP e seus derivados, bem como na utilização das funcionalidades do sistema de telefonia pertinentes à cada área;
- Identificação de problemas físicos na infraestrutura de TI;
- Backup e restaurações de configurações e dados.

Serviços em equipamentos ativos de rede classe 1 e afins (Modem, switches e roteadores)

- Instalação, configuração, atualizações de firmwares de roteadores e switches;
- Implantação, configuração e gerenciamento de roteamentos dinâmicos, estáticos ou trunking, conforme necessidade;
- Gerenciamento de redes sem fio e cabeadas;
- Inclusão, exclusão e gerenciamento de Vlans de modo tagged ou untagged, nas Switches, de acordo com a necessidade;
- Configuração de interfaces, endereçamento e serviços de rede;
- Implantação, configuração e gerenciamento de interconexões através de VPN's, MPLS, etc., conforme necessidade e disponibilidade dos serviços;
- Backup e restauração de configurações dos equipamentos.

Serviços de segurança de redes, configuração, manutenção e gerenciamento de firewalls

- Criação, configuração e gerenciamento de redes lógicas, faixas de IP, perfis usuários;
- Inclusão e exclusão de dispositivos nas faixas de IP e perfis correspondentes;
- Atualização periódica da solução de segurança (firewall) conforme a disponibilidade;
- Criação, configuração e gerenciamento de políticas de segurança, regras de acesso e bloqueios necessários para o bom funcionamento da rede e para segurança dos dados trafegados;
- Análise de conformidade/aderência a políticas e normas de segurança. Esta atividade inclui a elaboração de relatórios técnicos indicando práticas a serem aplicadas em cada serviço para atender às normas de segurança;
- Elaboração de relatórios analíticos de acessos e estatísticas de tráfego de rede;
- Backup e restauração de configurações.

Instalação, configuração, atualização e manutenção em servidores

- Atualizações de firmwares;
- Configuração de sistema, tipos de particionamento e tipos de RAID a serem utilizados nos servidores;
- Instalação e configuração de Sistemas Operacionais (Windows servers, Linux ou seus derivados), além das configurações de rede e serviços dos mesmos;
- Backup e restauração de configurações.

Análise, manutenção, atualização e gerenciamento da Central Telefônica

- Gerenciamento de entroncamentos SIP, gateways e troncos analógicos, digitais e GSM; bem como análise de possíveis problemas decorrentes dos mesmos e resolução de incidentes junto aos provedores destes serviços;
- Manutenção corretiva/preventiva/limpeza dos servidores IPBX;
- Atualizações de firmware ou do sistema Asterisk, bem como do banco de dados, DAHDI ou outras ferramentas necessárias para o funcionamento da solução. Este serviço, por padrão, só deve ser feito caso exista necessidade comprovada pelo setor de suporte;
- Provimento, configuração e gerenciamento de todas as funcionalidades da Central Telefônica PBX IP, conforme descrito no item 2.2.2 deste projeto; além de manutenção e resolução de incidentes pertinentes às mesmas;
- Análise, configuração, atualização de firmwares e correção nos Storages que compõem a solução de telefonia, caso se faça necessário;
- Análise, configuração, atualização de firmwares e correção nos Gateways SIP/GSM que compõem a solução de telefonia, caso se faça necessário;
- Backup e restauração de dados e configurações.

Serviços em ambientes virtuais (VMware vSphere ESXI ou Citrix XenServer e outros)

- Instalação, configuração e resolução de problemas no software de virtualização da VMware e Citrix Xenserver;
- Inclusão e exclusão de máquinas virtuais, conforme necessidade;
- Gerenciamento de memória, discos e CPU's das MV's, alterando as configurações das mesmas, caso seja necessário, para o bom funcionamento do ambiente virtual;
- Instalação, configuração e manutenção de softwares de gerência de virtualização correspondentes;
- Conversão de servidores físicos para virtuais, caso se faça necessário(P2V);
- Backup e restauração de configurações.

Serviços de análise, identificação de incidentes e soluções relacionados a Nobreaks

- Identificação de possíveis surtos, falta de energia ou tensão de entrada inferior à aceitável;
- Identificação da autonomia das baterias;
- Contato junto ao prestador de serviços de eletricidade do local e reporte aos usuários e à Central de Serviços sobre detalhes do problema;
- Desligamento preventivo de equipamentos que possam ser impactados caso o nobreak descarregue completamente;

Elaboração de documentos técnicos

- Elaboração de documentos contendo todos os dispositivos existentes no ambiente de TI do local e informações que possam vir a ser necessárias no auxílio de resoluções de eventos ou incidentes;
- Criação de diagramas de rede;
- Criação de diagramas de rack contendo informações dos servidores e equipamentos;
- Atualização da base de conhecimento sobre os problemas e soluções relacionados.

Serviço de Monitoramento Proativo da Infraestrutura

- Consiste no monitoramento proativo de toda a infraestrutura de rede acordo com o item 2.3.4 deste projeto.

OBS.: O escopo dos serviços a serem contratados está segmentado por áreas de conhecimento, e devidamente especificado. Esta especificação foi baseada no parque computacional descrito nos **itens 2.1 e 2.2** deste projeto. Cabe ressaltar que a infraestrutura de TI sofre processo contínuo de atualização tecnológica, podendo se fazer necessário outros tipos de serviços pertinentes não inclusos neste escopo, mas, no entanto, pertinentes às áreas de conhecimento abordadas nas especificações. Deve o Suporte Técnico, portanto, prover a alocação de recursos especializados e adequados à prestação dos serviços aqui especificados.

2.3.3. Monitoramento

A rede de dados é composta de vários dispositivos e/ou serviços que precisam estar interligados, para que haja o compartilhamento de informações e recursos disponíveis dos ativos de rede, agilizando os processos das organizações. Por este motivo, se faz necessário o monitoramento, que através do NMS (*Network Management Station* ou Estação de Gerenciamento de Redes) e de protocolos/agentes presentes nos dispositivos, permite monitorar diversos estados e/ou serviços dos equipamentos que a rede oferece, facilitando assim o suporte proativo de problemas.

É de extrema importância o gerenciamento, para que se obtenha um bom fluxo no tráfego das informações, garantindo que os recursos sejam corretamente utilizados e visualizados

não sobrecarregando no transporte de dados, trazendo confiabilidade e segurança da estrutura.

O monitoramento, deve ser feito de forma remota, 24 horas por dia, através de uma central, com o objetivo de detectar atividades em tempo real, que porventura ocasionará futuras falhas, assim agindo de forma antecipada corrigindo-as em um curto espaço de tempo, prevenindo paradas e prejuízo ao processo operacional do SAMU.

Todos os eventos críticos na rede devem ser documentados, a partir de sistemas de help desk, com o objetivo criar um histórico para futuras consultas por relatórios gerenciais para análises de desempenho da infraestrutura.

A equipe de suporte é responsável pelo monitoramento da rede, porém, deve possuir capacidades específicas na área de informática, com conhecimento de especificações de hardware e software dos servidores, roteadores, switches, storage's, nobreaks, dentre outros dispositivos ou serviços que estarão conectados à rede e estações de trabalho.

Para o monitoramento da rede na unidade do SAMU, será necessário a utilização do protocolo SNMP (Simple Network Management Protocol) em conjunto com o RMON (Remote Network Monitoring) presente nos equipamentos, ou agentes próprios do sistema NMS, como uma ferramenta de monitoramento. O SNMP e o RMON foram criados para atender a necessidade de um padrão, de gerenciar dispositivos IP, além de fornecer aos usuários um conjunto simples de operações que permitem o gerenciamento remoto de dispositivos associados a esse protocolo, como roteadores, switches, servidores, storages e dentre outros equipamentos da rede, que contenham este protocolo embarcado.

Deve ser monitorada proativamente toda a infraestrutura cadastrada nesta solução, que abrange ativos de rede tais como: servidores (físicos), sistemas operacionais, Switches, Storages, Roteadores, Virtualizadores, Nobreaks, Gateways, Telefones IP, Links de internet, VPN's, dentre outros, e além disso, serviços do banco de dados, central telefônica, HTTP e FTP, que variam de acordo com a necessidade de informações disponibilizada pelos dispositivos e/ou sistemas.

O Monitoramento proativo da infraestrutura, deverá compreender os seguintes serviços:

- Instalação e configuração dos agentes de monitoramento nos servidores e clientes;
- Configurar os protocolos de monitoramento nos demais equipamentos que não suportam agentes (Agentless);
- Inclusão dos clientes na solução de monitoramento;
- Configurar os limites desejados para o bom funcionamento da infraestrutura e, com base nos valores individuais, gerar alertas programados quando eles apresentarem incidentes ou falhas;
- Configurar envio de alertas por e-mail;
- Configurar a geração de relatórios customizados de disponibilidade e informações específicas de equipamentos conforme o mesmo que, devidamente configurado, a disponibilize;
- O monitoramento deverá funcionar em regime 24x7 (24 horas por dia, 7 dias por semana).

Neste serviço, deverão ser atendidas as seguintes diretrizes de monitoramento, para que atinja um grau de informação desejado:

Ativo de TI	O que precisa ser monitorado	Protocolos padrão*
Sistemas operacionais dos servidores	Interfaces ethernet (Status UP/DOWN, consumo de rede), Carga de CPU, Memória RAM (total, livre e utilizada), Espaço em disco total e livre, Terminal services, banco de dados, Asterisk, HTTP, FTP.	- Agente próprio do sistema NMS - SNMP
Servidores	Interfaces ethernet (Status UP/DOWN, consumo de rede), Carga de CPU, Memória RAM (total, livre e utilizada), Espaço em disco total e livre.	- SNMP
Storage	Interfaces ethernet (Status UP/DOWN, consumo de rede), Carga de CPU, Espaço em disco total e livre.	- SNMP - Agente próprio do sistema NMS**
Roteadores	Interfaces ethernet (Status UP/DOWN, consumo de rede)	- SNMP - ICMP

Virtualizadores	Interfaces ethernet (Status UP/DOWN, consumo de rede), Carga de CPU, Espaço em disco total e livre, saúde da aplicação**	- SNMP - Agente próprio do sistema NMS**
Nobreaks	Interfaces ethernet (Status UP/DOWN, consumo de rede), Carga total, Carga Utilizada, Carga Restante, Temperatura, Tensão de entrada e saída, Tempo restante de baterias	- SNMP
Gateways	Interfaces ethernet (Status UP/DOWN, consumo de rede, tráfego), interfaces em uso, status das interfaces, status do dispositivo, status de VPN's	- SNMP - ICMP
Telefones IP	Interfaces ethernet (Status UP/DOWN, consumo de rede), status de conta registrada**	- ICMP - SNMP**
Links de internet	Status do link (UP/DOWN), Tráfego e latência	- ICMP

** Podem ser aplicados outros tipos de protocolos ou agentes, dependendo do modelo do dispositivo.*

*** Dependerá do dispositivo ou sistema suportar essa funcionalidade.*

2.3.4. E-mail

Deverá ser fornecida uma solução de e-mail hospedado com alta disponibilidade, com capacidade de 25gb por conta. O acesso deverá ser compatível com sistemas operacionais Windows, Linux, Mac OS, Android, IOS, navegadores Chrome, Internet Explorer, Firefox e Safari. O mesmo deverá possuir a possibilidade de sincronização das mensagens com clientes de e-mail, como Outlook, Mozilla Thunderbird ou algum outro, desde que este trabalhe com os protocolos IMAP e POP3.

2.3.5. Internet

Devido a vários serviços importantes que o SAMU utiliza sob a internet durante o dia, é necessário que sejam instalados links de internet que trabalhem em redundância na sede operacional, ou seja, caso o link principal pare, os secundários assumirão instantaneamente, garantindo uma maior segurança e confiabilidade no serviço. O link deverá apresentar as seguintes características:

2.3.5.1. Internet Setores Administrativo e Regulação

Link para acesso à rede mundial de computadores, INTERNET, de velocidade de 100 Mbps com garantia de banda de 80% sobre o valor nominal do link, que suporte aplicações TCP/IP e proveja o acesso à rede internet. Fornecimento de, no mínimo, 01 (um) endereço IPv4 público e válido na internet. O acesso deverá ser permanente (24 horas por dia e 07 dias por semana, a partir de sua ativação). Garantia e atendimento preferencial com SLA de no mínimo 97% (ou 10 dias parados em 365 dias do ano), sendo que não poderão ser dias consecutivos ou mais de dois dias no mesmo mês ou mês seguinte. Fornecimento de equipamentos para instalação do link, bem como para o funcionamento do mesmo. A tecnologia de acesso deverá ser através de fibra óptica ou par metálico. A entrega do link deverá ser feita com cabo de rede padrão categoria 5e e conectores RJ45 tipo 568B. O link deverá ser monitorado 24hs por dia.

2.3.5.2 Almoxarifado

Link para acesso à rede mundial de computadores, INTERNET, de velocidade de 50 Mbps com garantia de banda de 50% sobre o valor nominal do link. Garantia e atendimento preferencial com SLA de no mínimo 97% (ou 10 dias parados em 365 dias do ano), sendo que não poderão ser dias consecutivos ou mais de dois dias no mesmo mês ou mês seguinte. Fornecimento de equipamentos para instalação do link, bem como para o funcionamento do mesmo. A tecnologia de acesso deverá ser através de fibra óptica, par metálico ou rádio. A entrega do link deverá ser feita com cabo de rede padrão categoria 5e e conectores RJ45 tipo 568B. O link deverá ser monitorado 24hs por dia.

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: 7FE0-0754-7858-8E97

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

DAUDICEIA RENATA MOREIRA (CPF 033.XXX.XXX-80) em 17/12/2025 15:22:24 GMT-03:00
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://cisdeste.1doc.com.br/verificacao/7FE0-0754-7858-8E97