**TERMO DE REFERÊNCIA**

Considerando as disposições da Lei n.º 14.133/2021, suas posteriores alterações e o Decreto municipal nº 936/2022 e 937/2022, bem como conforme exposto e fundamentado no Estudo Técnico Preliminar, ante ao interesse público, a Fundação Estatal de Saúde de Maricá – FEMAR, realizará processo licitatório na modalidade Pregão Eletrônico, objetivando a **CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM EXPANSÃO E SOLUÇÕES DE REDE**,a fim de atender a demanda da FEMAR na consecução de suas atividades – meio e fim.

1. **CONDIÇÕES GERAIS DA CONTRATAÇÃO**
	1. O presente Termo de Referência tem por objeto a contratação de serviço para ampliação de solução integrada de infraestrutura de suporte a serviços em rede, a fim de atender a demanda da FEMAR na consecução de suas atividades – meio e fim, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **DESCRIÇÃO** | **TIPO** | **QTD.** |
| 1 | Câmera de Vídeo IP Tipo I com Licença de software e instalação | un. | 61 |
| 2 | Câmera de Vídeo IP Tipo II com Licença de software e instalação | un. | 131 |
| 3 | Câmera de Vídeo IP Tipo III com Licença de software e instalação | un. | 205 |
| 4 | Comutador | un. | 4 |
| 5 | Instalação do item 4 | un. | 4 |
| 6 | Firewall/Roteador Tipo I com licença de software para plataforma de gerenciamento em nuvem | un. | 16 |
| 7 | Instalação do item 6 | un. | 16 |
| 8 | Firewall/Roteador Tipo II com licença de software para plataforma de gerenciamento em nuvem | un. | 2 |
| 9 | Instalação do item 8 | un. | 2 |
| 10 | Gateway de voz | un. | 2 |
| 11 | Instalação do item 10 | un. | 2 |
| 12 | Ponto de Acesso WiFi 6 + Licença de software para plataforma de gerenciamento em nuvem e instalação | un. | 158 |
| 13 | Módulo de interface SFP, 1000BASE-LX e instalação | un. | 40 |
| 14 | Patch Panel 24 Portas e instalação | conj. | 136 |
| 15 | Patch Panel descarregado de 24 Portas e instalação | un. | 4 |
| 16 | Ponto de Rede Tipo I e instalação | conj. | 1.337 |
| 17 | Ponto de Rede Tipo II e instalação | conj. | 1.516 |
| 18 | Ponto de Rede Tipo III e instalação | conj. | 160 |
| 19 | Rack de Piso de 19" Fechado de 12U e instalação | un. | 5 |
| 20 | Rack de Piso de 19" Fechado de 42U e instalação | un. | 15 |
| 21 | Rack de Piso de 19" Fechado de 44U e instalação | un. | 2 |
| 22 | Sensor IP de Temperatura e Umidade do ar com interface Ethernet com licença de software para plataforma de gerenciamento em nuvem e instalação | un. | 55 |
| 23 | Servidor de comunicação unificada IP | un. | 2 |
| 24 | Instalação do item 23 | un. | 2 |
| 25 | Servidor de hiperconvergência com licença de software | un. | 6 |
| 26 | Instalação do item 25 | un. | 6 |
| 27 | Solução de Backup + Licença de software | un. | 2 |
| 28 | Instalação do item 27 | un. | 2 |
| 29 | Subscrição de Software HCI | un. | 192 |
| 30 | Instalação do item 29 | un. | 192 |
| 31 | Switch L2, 24 portas Gigabit Ethernet, stackable (empilhável), PoE+ com licença de software para plataforma de gerenciamento em nuvem | un. | 1 |
| 32 | Instalação do item 31 | un. | 1 |
| 33 | Switch L2, 48 portas Gigabit Ethernet, stackable (empilhável), PoE+ com licença de software para plataforma de gerenciamento em nuvem | un. | 63 |
| 34 | Instalação do item 33 | un. | 63 |
| 35 | Telefone IP Tipo I com Licença de software e instalação | un. | 611 |
| 36 | Telefone IP Tipo II com Licença de software e instalação | un. | 98 |
| 37 | Telefone IP Tipo III com Licença de software e instalação | un. | 32 |
| 38 | Suporte Técnico e Manutenção | mês | 12 |

* 1. As informações constantes na tabela contêm a indicação das unidades e quantidades estimadas, em função do consumo e utilização prováveis, no entanto, informa-se que a descrição detalhada dos itens que compõem o objeto do presente processo encontra-se pormenorizada no **Anexo A** do presente documento.
	2. Trata-se de prestação de serviço contínuo em ampliação de solução integrada de infraestrutura de suporte a serviços em rede, a ser contratado mediante licitação e aquisição de equipamentos de Tecnologia da Informação e Comunicações – TIC, na modalidade pregão, em sua forma eletrônica, por meio do procedimento auxiliar de Registro de Preços, conforme definido no art. 6º, incisos X e XIII da Lei n.º 14.133/2021, uma vez que os padrões de desempenho e qualidade estão objetivamente definidos, tendo como base as especificações usuais de mercado;
	3. O prazo de vigência da contratação é de 12 (doze) meses, contados da comunicação formal, na forma do art. 107 da Lei n° 14.133/2021, prorrogável por interesse das partes, até o limite de 10 (dez) anos, desde que haja autorização formal da autoridade competente.
	4. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.
1. **FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO**
	1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em Tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.
2. **DESCRIÇÃO DA SOLUÇÃO COMO UM TODO**
	1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.
3. **REQUISITOS DA CONTRATAÇÃO**
	1. A contratação deverá observar os seguintes requisitos de contratação:
		1. Cumprir os requisitos técnicos previstos na Portaria Inmetro nº 170/2012.
		2. Atender as Normas Nacionais e Padrões Internacionais abaixo:
4. ABNT–NBR14565 – Cabeamento estruturado para edifícios comerciais e data centers;
5. ANSI/TIA-568-C.1 – Norma de cabeamento de telecomunicações em edifícios comerciais;
6. ANSI/TIA-568-C.2 – Norma de cabeamento de par trançado e componentes para telecomunicações;
7. NEMA - National Electrical Manufacturers Association;
8. IEEE – Institute of Electrical and Electronics Engineers;
9. IEC - International Electric Commission;
10. ANSI - American National Standard Institute
11. EIA - Electronic Industries Alliance;
12. TIA – The Telecommunications Industry Association.
	1. Manter o mais completo e absoluto sigilo sobre os dados, materiais, documentos e informações que serão acessados, direta ou indiretamente, durante a execução do objeto, devendo orientar os profissionais envolvidos a cumprir esta obrigação, respeitadas, inclusive, as normas previstas na Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).
	2. A solução de comunicação *wireless* deverá utilizar controladora baseada em nuvem, sendo responsável pelas funções de administração, configuração e gerenciamento da rede sem fio.
	3. A configuração dos Pontos de Acesso (*Access Point*) deverá ser por meio de plataforma em nuvem, de modo que os parâmetros operacionais, bem como o gerenciamento das políticas de segurança e de radiofrequência sejam gerenciadas pela Controladora *Wireless* em nuvem, cujo fabricante deverá ser o mesmo do Ponto de Acesso, a fim de garantir total interoperabilidade. A estratégia da solução de gerenciamento em nuvem adotada para os Pontos de Acesso também deverá ser utilizada para os *switches, firewalls* e câmeras de videomonitoramento a serem fornecidos, de modo a ser utilizado um único *dashboard* para funções de administração, configuração e gestão completa e centralizada desses ativos.
	4. Os ativos de voz ofertados deverão ser genuinamente baseados em plataforma IP e totalmente integrados à solução.
	5. A solução de gerenciamento em nuvem deverá incluir funções de segurança contra padrões de comportamentos hostis, tentativas de ataque cibernético, bem como definições de filtros para análise de conteúdo, de modo a prover proteção aos dispositivos e usuários locais.
	6. A instalação de cabeamento estruturado nas Unidades de Saúde da Família (USF) e galpões, em conformidade com a NBR 14565, NBR 16415 e demais normas pertinentes, é de inteira responsabilidade da Contratada.

**Da Sustentabilidade**

* 1. Além dos critérios de sustentabilidade eventualmente ao longo deste Termo de Referência, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis, no que couber:
		1. A Contratada deve responsabilizar-se pela correta destinação final de todos os resíduos gerados pelos produtos fornecidos que necessitam de destinação ambientalmente adequada bem como, realizar descarte em local devidamente licenciado pelo órgão competente.
		2. A Contratada deverá executar os serviços em conformidade com as orientações e normas voltadas para a sustentabilidade, bem como para as práticas sustentáveis, no que se refere a economia de energia; economia de água; reciclagem do lixo.
		3. Além disso, cabe a empresa a ser contratada, sempre que possível, realizar práticas sustentáveis de manejo dos recursos renováveis, a redução dos resíduos e poluições, a utilização de energia e materiais eficientemente energéticos (economia de energia), empregando equipamentos condizentes com às normas e preservação ambiental.
		4. A Contratada deverá executar os serviços respeitando e atendendo as Normas Brasileiras Regulamentadoras – NBR e todas as normas atinentes ao objeto do contrato, existentes ou que venham a ser editadas.

**Da exigência de amostra**

* 1. Não haverá exigência de amostra da contratação.

**Da indicação de marcas ou modelos**

* 1. Salienta-se que as especificações dos itens, objeto deste Termo de Referência são suficientes à escolha do futuro contratado, certificando ainda, que não há determinação de marca, nem tão pouco importam em cerceamento da competitividade do certame.

**Da Subcontratação**

* 1. Não é admitida a subcontratação do objeto contratual.

**Da Garantia da Contratação**

* 1. Não haverá exigência da garantia da contratação dos artigos 96 e seguintes da Lei nº 14.133, de 2021, por se tratar de objeto de baixo risco e complexidade, conforme descrito no item 1 – Das Condições Gerais da Contratação deste Termo de Referência;

**Da Visita Técnica**

* 1. Para o correto dimensionamento e elaboração de sua proposta, o licitante poderá realizar vistoria nas instalações do local de execução dos serviços, acompanhado por empregado designado para esse fim, de segunda à sexta-feira, das 10h (dez horas) às 16h (dezesseis horas), em dias úteis, com posterior emissão do Certificado de Visita Técnica, sendo concedidos 15 min (quinze minutos) de tolerância para atrasos, devendo o agendamento ser efetuado previamente pelo e-mail: infra.ti.femar@gmail.com ou pelo telefone (21) 97180-0865.
	2. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até o dia útil anterior à data prevista para a abertura da sessão pública.
	3. Para a vistoria o licitante, ou seu representante legal, deverá estar devidamente identificado, apresentando o documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.
	4. A licitante deverá declarar que tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.
	5. Será realizada individualmente a visita técnica com os licitantes interessados, a fim de evitar que o universo de concorrentes seja conhecido antes da licitação.
	6. As empresas interessadas poderão **dispensar a visita técnica, desde que assim a declarem** e em hipótese alguma poderá ser alegado desconhecimento, incompreensão, dúvida ou esquecimento das cláusulas e condições do contrato e das especificações técnicas ou de qualquer documento parte desta contratação.
	7. É de fundamental importância o interesse da licitante em ter pleno conhecimento de todas as informações que se relacionam com a execução do objeto deste Termo de Referência, a serem disponibilizados na visita técnica, incluindo-se as condições do local dos serviços, transportes, energia, abastecimento, bem como quaisquer dificuldades eventuais relacionadas às atividades pertinentes à disponibilização e instalação dos equipamentos e serviços.
1. **MODELO DE EXECUÇÃO DO OBJETO**
	1. A prestação dos serviços em comento se dará de forma parcelada, conforme a necessidade, visando minimizar os custos desnecessários, bem como garantir que a Administração tenha a discricionariedade de agir conforme suas demandas, podendo flexibilizar suas despesas, com a devida adequação aos recursos disponíveis, na forma autorizada pelo Art. 40, inciso V, alínea b, da Lei nº 14.133, de 2021.
	2. A execução do objeto seguirá a seguinte dinâmica:
		1. Após a comunicação formal da Contratante, o fornecedor terá o prazo de até **30 (trinta) dias úteis**, para entrega dos ativos e execução da solução de infraestrutura integrada a partir da solicitação realizada pela Diretoria Requisitante.
	3. A Contratada deverá comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas, que antecede a prazo de entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação, para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.
	4. O prazo referido no subitem anterior poderá ser postergado a critério da Contratante.
	5. Deverá ser elaborada e entregue toda a documentação técnica da solução em formato texto, planilha e gráfica. Os desenhos, quando em formato *.dwg*, terão suas pranchas com as dimensões mínimas no formato A-1, preferencialmente, e no máximo A-0 da ABNT (Associação Brasileira de Normas Técnicas). As escalas mínimas serão de:
2. 1:2000 (um para dois mil) para plantas gerais esquemáticas de localização;
3. 1:500 (um para quinhentos) para plantas de situação;
4. 1:50 (um por cinquenta) ou 1:100 (um por cem) para plantas baixas e cortes;
5. 1:25 (um por vinte e cinco) para os detalhes;
6. Relação mínima entre escalas vertical e horizontal:

$$\frac{E\_{v}}{E\_{h}}\geq 10$$

* 1. Os serviços executados em vias públicas deverão ter os seus horários agendados e liberados pela FEMAR.
	2. O *datacenter* principal será implantado na sede da FEMAR, localizada à Rua Clímaco Pereira nº 367, lote b1 e b2 – Araçatiba – Maricá/RJ, cep: 24.902-035 e centralizará o tráfego das aplicações de/para 15 (quinze) Unidades de Saúde da Família (USF). Deve ser instalado, ainda, nas dependências da FEMAR, *datacenter* secundário (contingência), de modo a permitir a continuidade dos acessos em caso de indisponibilidade do *datacenter* principal.
	3. Todos os locais onde houver passagem de dutos (eletrocalhas, eletrodutos, etc.) por superfícies de vidro (janelas fixas, painéis, etc.) devem ter o vidro anteriormente retirado, recortado exatamente nas dimensões do elemento passante e recolocado de forma a assumir a mesma posição e qualidade de fixação previamente existente.
	4. Não será emitido aceite do serviço para os locais em que não tiverem sido reparados todos os danos causados.

**Do Prazo e Local de Entrega**

* 1. A entrega dos equipamentos deverá ser realizada na Superintendência de Infraestrutura – Fundação Estatal de Saúde de Maricá – FEMAR, situada na Rua Clímaco Pereira nº 367 lote b1 e b2 – Araçatiba – Maricá/RJ, cep: 24.902-035, e nas Unidades de Saúde da Família descritas no **Anexo B**, do presente documento, no período compreendido entre 09h e 16h, de segunda à sexta-feira, em dias úteis.
	2. Os serviços poderão ser rejeitados, no todo ou em parte, quando realizados em desacordo com as especificações constantes neste Termo de Referência e na proposta, bem como caso seja detectado qualquer vício ou defeito, em sua prestação, devendo ser corrigidos/refeitos/substituídos no prazo de 5 (cinco) dias úteis, a contar da comunicação formal da Contratante.
	3. A reposição deverá ser por outro material com especificações técnicas iguais, ou superiores, com aprovação prévia da Contratante, e às custas da Contratada, sem prejuízo da aplicação das penalidades cabíveis, na forma do artigo 119 da Lei nº 14.133/2021;
	4. Toda logística para entrega do objeto da contratação nos endereços informados, ficará integralmente por conta da Contratada.

**Da Garantia do Equipamentos**

* 1. O prazo de garantia dos equipamentos é aquele estabelecido em cada um dos itens previstos no Anexo A do presente Termo de Referência.
	2. A cobertura de garantia prevê a substituição de peças, módulos e equipamentos fornecidos pela CONTRATADA para atendimento do Edital. Todos os equipamentos serão novos e com o prazo previsto no Anexo A, contados a partir do recebimento definitivo do item da solução.

**Do Suporte Técnico**

* 1. Entende-se por **suporte técnico** a prestação de serviços especializada, prestada por profissionais devidamente qualificados, com experiência no escopo do objeto deste Termo de Referência consubstanciada no ato efetivo de solicitar assistência técnica visando à solução de problemas de caráter técnico, operacional ou funcional, à orientação no uso, à instalação e à configuração de dispositivos, equipamentos, periféricos, bem como de softwares especificados neste instrumento.
	2. O suporte técnico deverá estar disponível na modalidade de **24x7 (24 horas por dia, 7 dias por semana)**, com **vigência de 12 meses**, e abrangem os serviços de natureza corretiva, preventiva e evolutiva referentes à manutenção para todos os materiais, equipamentos e softwares que compõem a solução integrada de infraestrutura de rede.
	3. A empresa CONTRATADA deverá proporcionar corpo técnico qualificado e especializado para garantir os serviços de manutenção e suporte on-site.

**Das Manutenções Preventivas e Corretivas e Assistência Técnica**

* 1. Os serviços de **manutenção corretiva** são aqueles efetuados com objetivo de solucionar problemas de funcionamento e disponibilidade dos sistemas, incluindo a substituição de peças e equipamentos, caso seja constatada a impossibilidade de manutenção.
	2. A manutenção corretiva será procedida quando a FEMAR acusar funcionamento irregular de algum dos equipamentos contidos no contrato. Depois de efetuado o atendimento corretivo, a CONTRATADA informará formalmente à FEMAR, e em caso de ocorrência de não solução do problema, deverá ser informado o prazo para restabelecimento, quando este for maior do que o estabelecido na tabela de acordos de nível de serviço (SLA).
	3. Todos os serviços necessários para o pronto reestabelecimento dos equipamentos e sistemas contratados correrão por conta da empresa CONTRATADA.
	4. A empresa CONTRATADA deverá prestar suporte de serviços, compreendendo reparos e substituições de peças, às suas expensas, obrigando-se a colocar os equipamentos em perfeito estado de funcionamento, no prazo máximo estabelecido no SLA de atendimento, contado a partir da abertura do chamado.
	5. Em caso de necessidade de troca de equipamento, a empresa CONTRATADA será responsável por intermediar com o fabricante o processo substituição. Caso a previsão de resolução do problema ultrapasse o previsto no SLA, deverá ser disponibilizado equipamento equivalente até que a troca seja efetivada.
	6. Os serviços de **manutenção preventiva** são aqueles nas quais a CONTRATADA realiza ações planejadas de verificação periódica da saúde e funcionamento do sistema implementado, permitindo um diagnóstico preciso do “status” atual do ambiente. Essas ações incluem:
	7. Testes periódicos de conexões de cabeamento lógico;
	8. Testes de desempenho dos elementos da rede lógica;
	9. Testes de desempenho de componentes de servidores;
	10. Limpeza de cúpulas de câmeras;
	11. Limpeza de contatos elétricos;
	12. Verificação, via SNMP, das condições físicas e lógicas dos servidores, unidades de armazenamento, *(storage)*, *switches, access points* e demais equipamentos contemplados neste ETP.
	13. A CONTRATADA deverá manter alta disponibilidade dos servidores e *storages*, de modo que o ambiente de instalação nos dois datacenters possa prover, em caso de falha, uma transição transparente entre servidores e sem interrupção dos sistemas instalados para o usuário final.
	14. Sempre que tais ações implicarem em paradas parciais ou totais da rede, estas deverão ser agendadas com a FEMAR com antecedência de uma semana.
	15. Deverá ser apresentado um plano de ação e cronograma de manutenção preventiva até 30 dias após a assinatura do Contrato, visando à adequação das ações da FEMAR e da CONTRATADA, bem como dos usuários da rede.
	16. Todos os materiais e insumos necessários a essas manutenções deverão estar inclusos nos valores das propostas apresentadas.
	17. Integra a manutenção preventiva a correção de todas as condições de irregularidade da instalação física dos equipamentos, como: reparo nas proteções, suspensões e fixações dos aparelhos (chumbadores, bases, abraçadeiras, mão francesa etc.).
	18. A manutenção preventiva é obrigatória em todos os equipamentos contratados, no mínimo, uma vez a cada 30 (trinta) dias corridos.
	19. Os serviços de **manutenção evolutiva** são aqueles em que a CONTRATADA, mediante solicitação da CONTRATANTE, implementará atualizações de software para os equipamentos objeto deste contrato, mantendo a solução em pleno funcionamento e na versão desejada pela CONTRATANTE.

**Acordos de Nível de Serviço (SLA) para serviços de suporte técnico em regime 24x7**

* 1. Para realização dos serviços de manutenção preventiva e corretiva com suporte técnico 24x7 deverão ser respeitados os acordos de tempo e especificação de atendimentos conforme Tabela 4 e Tabela 5.
		1. Classificação das prioridades para a regularização do funcionamento:

**Tabela 3** – Tipos de Prioridade

|  |  |  |
| --- | --- | --- |
| **Prioridade 1** | **Urgente** | O problema causa perda ou paralisação total do equipamento ou solução. A não operação passa a ser crítica para o negócio do cliente e a situação constitui uma emergência. Completa falha do equipamento ou solução. O equipamento ou solução continua no mesmo estado indefinidamente, causando demoras inaceitáveis ou indefinidas para recursos ou respostas. O equipamento ou solução falha repetidamente, após as tentativas de reinicialização. |
| **Prioridade 2** | **Média** | O problema causa uma perda de funcionalidade. As operações podem continuar ainda que de modo restrito. Problema de performance do equipamento ou solução. Equipamentos ou solução sem controle, mantidos pela redundância. O problema restringe a disponibilidade do equipamento ou da solução. |
| **Prioridade 3** | **Normal** | Falha de componentes ou módulos isolados que não resultem em restrições substanciais. O problema causa perda menor de funcionalidade, constituindo uma inconveniência. Erro irrelevante, comportamento incorreto ou erro de documentação, que de nenhuma maneira impede a operação do equipamento. O problema é pontual e não afeta seriamente a operação do equipamento. Baixo impacto no negócio do cliente. |

* + 1. SLA de atendimento e solução do problema:

**Tabela 4** – Níveis de Prioridade

|  |  |  |  |
| --- | --- | --- | --- |
| **Nível de Prioridade** | **Tipo** | **SLA de atendimento** | **SLA de Solução do Problema** |
| Prioridade 1 | Urgente | Em até 4 horas a partir do contato realizado com a contratada. | Em até 24 horas do contato realizado com a contratada. |
| Prioridade 2 | Média | Em até 6 horas a partir do contato realizado com a contratada. | Em até 48 horas a partir do contato realizado com a contratada. |
| Prioridade 3 | Normal | Em até 8 horas a partir do contato realizado com a contratada. | Em até 72 horas a partir do contato realizado com a contratada. |

* 1. A empresa CONTRATADA deverá prestar suporte de serviços, compreendendo reparos e substituições de peças ou demais componentes, às suas expensas, obrigando-se a colocar os equipamentos em perfeito estado de funcionamento, no prazo máximo estabelecido no SLA de atendimento, contado a partir da abertura do chamado.
	2. Todas as ocorrências relativas ao não cumprimento dos prazos estipulados serão registradas e calculadas pela fiscalização, conforme a Tabela 5.

**Tabela 5** – Níveis de Prioridade

|  |  |
| --- | --- |
| **Nível de Prioridade** | **Pontuação** |
| Prioridade 1 | 1,0 |
| Prioridade 2 | 0.5 |
| Prioridade 3 | 0,3 |

* 1. A cada mês será apurado o somatório da pontuação decorrente dos registros de ocorrências. Esta soma servirá como base para que a FEMAR aplique as sanções administrativas descritas na Tabela 6, de modo que, atingindo o quantum necessário à configuração de uma sanção, esta será imediatamente aplicada, observado o processo administrativo.

**Tabela 6** – Relação da Pontuação

|  |  |
| --- | --- |
| **Pontuação acumulada** | **Advertência/Glosa** |
| 1 ponto | Advertência, caso não tenha sido aplicado anteriormente durante a vigência do contrato |
| 2 a 4 pontos | Glosa correspondente a 3% do valor mensal da Fatura. |
| 5 a 7 pontos | Glosa correspondente a 5% do valor mensal da Fatura. |
| 8 a 10 pontos | Glosa correspondente a 10% do valor mensal da Fatura. |
| Acima de 10 pontos | Glosa correspondente a 20% acrescido de 3% a cada ponto extra, do valor mensal da Fatura. |

* 1. O resultado da apuração da pontuação e respectivo redimensionamento do pagamento será comunicado pela fiscalização, por meio de notificação formal à CONTRATADA, que terá 5 (cinco) dias úteis, a partir do recebimento da comunicação, para contestar.
	2. A CONTRATADA poderá apresentar justificativa para a prestação do serviço com menor nível de conformidade, que poderá ser aceita pelo fiscal técnico, desde que comprovada a excepcionalidade da ocorrência, resultante exclusivamente de fatores imprevisíveis e alheios ao controle do prestador, conforme disposto no item 3.2, anexo VIII-A da IN SLTI/MPOG nº 05/2017.
	3. Na hipótese de comportamento contínuo de desconformidade da prestação do serviço em relação à qualidade exigida, bem como quando esta ultrapassar os níveis mínimos toleráveis previstos nos indicadores, além dos fatores redutores, devem ser aplicadas as sanções à contratada de acordo com as regras previstas no ato convocatório.
	4. Para efeito de recebimento provisório, ao final de cada período mensal, a FISCALIZAÇÃO do Contrato deverá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos no ato convocatório, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao Gestor do Contrato;
	5. A cada redimensionamento, os valores do somatório serão zerados, de forma a não haver duplicidade.
	6. Em caso de a CONTRATADA somar 10 pontos, fica facultada à FEMAR a rescisão unilateral sem ônus financeiro do Contrato.
	7. A fim de não haver descontinuidade dos serviços, no caso acima, a FEMAR poderá aguardar a efetivação de nova contratação para rescindir unilateralmente o Contrato.

**Dos Procedimentos de Transição e Finalização do Contrato**

* 1. A Contratada compromete-se a prestar serviços de suporte e migração de arquivos, caso o contrato vigente entre as partes não seja renovado, todos os arquivos deverão ser encaminhados a um servidor apontado pelo Contratante, restaurando os serviços e acessos assim como presentes no atual servidor, de acordo com os termos e condições estabelecidos.
	2. A Contratada deverá garantir que a migração dos arquivos da Contratante seja realizada de forma segura, seguindo as melhores práticas e normas de segurança da informação vigentes.
	3. A migração dos arquivos da Contratante deverá ser realizada em conformidade com a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), garantindo a devida segurança e privacidade das informações pessoais contidas nos arquivos.
	4. A migração dos arquivos da Contratante será realizada exclusivamente sob o comando e orientação da Contratante, garantindo assim que todas as suas necessidades e requisitos sejam atendidos durante o processo
	5. A Contratada assume a responsabilidade de eliminar todos os dados e aplicações relacionados a Contratante contidos nos servidores da contratada de forma segura e definitiva após a migração ser realizada, em conformidade com a Lei Geral de Proteção de Dados (LGPD) (Lei nº 13.709/2018), garantindo a proteção da privacidade e a conformidade legal no tratamento dos dados.
1. **MODELO DE GESTÃO DO CONTRATO**
	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.
	2. As comunicações entre a FEMAR e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se, excepcionalmente, o uso de mensagem eletrônica para esse fim.
	3. A FEMAR poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.
	4. A execução do Contrato e a respectiva prestação dos serviços será acompanhada e fiscalizada por 02 (dois) funcionários a serem designados pela Diretoria Requisitante da FEMAR, na condição de representantes da CONTRATANTE.
	5. A execução do contrato deverá ser acompanhada e fiscalizada pelos fiscais do contrato, ou pelos respectivos substitutos, conforme art. 117, *caput*, da Lei nº 14.133/2021.
		1. O fiscal do contrato anotará em registro próprio todas as ocorrências relacionadas à execução do contrato, recomendando o que for necessário a regularização das faltas ou dos defeitos observados;
		2. Informar ao gestor do contrato, as ocorrências que demandem a adoção de medidas necessárias e saneadoras, bem como quaisquer ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas;
		3. Examinar a regularidade no recolhimento das contribuições fiscais, trabalhistas e previdenciárias e, em caso de descumprimento, informar imediatamente ao gestor do contrato para a adoção das medidas necessárias;
	6. O Gestor do Contrato deverá coordenar as atividades relacionadas à fiscalização, bem como dos atos preparatórios à instrução processual e encaminhar a documentação pertinente ao setor de contratos para formalização dos procedimentos quanto aos aspectos que envolvam a prorrogação, alteração, reequilíbrio, pagamento, eventual aplicação de sanções, extinção dos contratos, dentre outros.
	7. A Fiscalização técnica deverá acompanhar o contrato com o objetivo de avaliar a execução do objeto nos moldes contratados e, se for o caso, aferir se a quantidade, qualidade, tempo e modo da prestação ou execução do objeto estão compatíveis com os indicadores estipulados no edital, para efeitos de pagamento conforme o resultado pretendido pela Diretoria Requisitante.
	8. A Fiscalização deverá elaborar relatório final, de que trata a alínea “d”, do inciso VI, do §3º do art. 174 da Lei nº 14.133/2021, com as informações quanto à execução do contrato, concluindo com as lições aprendidas, como forma de aprimoramento das atividades da FEMAR.

**Do Reajuste**

* 1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, conforme art. 25, § 7° da Lei n.º 14.133/2021.
	2. Após o interregno de um ano, a contar da data do orçamento estimado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do índice IPCA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.
1. **DOS CRITÉRIOS DE MEDIÇÃO E PAGAMENTO**

**Do Recebimento do Objeto**

* 1. O **recebimento provisório** ocorrerá, no prazo de 5 (cinco) dias úteis, após o recebimento e início da execução dos serviços, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelos responsáveis pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência;
	2. O **recebimento definitivo** ocorrerá no prazo de 5 (cinco) dias úteis, a contar do recebimento provisório, para que ocorra a observação e vistoria, afim de comprovar o exato cumprimento das obrigações contratuais e consequente aceitação mediante termo de recebimento.
	3. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do objeto, nem a responsabilidade ético-profissional pela perfeita execução do contrato, nos limites estabelecidos pela lei ou pelo contrato.
	4. O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

**Do Pagamento**

* 1. O pagamento será efetuado em parcela única, no prazo de 30 (trinta) dias a contar da certificação de que os itens foram aceitos de forma definitiva, mediante a apresentação de Nota Fiscal/Fatura contendo a descrição dos itens, quantidades, preços unitários e o valor total, nota de entrega atestada e comprovante de recolhimento de multas aplicadas, se houver, e dos encargos sociais, mediante depósito em conta bancária indicada pela Contratada, uma vez satisfeitas as condições estabelecidas neste Termo de Referência.
	2. A Nota Fiscal/Fatura relativa à cobrança deverá ser emitida em nome da Fundação Estatal de Saúde de Maricá, CNPJ: 46.218.698/0001-17.
	3. O pagamento se efetivará após a regular liquidação da despesa, à vista de Nota Fiscal/Fatura apresentada pelo contratado, na forma do Art. 55, §3º, inc. III do Dec. Municipal n.º 936/2022.
	4. Havendo erro no documento de cobrança ou outra circunstância impeditiva, a liquidação da despesa ficará pendente e o pagamento sustado até que a contratada providencie as medidas saneadoras necessárias, não ocorrendo, neste caso, quaisquer ônus por parte da contratante.
1. **DA FORMA E CRITÉRIOS DE SELEÇÃO DE FORNECEDOR**
	1. O fornecedor será selecionado por meio da realização de procedimento de licitação, na modalidade **pregão**, sob a sua forma **eletrônica**, por meio do **sistema de registro de preços,** com adoção do critério de julgamento pelo **menor preço por grupo (grupo único),** no modo de disputa **aberto**.

**Regime de execução**

* 1. O regime de execução do contrato será o de empreitada por preço unitário.
	2. **Da Utilização do Sistema de Registro de Preços**
	3. A escolha do procedimento de Sistema de Registro de Preços visa agilidade nas contratações, tendo em vista que a licitação já estará realizada, as condições de fornecimento estarão ajustadas, os preços e os respectivos fornecedores já estarão definidos. Sendo assim, somente solicitará o fornecimento do objeto, cujo preço foi registrado, quando houver demanda e o fornecedor deverá realizar o fornecimento conforme as condições ajustadas.
	4. Importante destacar que se justifica a adoção do Sistema de Registro de Preços, uma vez que as contratações futuras se darão por meio de entregas parceladas, cuja definição da demanda não é possível ser previamente quantificada com precisão, visando minimizar os riscos de desabastecimento e reduzir os custos necessários - hipóteses do art. 3º, incisos I e II do Decreto Municipal nº 937/2022.
	5. Ressalta-se, ainda, que em observância ao Decreto Regulamentador n° 937/2022, em seu art. 12, inciso II, fica convencionado que **a quantidade mínima a ser cotada por item é de 10% (dez por cento)**.

**Dos Órgãos Participantes do Registro de Preços**

* 1. Define-se, como órgão participante do Sistema de Registro de Preços aFundação Estatal de Saúde de Maricá - FEMAR, por meio da Diretoria Administrativa, conforme repartição de atribuições estabelecida no Regimento Interno da FEMAR, aprovado pela Resolução n.º 04/2023**.**

**Dos Órgãos Não Participantes do Registro de Preços**

* 1. Conforme preconiza o Art. 31 do Decreto Municipal n° 937/2022, a ata de registro de preços, durante sua vigência, poderá ser aderida por órgãos ou entidades do Município que não tenham participado do certame licitatório, mediante anuência do órgão gerenciador da FEMAR, desde que haja tal previsão no edital de licitação de origem e seja realizado estudo que demonstre a viabilidade e a economicidade, bem como demonstre a necessidade de efetivação da adesão em detrimento da realização de um planejamento próprio para a realização do respectivo procedimento licitatório.
	2. Os órgãos e entidades que não participaram do registro de preços, quando desejarem aderir a ata de registro de preços, deverão consultar o órgão gerenciador da FEMAR para manifestação sobre a possibilidade de adesão.
	3. Caberá ao fornecedor beneficiário da ata de registro de preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente de adesão, desde que não prejudique as obrigações presentes e futuras decorrentes da ata, assumidas com o órgão gerenciador e órgãos participantes.
	4. As aquisições ou contratações adicionais a que se refere a adesão não poderão exceder, por órgão ou entidade, a cinquenta por cento dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e órgãos participantes.
	5. O quantitativo decorrente das adesões à ata de registro de preços não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e órgãos participantes, independente do número de órgãos não participantes que aderirem.
	6. Após a verificação do órgão gerenciador, o órgão aderente deverá efetivar a aquisição ou contratação solicitada em até noventa dias, observado o prazo de vigência da ata, devendo cumprir as atribuições inerentes a órgão participante e demais orientações do órgão gerenciador.
	7. A utilização pelos órgãos aderentes de cada item registrado na ata de registro ficará condicionada à existência de saldo dos quantitativos estipulados para os órgãos participantes.
	8. O órgão gerenciador da FEMAR somente poderá autorizar as adesões citadas depois de realizada a primeira aquisição ou contratação por órgão participante da ata de registro de preço.

**Da Vigência da Ata de Registro de Preços**

* 1. A Ata de Registro de Preços terá vigência de 1 (um) ano, e poderá ser prorrogada, por igual período, desde que comprovada que as condições e o preço permanecem vantajosos, nos termos do Art. 18 do Decreto Municipal n.º 937/2022.

**Do Cadastro de Reserva**

* 1. Será incluído na Ata de registro de preços, sob a forma de anexo, o registro dos licitantes que aceitarem cotar os bens com preços iguais aos do licitante vencedor na sequência da classificação do certame (cadastro de reserva), assegurada a preferência de contratação de acordo com a ordem de classificação, bem como do licitante que mantiver sua proposta original, conforme o inciso VI do § 5º do art. 82 da Lei n.º 14.133/21.

**Do Reajuste da Ata de Registro de Preços**

* 1. Os preços registrados poderão ser reajustados anualmente, contados da data da proposta, a pedido do fornecedor e conforme índice previsto no presente documento.
	2. Os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos materiais registrados, cabendo ao Órgão Gerenciador promover as negociações junto aos fornecedores.
	3. Quando o preço registrado se tornar superior ao preço praticado no mercado por álea extraordinária, o Órgão Gerenciador convocará os fornecedores para negociarem a redução dos preços aos valores praticados pelo mercado.
	4. Os fornecedores que não aceitarem reduzir seus preços aos valores praticados pelo mercado serão liberados do compromisso assumido, sem aplicação de penalidade.
	5. A ordem de classificação dos fornecedores que aceitarem reduzir seus preços aos valores de mercado observará a classificação obtida originalmente na licitação.
	6. A redução do preço registrado será comunicada pelo Órgão Gerenciador aos órgãos que tiverem formalizado contratos com fundamento no respectivo registro, para que avaliem a necessidade de efetuar a revisão dos preços contratados.
	7. Quando o preço registrado tornar-se inferior ao preço de mercado, é facultado ao fornecedor requerer, antes do pedido de fornecimento, a atualização do preço registrado, mediante demonstração de fato superveniente que tenha provocado elevação que supostamente impossibilite o cumprimento das obrigações contidas na ata e desde que atendidos os seguintes requisitos:

a) a possibilidade da atualização dos preços registrados seja aventada pelo fornecedor signatário da Ata de registro de preços;

b) a modificação nas condições registradas seja substancial, de forma que seja caracterizada alteração desproporcional entre os encargos do fornecedor signatário da Ata de registro de preços e da FEMAR;

c) seja demonstrado nos autos a desatualização dos preços registrados, por meio de apresentação de planilha de custos e documentação comprobatória correlata que demonstre que os preços registrados se tornaram inviáveis nas condições inicialmente pactuadas.

* 1. A iniciativa e o encargo da demonstração da necessidade de atualização de preço serão do fornecedor signatário da Ata de registro de preços, cabendo ao Órgão Gerenciador a análise e deliberação a respeito do pedido.
	2. Se não houver prova efetiva da desatualização dos preços registrados e da existência de fato superveniente, o pedido será indeferido pela FEMAR e o fornecedor continuará obrigado a cumprir os compromissos pelo valor registrado na Ata de registro de preços, sob pena de cancelamento do registro e aplicação das penalidades administrativas previstas em lei e no Edital.
	3. Na hipótese do cancelamento do registro prevista no sub antecedente, o órgão gerenciador poderá convocar os demais fornecedores integrantes do cadastro de reserva para que manifestem interesse em assumir o fornecimento dos bens pelo preço registrado na Ata de registro de preços.
	4. Comprovada a desatualização dos preços registrados decorrente de fato superveniente que prejudique o cumprimento da Ata, a FEMAR poderá efetuar a atualização do preço registrado, adequando-o aos valores praticados no mercado.
	5. Caso o fornecedor não aceite o preço atualizado pela FEMAR, será liberado do compromisso assumido, sem aplicação de penalidades administrativas.
	6. Liberado o fornecedor na forma do subitem antecedente, o Órgão Gerenciador poderá convocar os integrantes do cadastro de reserva, para que manifestem interesse em assumir o fornecimento dos bens pelo preço registrado.
	7. Na hipótese de não haver cadastro de reserva, a FEMAR poderá convocar os licitantes remanescentes, na ordem de classificação, para negociação e assinatura da Ata de registro de preços no máximo nas condições ofertadas por estes, desde que o valor seja igual ou inferior ao orçamento estimado para a contratação, inclusive quanto aos preços atualizados, nos termos do instrumento convocatório
	8. Não havendo êxito nas negociações, o Órgão Gerenciador deverá proceder à revogação da Ata de registro de preços, adotando de imediato as medidas cabíveis para a satisfação da necessidade administrativa.

**Do Cancelamento do Registro de Preços**

* 1. O registro do fornecedor será cancelado quando:
1. descumprir as condições da Ata de registro de preços, sem justificativa plausível;
2. não retirar a nota de empenho ou instrumento equivalente no prazo estabelecido pela FEMAR, sem justificativa aceitável;
3. não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado;
4. sofrer sanção de impedimento de licitar ou contratar ou de declaração de inidoneidade;
5. não aceitar o preço revisado pela FEMAR.
	1. O cancelamento de registros será formalizado por despacho do Órgão Gerenciador, assegurado o contraditório e a ampla defesa.
	2. O cancelamento do registro de preços poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da Ata, devidamente comprovados e justificados:
6. por razão de interesse público; ou
7. a pedido do fornecedor.

**Da Habilitação**

* 1. Para fins de contratação, deverá o fornecedor comprovar os seguintes requisitos de habilitação: *i.* Habilitação Jurídica (Art. 66, Lei nº 14.133/2021); *ii.* Habilitações fiscal, social e trabalhista (Art. 68, Lei nº 14.133/2021); *iii*. Habilitação econômico-financeira (Art. 69, Lei nº 14.133/2021); e *iv.* Habilitação Técnica (Art. 67, Lei nº 14.133/2021), cujas quais serão pormenorizadas em Edital.

**Da Habilitação Técnica (art. 67, Lei nº 14.133/2021)**

* 1. Os critérios de habilitação técnica a serem atendidos pelo fornecedor serão:
1. 01 (um) atestado, no mínimo, emitido por pessoa jurídica de direito público ou privado, em nome da Licitante, que comprove a aptidão para desempenho de atividade pertinente e compatível em características e quantidades com o objeto deste Termo de Referência, de forma satisfatória, demonstrando que a Licitante gerencia ou gerenciou serviços de natureza similar;
2. A fim de comprovar o requisito acima, a Licitante, caso julgue necessário, poderá encaminhar, juntamente com o(s) atestado(s), cópias de contratos, Ordens de Serviços (devidamente assinadas), Notas de Empenho, Notas Fiscais/Faturas ou outros documentos equivalentes.
3. A Licitante deverá disponibilizar todas as informações essenciais à comprovação da legitimidade dos atestados solicitados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, Notas Fiscais/Faturas, Notas de Empenho, endereço atual da Contratante e local em que foram prestados os serviços, sendo que estas e outras informações complementares poderão ser requeridas mediante diligência.
4. **DA PARTICIPAÇÃO DE MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE**
	1. Caso o licitante se enquadre como microempresa, empresa de pequeno porte ou equiparada e queira utilizar-se do tratamento diferenciado a elas destinado, nos termos da Lei Complementar n.º 123/06, deve informar o seu interesse, no momento oportuno, sob pena de, não o fazendo, renunciar a tal tratamento.
		1. O tratamento favorecido a que se refere o subitem acima se dará de duas formas, quais sejam:
5. Para os itens com valor total estimado de até R$ 80.000,00 (oitenta mil reais), a participação é exclusiva a microempresas, empresas de pequeno porte e equiparadas, nos termos do art. 48, inciso I, da Lei Complementar n.º 123/06;
6. Para os itens com valor estimado acima de R$ 80.000,00 (oitenta mil reais), haverá reserva do percentual de **20% (vinte por cento)** exclusivamente para a concorrência entre microempresas, empresas de pequeno porte e equiparadas, na forma do disposto no art. 48, inciso III, da Lei Complementar n.º 123/06, cabendo ampla concorrência para o percentual restante de 80% (oitenta por cento), inclusive com participação de microempresas, empresas de pequeno porte e equiparadas.
	* 1. A obtenção dos benefícios a que se refere o subitem 9.1.1 fica limitada às microempresas, empresas de pequeno porte e equiparadas que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.
		2. Não será concedido tratamento favorecido previsto nos arts. 42 a 49 da LC 123/06:
7. No caso de licitação para aquisição de bens, ao item cujo valor estimado for superior à receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.
	1. Quando não houver um mínimo de 3 (três) fornecedores competitivos enquadrados como microempresas, empresas de pequeno porte ou equiparadas sediados local ou regionalmente e capazes de cumprir as exigências estabelecidas no instrumento convocatório, conforme disposto no art. 49, inciso II, da Lei Complementar n.º 123/06, a totalidade do objeto licitado passará à ampla concorrência, participando tanto microempresas ou empresas de pequeno porte, quanto também empresas assim não enquadradas.
8. **DAS EMPRESAS REUNIDAS EM CONSÓRCIO**
	1. Será vedada a participação de empresas reunidas em consórcio, não havendo elementos que justifiquem tal participação no objetivo em apreço. O objeto em questão não se reveste de alta complexidade, tratando-se de simples contratação de serviço para ampliação de solução integrada de infraestrutura de suporte a serviços em rede.
9. **DAS COOPERATIVAS**
	1. Será permitida a participação de cooperativas, quando:
		1. A constituição e o funcionamento da cooperativa observarem as regras estabelecidas na legislação aplicável, em especial a Lei nº 5.764, de 16 de dezembro de 1971, a Lei nº 12.690, de 19 de julho de 2012, e a Lei Complementar nº 130, de 17 de abril de 2009;
		2. A cooperativa apresentar demonstrativo de atuação em regime cooperado, com repartição de receitas e despesas entre os cooperados;
		3. Qualquer cooperado, com igual qualificação, for capaz de executar o objeto contratado, vedado à Administração indicar nominalmente pessoas;
		4. O objeto da licitação referir-se, em se tratando de cooperativas enquadradas na Lei nº 12.690, de 19 de julho de 2012, a serviços especializados constantes do objeto social da cooperativa, a serem executados de forma complementar à sua atuação.
		5. Apresentem modelo de gestão operacional adequado ao objeto desta licitação, com compartilhamento ou rodízio das atividades de coordenação e supervisão do objeto contratual;
		6. A execução ocorra obrigatoriamente pelos cooperados, vedando-se qualquer intermediação ou subcontratação.
	2. Em sendo permitida a participação de cooperativas, serão estendidas a elas os benefícios previstos para as microempresas e empresas de pequeno porte quando elas atenderem ao disposto no art. 34 da Lei n.º 11.488/07.
10. **DAS OBRIGAÇÕES DAS PARTES**

**Das Obrigações da Contratada**

* 1. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Termo de Referência, acompanhado da respectiva nota fiscal;
	2. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27 do Código de Defesa do Consumidor – Lei n.º 8.078/1990;
	3. Observar os prazos para a execução do objeto, bem como montagem e instalação;
	4. Comunicar, por escrito, eventual atraso ou paralisação das entregas, apresentando razões justificadas que serão objeto de apreciação pela FEMAR;
	5. Manter-se, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, as condições de habilitação e qualificação exigidas;
	6. Indicar preposto para representá-la durante a execução do contrato;
	7. Responsabilizar-se pelos encargos fiscais, comerciais e trabalhistas, resultantes da execução do contrato, devendo, portanto, responsabilizar-se por todos os ônus referentes a entrega e/ou execução do serviço à Diretoria Requisitante, na forma da Lei nº 14.133/2021, Art. 121, *caput*;
	8. Responder pelos danos causados diretamente à Administração desta Fundação ou a terceiros, decorrentes de sua culpa ou dolo, quando da entrega do objeto, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pela FEMAR, na forma da Lei nº 14.133/2021, art. 120;
	9. Reparar e providenciar acabamento de alvenaria/gesso e pintura em todo e qualquer furo, corte, passagem e demais alterações que forem feitas em elementos arquitetônicos do prédio (alvenaria, gesso, aberturas) de forma a apresentarem a mesma qualidade de acabamento previamente existente.
	10. A licitante deverá prever nos seus custos as despesas com atividades secundárias relacionadas aos reparos, sinalizações, serviços e materiais eventuais relacionados aos reparos.
	11. Apresentar, sempre que solicitada, documentos que comprovem a procedência do objeto fornecido;
	12. Acatar as instruções emanadas da fiscalização.
	13. Proporcionar todas as facilidades indispensáveis ao bom cumprimento das obrigações contratuais;
	14. A inadimplência do contratado em relação aos encargos trabalhistas, fiscais e comerciais não transferirá à Administração a responsabilidade pelo seu pagamento e não poderá onerar o objeto do contrato, na forma da Lei nº 14.133/2021, Art. 121, §1º.
	15. A Contratada deverá garantir a qualidade do serviço ofertado, devendo realizar a correção em caso de defeito no objeto contratado, correndo todo o ônus por sua conta.

**Das Obrigações da Contratante**

* 1. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;
	2. Verificar minuciosamente, no prazo fixado, a conformidade do objeto recebido provisoriamente com as especificações constantes neste Termo e na proposta, para fins de aceitação e recebimento definitivo;
	3. Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no cumprimento contratual para que seja substituído, reparado ou corrigido;
	4. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através dos fiscais de contrato;
	5. A Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, incluindo encargos tributários e trabalhistas, ainda que vinculados à execução do presente Termo de Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.
	6. Designar funcionários, para acompanhar e fiscalizar o cumprimento contratual, bem como para aprovar a execução do objeto, exercer o acompanhamento e fiscalização do contrato;
	7. Exigir da Contratada, sempre que necessário, a comprovação da manutenção das condições de habilitação e de qualificação exigidas no procedimento de contratação;
	8. Efetuar o pagamento devido, após o adimplemento da obrigação, no prazo e forma estabelecidos no Termo de Referência, mediante Nota Fiscal/fatura devidamente atestada, desde que cumpridas todas as formalidades e as exigências da contratação;
1. **DA VALIDADE DAS PROPOSTAS**
	1. As propostas apresentadas no certame licitatório deverão ser válidas por, no mínimo, 90 (noventa) dias, contados a partir da data de abertura do certame, na forma do art. 90, §3º da Lei n.º 14.133/2021, a saber:

Art. 90. A Administração convocará regularmente o licitante vencedor para assinar o termo de contrato ou para aceitar ou retirar o instrumento equivalente, dentro do prazo e nas condições estabelecidas no edital de licitação, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas nesta Lei.

(...)

§ 3º Decorrido o prazo de validade da proposta indicado no edital sem convocação para a contratação, ficarão os licitantes liberados dos compromissos assumidos.

1. **DA ESTIMATIVA DE VALOR DA CONTRATAÇÃO**
	1. O valor deverá ser estimado **após pesquisa de mercado a ser realizada pela Superintendência de Compras**, nos termos do Decreto Municipal n° 936/2022;
2. **DA ADEQUAÇÃO ORÇAMENTÁRIA**
	1. Os recursos orçamentários decorrentes da presente contratação correrão à conta dos recursos informados pela Diretoria Financeira, conforme art. 12°, inciso IV do Decreto n.º 936/2022;
3. **DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS**
	1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:
		1. der causa à inexecução parcial do contrato;
		2. der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
		3. der causa à inexecução total do contrato;
		4. deixar de entregar a documentação exigida para o certame;
		5. não mantiver a proposta, salvo em decorrência de fato superveniente devidamente justificado;
		6. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta, na forma do item 13;
		7. ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
		8. apresentar declaração ou documentação inidônea exigida para o certame ou prestar declaração falsa durante a execução do contrato;
		9. fraudar a contratação ou praticar ato fraudulento na execução do contrato;
		10. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
		11. praticar atos ilícitos com vistas a frustrar os objetivos do certame;
		12. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.
	2. Serão aplicadas ao responsável pelas infrações administrativas acima descritas as seguintes sanções:
		1. **Advertência**, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei n.º 14.133/2021);
		2. **Impedimento de licitar e contratar**, quando praticadas as condutas descritas nas alíneas b, c, d, e, f e g do subitem acima, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §4º, da Lei 14.133/2021);
		3. **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nas alíneas h, i, j, k e l do subitem acima, bem como nas alíneas b, c, d, e, f e g, que justifiquem a imposição de penalidade mais grave;
		4. **Multa:**
	3. moratória de 1% (um por cento) por dia útil de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 20% (vinte por cento) do valor global do contrato;
	4. administrativa de 20% (vinte por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;
	5. A aplicação das sanções previstas no Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante.
	6. Todas as sanções previstas neste Termo de Referência poderão ser aplicadas cumulativamente com a multa.
		1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.
		2. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.
		3. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 10 (dez)dias, a contar da data do recebimento da comunicação enviada pela autoridade competente;
	7. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no *caput* e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.
	8. Na aplicação das sanções serão considerados:

a) a natureza e a gravidade da infração cometida;

b) as peculiaridades do caso concreto;

c) as circunstâncias agravantes ou atenuantes;

d) os danos que dela provierem para o Contratante;

* 1. O Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal.
	2. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.
	3. As multas serão aplicadas, conforme as infrações cometidas e o nível de gravidade respectivo, indicados nas tabelas a seguir:

**TABELA 1**

**CLASSIFICAÇÃO DAS INFRAÇÕES E MULTAS**

|  |  |
| --- | --- |
| **NÍVEL** | **CORRESPONDÊNCIA****(por ocorrência sobre o valor global do Contratada)** |
| 1 (menor ofensividade) | 0,2%. |
| 2 (leve) | 0,4%. |
| 3 (médio) | 0,8%. |
| 4 (grave) | 1,6%. |
| 5 (muito grave) | 3,2%. |
| 6 (gravíssimo) | 4%. |

* 1. As gradações dispostas na tabela acima, somadas, limitar-se-ão ao percentual de 20% (vinte por cento) sobre o valor global do contrato, na forma estabelecida no subitem 16.2.4.
	2. Todas as ocorrências contratuais serão registradas pela FEMAR, que notificará empresa a ser contratada.

**TABELA 2**

**INFRAÇÕES E CORRESPONDENTES NÍVEIS**

|  |
| --- |
| **INFRAÇÃO** |
| **Item** | **Descrição** | **Nível** |
| 1 | Transferir a outrem, no todo ou em parte, o objeto do Contrato sem prévia e expresso acordo do CONTRATANTE. | 6 |
| 2 | Caucionar ou utilizar o Contrato para quaisquer operações financeiras. | 6 |
| 3 | Reproduzir, divulgar ou utilizar, em benefício próprio ou de terceiros, quaisquer informações de que tenha tomado ciência em razão do cumprimento de suas obrigações sem o consentimento prévio e por escrito do CONTRATANTE. | 5 |
| 4 | Utilizar o nome do CONTRATANTE, ou sua qualidade de CONTRATADA, em quaisquer atividades de divulgação empresarial, como, por exemplo, em cartões de visita, anúncios e impressos. | 5 |
| 5 | Deixar de relacionar-se com O CONTRATANTE, exclusivamente, por meio do fiscal do Contrato. | 3 |
| 6 | Deixar de se sujeitar à fiscalização do CONTRATANTE, que inclui o atendimento às orientações do fiscal do Contrato e a prestação dos esclarecimentos formulados. | 4 |
| 7 | Deixar de responsabilizar-se pelos produtos e materiais entregues, assim como deixar de substituir imediatamente qualquer material ou objeto que não atenda aos critérios especificados neste termo. | 6 |
| 8 | Não zelar pelas instalações do CONTRATANTE | 3 |
| 9 | Deixar de responsabilizar-se por quaisquer acidentes de trabalho sofridos pelos seus empregados quando em serviço. | 6 |
| 10 | Deixar de responsabilizarem-se pelos encargos trabalhista, fiscal e comercial, pelos seguros de acidente e quaisquer outros encargos resultantes da prestação do objeto. | 6 |
| 11 | Deixar de observar rigorosamente as normas regulamentadoras de segurança do trabalho. | 6 |
| 12 | Deixar de manter nas dependências do CONTRATANTE, os funcionários identificados e uniformizados de maneira condizente com o serviço, observando ainda as normas internas e de segurança. | 2 |
| 13 | Deixar de manter, durante todo o período de vigência contratual, todas as condições de habilitação e qualificação que permitiram sua contratação. | 6 |
| 14 | Deixar de disponibilizar e manter atualizados conta de e-mail, endereço e telefones comerciais para fins de comunicação formal entre as partes. | 2 |
| 15 | Deixar de responsabilizar-se pela idoneidade e pelo comportamento de seus prestadores de serviço e por quaisquer prejuízos que sejam causados à CONTRATANTE e a terceiros. | 6 |
| 16 | Deixar de encaminhar documentos fiscais e todas as documentações determinadas pelo fiscal do Contrato para efeitos de atestar a entrega dos bens e comprovar regularizações. | 4 |
| 17 | Deixar de resguardar que seus funcionários cumpram as normas internas do CONTRATANTE e impedir que os que cometerem faltas a partir da classificação de natureza grave continue na prestação dos serviços. | 3 |
| 18 | Deixar de assumir todas as responsabilidades e tomar as medidas necessárias para o atendimento dos prestadores de serviço acidentados ou com mal súbito. | 6 |
| 19 | Deixar de relatar à CONTRATANTE toda e quaisquer irregularidades ocorridas, que impeça, altere ou retarde a execução do Contrato, efetuando o registro da ocorrência com todos os dados e circunstâncias necessárias a seu esclarecimento. | 5 |
| 20 | Suspender ou interromper, salvo motivo de força maior ou caso fortuito, a execução do objeto. | 5 |
| 21 | Recusar fornecimento determinado pela fiscalização sem motivo justificado. | 3 |
| 22 | Retirar das dependências da FEMAR quaisquer equipamentos ou materiais de consumo sem autorização prévia. | 3 |
| 23 | Destruir ou danificar documentos por culpa ou dolo de seus agentes. | 6 |

1. **DAS HIPÓTESES DE EXTINÇÃO CONTRATUAL**
	1. A inexecução do objeto deste Termo de Referência, total ou parcialmente, poderá ensejar a rescisão contratual, na forma dos artigos 137, 138, 139 e 155 da Lei nº 14.133/2021, com as consequências previstas em lei e neste instrumento;
	2. A rescisão unilateral do Contrato a ser firmado poderá ser determinada pela FEMAR, de acordo com o inciso I do Art. 138 da Lei nº 14.133/2021, com as consequências elencadas no Art. 139 do referido diploma legal.
	3. Constituem motivo para rescisão do Contrato, todos os incisos constantes do Artigo 137 da Lei nº 14.133/2021;
	4. As formas de rescisão estão previstas no Art. 138, Incisos de I a III, da Lei nº 14.133/2021;
	5. Os casos omissos de rescisão contratual serão formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa;
	6. Os casos de rescisão contratual serão formalmente motivados nos autos, assegurados o contraditório e a ampla defesa;
	7. A rescisão administrativa ou amigável será precedida de autorização escrita e fundamentada da autoridade competente.
2. **DO FORO**
	1. Ficará eleito o Foro da Comarca de Maricá para dirimir quaisquer questões decorrentes deste Termo de Referência, assim como do Edital de Convocação e do contrato que o sucederão, renunciando as partes, a qualquer outro, por mais privilegiado que seja.

Maricá, 01 de abril de 2024.

**Elaborado por,**

**Caroline Santos Felismino de Santiago**

Assessora - Mat.: 3.300.037

Gerência de Instrução Processual

Diretoria Administrativa

**Responsáveis técnicos,**

|  |  |
| --- | --- |
| **Walter Matoso Rosa Junior**Assistente - Mat.: 3.300.352Superintendência de Infraestrutura Diretoria Administrativa | **Alessandra Lopes Rangel** Mat.: 3.300.020Superintendente de Infraestrutura Diretoria Administrativa |

**Conferido e de acordo,**

**Daniel Ferreira da Silva**

Mat.:3.300.002

Diretor Administrativo

**ANEXO A - MEMÓRIA DE CÁLCULO**

|  |
| --- |
| **OS PRODUTOS DESCRITOS NESTA PLANILHA INCLUEM FORNECIMENTO, INSTALAÇÃO, CONFIGURAÇÃO LÓGICA E TREINAMENTO** |
| **ITEM** | **DESCRIÇÃO** |
| 1 | **CÂMERA DE VÍDEO IP TIPO I COM LICENÇA DE SOFTWARE PARA PLATAFORMA DE GERENCIAMENTO EM NUVEM POR PERÍODO DE 60 MESES, INCLUINDO INSTALAÇÃO.*** Câmera fixa interna do tipo dome;
* Utilizar um sensor CMOS para captação de imagens, com tamanho de 1/3” e pelo menos 4 MP (2688x1520);
* Possuir um iluminador infravermelho integrado até 30 metros de distância;
* Possuir IR adaptativo onde irá ligar automaticamente quando a luminosidade diminuir;
* Possuir lente com distância focal de 3-9 mm;
* Possuir ao menos os ângulos de visão de H: 36-112° / V: 20-57°, com variações superiores e inferiores de até 10%;
* Captar imagens em situações de baixa luminosidade, nas seguintes condições de iluminação incidente: deverá suportar no mínimo 0.18 lux; E a 0,01 lux modo noturno;
* Possuir resolução mínima de 1080p a 20 FPS;
* Possuir velocidade de obturador de 1/30s a 1/32.000s;
* Suportar compressão de vídeo H.264;
* Possuir interface de rede Ethernet com velocidades de 10/100/1000 Mbps (1000Base-T);
* Compatível com os protocolos IPv4; IPv6; HTTP; TCP; UDP; ARP; RTP; RTSP; RTCP; RTMP; SMTP; FTP; SFTP; DHCP; DNS; DDNS; QoS; UPnP; NTP; Multicast; ICMP; IGMP; NFS; PPPoE; Bonjour;
* Possuir padrão Wi-Fi 802.11b/g/n; frequência de 2,4 GHz, Canais de 20 e 40 MHz (802.11n) e Wi-Fi 802.11a/n/ac de 5 GHz, canais 20, 40 e 80 MHz (802.11ac);
* Possuir Antenas omnidirecionais integradas (ganho de 4,4 dBi a 2,4 GHz, ganho de 6,3 dBi a 5 GHz);
* Possuir opções para alimentação PoE (Alimentação sobre Ethernet – IEEE 802.3af), sendo que o consumo máximo de energia não deve ser superior a 13 W;
* Possuir involucro que forneça proteção do equipamento.
* Suportar no mínimo 15 conexões simultâneas.
* Possuir criptografia de disco completo (AES 256 bits)
* Possuir certificados TLS adquiridos e provisionados automaticamente (assinados publicamente)
* Possuir criptografia de gerenciamento e autenticação de dois fatores
* Possuir armazenamento interno de no mínimo de 512 GB
* Armazenar até 30 dias de vídeo contínuo 24 horas por dia, 7 dias por semana por câmera
* Possuir alta faixa dinâmica (HDR) áudio
* Possuir gravação de áudio suportada com microfone embutido
* Possuir rádio Bluetooth Low Energy (BLE) de 2,4 GHz
* A câmera deve estar acompanhada de todos os acessórios necessários para instalação, configuração e operacionalização, tais como: softwares, cabos, kits para fixação, documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;
* Fornecer, para cada câmera, suporte do fabricante, incluída na licença do equipamento, com tempo de duração equivalente ao tempo de subscrição da licença adquirida
* Estar licenciado para permitir o controle e gerenciamento centralizado através da solução em nuvem por um período de no mínimo 60 (sessenta) meses;
* **CARACTERÍSTICAS GERAIS DE GERENCIAMENTO**
* A solução proposta deve atender às seguintes especificações:
* Gestão centralizada a partir de uma console de administração baseada na Web e a partir da qual deve ser possível o acesso, configuração e monitoramento de toda as câmeras da solução.
* Por meio da console de gerenciamento deve ser possível a configuração de todas as funcionalidades descritas anteriormente;
* A plataforma de gerencia deve ser possível identificar cada uma das localidades remotas com uma identificação administrativa para posteriormente ser usada como filtro de pesquisa.
* O acesso a console de gerenciamento deve ser realizado com o uso de um método de autenticação de dois fatores
* O acesso a console deve ser por HTTPS (portas 8080 e 443) e seus certificados de segurança devem ser emitidos por entidades reconhecidas na Internet.
* A console de gerenciamento deve suportar a definição de contas de administrador com base em funções, relatar as alterações às mesmas em um log de eventos e alertas que podem ser consultados por meio da mesma console.
* O nível hierárquico de administrador da console deve conter:
* O administrador com acesso total pode efetuar as seguintes operações dentro da organização a qual ele pertence:
* Criar, editar e excluir contas de acesso total e somente leitura para a organização
* Redefinição de senhas.
* Criar, editar e excluir equipamentos.
* Adicionar novos dispositivos à rede da organização.
* Apresentar inventário de equipamentos da solução que estão, ou não, em utilização.
* Possível bloquear o acesso a plataforma após falhas de login

Possível configurar logout da plataforma após minutos sem atividade |
| 2 | **CÂMERA DE VÍDEO IP TIPO II COM LICENÇA DE SOFTWARE PARA PLATAFORMA DE GERENCIAMENTO EM NUVEM POR PERÍODO DE 60 MESES, INCLUINDO INSTALAÇÃO.*** Câmera fixa interna do tipo dome;
* Utilizar um sensor CMOS para captação de imagens, com tamanho de 1/3” e pelo menos 4 MP (2688x1520);
* Possuir um iluminador infravermelho integrado até 30 metros de distância;
* Possuir IR adaptativo onde irá ligar automaticamente quando a luminosidade diminuir;
* Possuir lente com distância focal de 3-9 mm;
* Possuir ao menos os ângulos de visão de H: 36-112° / V: 20-57°, com variações superiores e inferiores de até 10%;
* Capaz de captar imagens em situações de baixa luminosidade, nas seguintes condições de iluminação incidente: deverá suportar no mínimo 0.18 lux; E a 0,01 lux modo noturno;
* Possuir resolução mínima de 1080p a 20 FPS;
* Possuir velocidade de obturador de 1/30s a 1/32.000s;
* Suportar compressão de vídeo H.264;
* Possuir interface de rede Ethernet com velocidades de 10/100/1000 Mbps (1000Base-T);
* Ser compatível com os protocolos IPv4; IPv6; HTTP; TCP; UDP; ARP; RTP; RTSP; RTCP; RTMP; SMTP; FTP; SFTP; DHCP; DNS; DDNS; QoS; UPnP; NTP; Multicast; ICMP; IGMP; NFS; PPPoE; Bonjour;
* Possuir padrão Wi-Fi 802.11b/g/n; frequência de 2,4 GHz, Canais de 20 e 40 MHz (802.11n) e Wi-Fi 802.11a/n/ac de 5 GHz, canais 20, 40 e 80 MHz (802.11ac);
* Deve possuir Antenas omnidirecionais integradas (ganho de 4,4 dBi a 2,4 GHz, ganho de 6,3 dBi a 5 GHz);
* Possuir opções para alimentação PoE (Alimentação sobre Ethernet – IEEE 802.3af), sendo que o consumo máximo de energia não deve ser superior a 13 W;
* Possuir involucro que forneça proteção do equipamento.
* Suportar no mínimo 15 conexões simultâneas.
* Possuir criptografia de disco completo (AES 256 bits)
* Possuir certificados TLS adquiridos e provisionados automaticamente (assinados publicamente)
* Possuir criptografia de gerenciamento e autenticação de dois fatores
* Possuir armazenamento interno de no mínimo de 256 GB
* Armazenar até 30 dias de vídeo contínuo 24 horas por dia, 7 dias por semana por câmera
* Possuir alta faixa dinâmica (HDR) áudio
* Possuir gravação de áudio suportada com microfone embutido
* Possuir rádio Bluetooth Low Energy (BLE) de 2,4 GHz
* A câmera deve estar acompanhada de todos os acessórios necessários para instalação, configuração e operacionalização, tais como: softwares, cabos, kits para fixação, documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;
* Ser fornecido, para cada câmera, suporte do fabricante, incluída na licença do equipamento, com tempo de duração equivalente ao tempo de subscrição da licença adquirida
* Estar licenciado para permitir o controle e gerenciamento centralizado através da solução em nuvem por um período de no mínimo 60 (sessenta) meses;
* **CARACTERÍSTICAS GERAIS DE GERENCIAMENTO**

A solução proposta deve atender às seguintes especificações:* Gestão centralizada a partir de uma console de administração baseada na Web e a partir da qual deve ser possível o acesso, configuração e monitoramento de toda as câmeras da solução.
* Por meio da console de gerenciamento deve ser possível a configuração de todas as funcionalidades descritas anteriormente;
* A plataforma de gerencia deve ser possível identificar cada uma das localidades remotas com uma identificação administrativa para posteriormente ser usada como filtro de pesquisa.
* O acesso a console de gerenciamento deve ser realizado com o uso de um método de autenticação de dois fatores;
* O acesso a console deve ser por HTTPS (portas 8080 e 443) e seus certificados de segurança devem ser emitidos por entidades reconhecidas na Internet;
* A console de gerenciamento deve suportar a definição de contas de administrador com base em funções, relatar as alterações às mesmas em um log de eventos e alertas que podem ser consultados por meio da mesma console;

O nível hierárquico de administrador da console deve conter:* O administrador com acesso total pode efetuar as seguintes operações dentro da organização a qual ele pertence;
* Criar, editar e excluir contas de acesso total e somente leitura para a organização;
* Redefinição de senhas;
* Criar, editar e excluir equipamentos;
* Adicionar novos dispositivos à rede da organização;
* Apresentar inventário de equipamentos da solução que estão, ou não, em utilização;
* Bloquear o acesso a plataforma após falhas de login;
* Configurar logout da plataforma após minutos sem atividade.
 |
| 3 | **CÂMERA DE VÍDEO IP TIPO III MAIS LICENÇA DE SOFTWARE PARA PLATAFORMA DE GERENCIAMENTO EM NUVEM POR PERÍODO DE 60 MESES, INCLUINDO INSTALAÇÃO.*** **CARACTERÍSTICAS GERAIS**
	+ Câmera inteligente fixa interna/externa;
	+ Deve utilizar um sensor CMOS para captação de imagens, com tamanho de 1/1.8” e pelo menos 8.4MP (8,4 Megapixels) efetivos;
	+ Deve possuir armazenamento interno de no mínimo de 1TB
	+ O disco deve ter criptografia AES 256-Bit
	+ Certificados TLS adquiridos e provisionados automaticamente
	+ Deve possuir um iluminador infravermelho do tipo LED de no mínimo 50 metros de distância;
	+ Deverá possuir IR adaptativo onde irá ligar automaticamente quando a luminosidade diminuir;
	+ Deverá possuir lente com distância focal de 12-40 mm;
	+ Deverá possuir ao menos os ângulos de visão de H: 12°-37° / V: 7°-22;
	+ Deve possuir resolução mínima de 3840 x 2160 a 15 FPS;
	+ Possuir velocidade de obturador de 1/30 a 1/1000s de forma manual ou automática;
	+ Deve suportar compressão de vídeo H.264;
	+ Deve possuir interface de rede Ethernet com velocidades de (10/100/1000 Mbps Base-T);
	+ Deve possuir padrão Wi-Fi 802.11b/g/n; frequência de 2,4 GHz, Canais de 20 e 40 MHz (802.11n) e Wi-Fi 802.11a/n/ac de 5 GHz, canais 20, 40 e 80 MHz (802.11ac);
	+ Deve possuir Antenas omnidirecionais integradas (ganho de 4,4 dBi a 2,4 GHz, ganho de 6,3 dBi a 5 GHz);
	+ Deve ser compatível com os protocolos IPv4; IPv6; HTTP; TCP; UDP; ARP; RTP; RTSP; RTCP; RTMP; SMTP; FTP; SFTP; DHCP; DNS; DDNS; QoS; UPnP; NTP; Multicast; ICMP; IGMP; NFS; PPPoE; Bonjour;
	+ Deve possuir opções para alimentação 12VDC e PoE (Alimentação sobre Ethernet – IEEE 802.3af), sendo que o consumo máximo de energia não deve ser superior a 25.5 W;
	+ Deve possuir involucro que forneça proteção do equipamento com grau de proteção IP67.
	+ Deve possuir o recurso de inteligência artificial com a capacidade de identificar cruzamento de linhas e cercamento virtual;
	+ A câmera deve estar acompanhada de todos os acessórios necessários para instalação, configuração e operacionalização, tais como: softwares, cabos, kits para fixação, documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;
	+ Deverá ser fornecida, para cada câmera, suporte do fabricante, incluída na licença do equipamento, com tempo de duração equivalente ao tempo de subscrição da licença adquirida
	+ Estar licenciado para permitir o controle e gerenciamento centralizado através da solução em nuvem por um período de no mínimo 60 (sessenta) meses;
	+ Deve armazenar no mínimo 60 (sessenta) dias de vídeo contínuo 24 horas por dia, 7 dias por semana por câmera.
* **CARACTERÍSTICAS GERAIS DE GERENCIAMENTO**
	+ A solução proposta deve atender às seguintes especificações:
	+ Gestão centralizada a partir de uma console de administração baseada na Web e a partir da qual deve ser possível o acesso, configuração e monitoramento de toda as câmeras da solução.
	+ Por meio da console de gerenciamento deve ser possível a configuração de todas as funcionalidades descritas anteriormente;
	+ A plataforma de gerencia deve ser possível identificar cada uma das localidades remotas com uma identificação administrativa para posteriormente ser usada como filtro de pesquisa.
	+ O acesso a console de gerenciamento deve ser realizado com o uso de um método de autenticação de dois fatores
	+ O acesso a console deve ser por HTTPS (portas 8080 e 443) e seus certificados de segurança devem ser emitidos por entidades reconhecidas na Internet.
	+ A console de gerenciamento deve suportar a definição de contas de administrador com base em funções, relatar as alterações às mesmas em um log de eventos e alertas que podem ser consultados por meio da mesma console.
	+ O nível hierárquico de administrador da console deve conter:
	+ O administrador com acesso total pode efetuar as seguintes operações dentro da organização a qual ele pertence:
	+ Criar, editar e excluir contas de acesso total e somente leitura para a organização
	+ Redefinição de senhas.
	+ Criar, editar e excluir equipamentos.
	+ Adicionar novos dispositivos à rede da organização.
	+ Deve apresentar inventário de equipamentos da solução que estão, ou não, em utilização.
	+ Deve ser possível bloquear o acesso a plataforma após falhas de login
* Deve ser possível configurar logout da plataforma após minutos sem atividade.
 |
| 4 | **COMUTADOR COM GARANTIA DE 60 MESES*** CARACTERÍSTICAS GERAIS
	+ Estrutura para instalação em rack padrão EIA 19", incluindo todos os acessórios necessários;
	+ Possuir no máximo 1 Rack Unit (RU).
	+ LEDs de identificação de atividades de status do sistema, de cada porta e da alimentação elétrica;
	+ Fonte de alimentação de 100-240 VAC, 50/60 Hz com opção de redundância, com chaveamento automático, operação em modo load-sharing, do po hot-swappable. Em caso de falha de uma das fontes, a outra deverá suportar toda a carga do switch. É necessário fornecer a fonte redundante. As fontes deverão possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos.
	+ Em caso de falha de uma das fontes, a outra deverá suportar toda a carga do switch.
	+ Suporte a configuração unificada de mais de um equipamento que possibilita a configuração e avançada de interconexões entre portas de comutadores distintos sem necessidade de acessar a configurar cada switch em separado, sem necessidade de uso de software de gerência adicional.
* CONECTIVIDADE
* Suporte às seguintes tecnologias:
	+ IEEE 802.3z- (1000BASE-SX, 1000BASE-LX)
	+ IEEE 802.3ba-(40GBASE-LR4, 40GBASE-ER4)
	+ IEEE 802.3bm-(40GBASE-SR4)
	+ IEEE 802.3ab 1000BASE-T
	+ IEEE 802.3z 1000BASE-X
	+ IEEE 802.3bz Multirate 5G
* Pelo menos 48 portas 1/10/25G com autosensing de velocidade. Todas as 48 portas devem operar simultaneamente em conjunto com as portas de uplink
* Pelo menos 6 portas para módulos transceivers com suporte a velocidades de 40/100Gbps com soquetes QSFP.
* Porta ethernet para rede de gerência independente, out-of-band, com permissão de acesso a todos os recursos do equipamento utilizando endereço IP de gerência.
* Porta de console RS232
* Porta USB
* FUNCIONALIDADES
* Permite a implementação do protocolo IPv6;
* Capacidade de armazenamento no mínimo 510000 endereços MAC na tabela;
* Suporte a VLANs, com pelo menos 4095 VLAN IDs e VLAN de gerenciamento:
* Baseadas em porta; e. Baseadas em protocolo;
* Baseadas em endereço MAC;
* Possuir capacidade de no mínimo 3500 Gbps e taxa de encaminhamento de pacotes de no mínimo 1.1 Bpps.
* Suporte a listas de controle de acesso (ACLs) para bloqueio de pacotes por endereços IP de origem e destino, por porta IP de origem e destino e por endereço MAC, com pelo menos 2000 regras distintas, para tráfego entrando ou saindo nas portas.
* Implementar “accounting” das conexões IEEE 802.1x. O switch (cliente AAA) deve ser capaz de enviar, ao servidor AAA, pelo menos as seguintes informações sobre a conexão
* Nome do usuário;
* Switch em que o computador do usuário está conectado;
* Porta do switch utilizada par acesso;
* Endereço MAC da máquina utilizada pelo usuário;
* Endereço IP do usuário; Horários de início e término da conexão;
* Bytes transmitidos e recebidos durante a conexão.
* Suporte aos seguintes padrões, protocolos e funcionalidades:IEEE 802.1d Spanning Tree
	+ IEEE 802.1Q VLAN tagging
	+ IEEE 802.1w Rapid Spanning Tree
	+ IEEE 802.1ab LLDP
	+ IEEE 802.3ad LACP
	+ RFC 3768 VRRP
* Secure Shell (SSH-2) client and server
* Secure Copy (SCP-2) client and server
* Relay DHCP e DHCPv6
* IGMPv2 snooping
* PIM-SM
* DHCP snooping ou funcionalidade similar que permita o bloqueio de servidores DHCP não autorizados na rede
* Espelhamento (Port Mirroring) do tráfego de entrada e saída de múltiplas portas do switch em uma única porta, inclusive sobre portas de diferentes módulos do chassi e sobre links agregados com IEEE 802.3ad
* Espelhamento (VLAN Mirroring) de VLAN. Será aceita implementação de espelhamento com possibilidade de seleção do tráfego por lista de controle de acesso (ACL), ou funcionalidade similar, segundo o identificador de VLAN
* Supressão de broadcast
* Encaminhamento de Jumbo frames
* Cliente e servidor NTP
* OSPF e OSPFv3
* BGPv4
* VRF
* SEGURANÇA
* Disponibilizar, no mínimo, dois níveis de senha de acesso, sendo uma com restrição total à configuração do equipamento e a comandos que alterem seu funcionamento, e outra, sem qualquer restrição;
* Suporte a autenticação TACACS+ ou RADIUS, para acesso ao equipamento;
* Limitação de endereços MAC por porta, aprendidos automaticamente ou configurados manualmente, implementado ou em roadmap;
* Suporte a bloqueio de MAC por porta, implementado ou em roadmap.
* Suportar filtragem de pacotes (ACL - Access Control List) para IPv4 e IPv6.
* Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e flags TCP.
* GERENCIAMENTO E CONFIGURAÇÃO
* Gerenciamento do chassi através de um único endereço IP;
* Possuir porta de console, RJ-45, acompanhado do cabo específico;
* Implementar os seguintes protocolos e funcionalidades de gerenciamento:
* CLI - interface de linha de comando capaz de expor todas as funcionalidades de configuração e monitoração do equipamento
* SNMP
* Telnet
* SSHv2
* SNMPv2c e SNMPv3, com autenticação e/ou criptografia
* Syslog para servidores remotos

🡪 SUPORTE* Múltiplas configurações;
* Múltiplas imagens do sistema;
* Cópia de segurança das configurações em modo texto;
* Linguagem de programação para criação de scripts a serem executados no equipamento;
* Possibilidade de especificar uma descrição para cada interface, acessível via SNMP.
* Suporte às seguintes MIBs:
	+ IEEE 802.3 Ethernet (RFC 1643)
	+ MIB-II (RFC 1212, RFC 1213, RFC 1215)
	+ Evolution of Interface (RFC 1573)
	+ Ethernet-Like MIB (RFC 1650)
	+ Ping/Traceroute (RFC 2925)
	+ Bridge (RFC 1493)
	+ Interface MIB (RFC 2233)
	+ IEEE 802.1ag
	+ RMON (RFC 1757)
 |
| 5 | Instalação do item 4 |
| 6 | **FIREWALL/ROTEADOR TIPO I COM LICENÇA DE SOFTWARE PARA PLATAFORMA DE GERENCIAMENTO EM NUVEM POR PERÍODO DE 60 MESES.*** Novos e homologados pela ANATEL;
* Todos os hardwares e softwares devem ser do mesmo fabricante;
* Todas as características avançadas de segurança (URL Filtering, IPS e Antimalware) devem ser do mesmo fabricante e nativamente integradas aos equipamentos ofertados.
* O equipamento de segurança com capacidade de SD-WAN deve ser um sistema integrado UTM (Unified Threat Management) que inclua pelo menos as seguintes características:
* Firewall de estados (Stateful Firewall).
* Filtro de conteúdo com no mínimo oitenta (80) categorias pré-definidas.
* Antimalware.
* Concentrador VPN para gateways e clientes.
* IDS e IPS.
* Roteamento baseado em políticas.
* Balanceamento de, no mínimo, 02 (dois) links WAN e mecanismo para seleção de melhor caminho a ser definido por aplicação camada 7, automaticamente baseado em, no mínimo, jitter, perda de pacotes e delay.
* Características físicas do equipamento:
* Suportar no mínimo 500Mbps de tráfego de IPSEC VPN com criptografia AES de até 256 bits;
* Suportar no mínimo 1Gbps de tráfego de “stateful firewall”, com as todas as funcionalidades de segurança habilitadas;
* Possuir interface USB para conexão de modem 3G/4G/5G.
* Possibilidade de ser configurado em alta disponibilidade;
* Mínimo de 02 (duas) interfaces 1Gigabit Ethernet SFP ou RJ45 para segmento WAN/Internet, sendo necessário que no mínimo, as duas interfaces WAN estejam simultaneamente ativas
* Mínimo de 08 (oito) interfaces Gigabit-Ethernet para segmento LAN com conectores padrão UTP RJ45;
* Mínimo de 02 (duas) interfaces Gigabit-Ethernet para segmento LAN com conectores padrão SFP;
* Implementar recurso de web-caching sem a necessidade de utilizar equipamento externo para tal;
* Acompanhado com fonte de alimentação AC 110/220v padrão ABNT;
* Serviços de segurança:
* Implementar funcionalidade de Firewall Stateful camada 7;
* A solução deverá suportar a definição de regras de firewall de camada 3, 4 e Camada 7;

Regras de políticas de acesso de camada 3 definidas por:* Protocolo (UDP ou TCP);
* Host, sub-rede ou rede de origem;
* Porta TCP ou UDP de origem;
* Host, sub-rede ou rede de destino;
* Porta TCP ou UDP de destino.
* Através das regras da camada 7, deve suportar a restrição de tráfego a partir de categorias definidas, incluindo:
* Blog;
* E-mail;
* Compartilhamento de arquivos;
* Jogos;
* Noticias;
* Backup on-line;
* Ponto a ponto;
* Redes sociais e compartilhamento de fotos;
* Atualizações de softwares e antivírus;
* Esportes;
* Videoconferência e VoIP;
* Compartilhamento de arquivos via Web;
* Hostname http;
* Por Países, GeoIP-Firewall.
* Suporte a NAT 1:1 e o redirecionamento de portas (Port Forwarding) para a publicação de sistemas específicos para a Internet.
* Implementar funcionalidade de criação automatizada de túneis IPSEC VPN entre equipamentos dentro da mesma organização;
* Implementar a criação de VPNs para acesso remoto de usuários usando IPSec L2TP
* As VPNs site-to-site deve poder ser configuradas em modo hub-spoke ou full-mesh
* Suportar NAT-transversal
* Permitir a criação de tuneis IPSEC VPN site-to-site com equipamentos de terceiros.
* Permitir a conexão com client VPN
* Permitir a integração nativa com Active Directory
* SDWAN
* Implementar solução de SDWAN capaz de balancear trafego entre os links WAN;
* Quando a função de balanceamento de carga estiver desativada, todo o tráfego da WAN deve usar o link principal, com redundância para link secundário e como uma terceira opção a conexão 3G/4G em caso de falha dos links primário e secundário
* Configurar a largura de banda dos links principais e backup (celular) de maneira independente
* Definir qual o link principal do equipamento
* Habilitar ou desabilitar o balanceamento de trafego entre os links
* Configurar qual dos links WAN será utilizado para acessar a internet por determinada rede (IP e/ou porta TCP-UDP) para trafego encapsulado e deve ser possível escolher qual link será utilizado para acessar a localidade central baseado em camada 3, 4 e 7, a escolha de qual link será utilizado deve ser automatizada e inteligente baseado em, no mínimo, condições do link como jitter, delay e perda de pacotes.
* O chaveamento entre os links deve ser automático uma vez atingido níveis não aceitáveis das características citadas acima.
* Decidir os níveis de qualidade do link e seu chaveamento por aplicação.
* A política de modelagem de tráfego deve permitir a atribuição de limites de largura de banda simétricos ou assimétricos por aplicativo, por usuários e por grupo de usuários.
* Suportar BGP, OSPF e roteamento estático para divulgar as rotas as localidades remotas.
* Através da política de modelagem de tráfego deve ser capaz de serem priorizados determinados tipos de tráfego e/ou associados com um rótulo de QoS usando DSCP com pelo menos 4 classes de serviço (Melhor esforço, background, vídeo e voz).
* Filtro de conteúdo
* A solução deverá implementar recursos de filtro de conteúdo
* A solução de filtro de conteúdo deverá ter categorias pré-definidas para bloqueio.
* Permitir a habilitação da funcionalidade "safesearch" ou equivalente assegurando o conteúdo das páginas de busca como google, bing, etc.
* Permitida criação de blacklist baseada em URL, para sites que nunca devem ser acessados.
* Permitida também a criação de whitelist, onde estas URL não serão avaliadas pelo filtro de conteúdo.
* Detecção e prevenção de intrusões IPS/IDS.
* A solução deve colocar à disposição da instituição a habilidade de ativar o módulo IDS e IPS.
* Ativação ou desativação do módulo IDS/IPS para grupos de usuários.
* Inclusão em whitelist de uma ou várias assinaturas de IDS/IPS para remover da ação de bloqueio.
* Deve ser possível habilitar o nível de proteção baseado em score CVSS
* As assinaturas devem ser atualizadas diariamente, automaticamente, diretamente com o serviço de segurança da fabricante;
* Detectar e bloquear exploits, vírus, rootkits entre outras ameaças;
* Antimalware
* A solução deve possuir antimalware protection
* A funcionalidade de antimalware deve, no mínimo, avaliar os seguintes tipos de arquivos:
	+ MS OLE2 (.doc, .xls, .ppt);
	+ MS Cabinet (Microsoft compression type);
	+ MS EXE;
	+ ELF (Linux executable);
	+ Mach-O/Unibin (OSX executable);
	+ Java (class/bytecode, jar, serialization);
	+ PDF;
	+ ZIP (regular and spanned)\*;
	+ EICAR (standardized test file);
	+ SWF (shockwave flash 6, 13, and uncompressed);
* Caso algum malware seja encontrado deve ser possível enviar um alerta ao administrador da rede.
* Características gerais de gerenciamento da solução:
* A solução proposta deve atender às seguintes especificações:
* Gestão centralizada a partir de uma console de administração baseada na Web e a partir da qual deve ser possível o acesso, configuração e monitoramento de todos os equipamentos de segurança contemplados na solução;
* Por meio da console de gerenciamento deve ser possível a configuração de todas as funcionalidades descritas anteriormente;
* Deve haver mecanismos para agrupar logicamente a administração de um certo número de dispositivo UTM para envio de modificações em suas configurações simultaneamente;
* A plataforma de gerencia deve ser possível identificar cada uma das localidades remotas com uma identificação administrativa para posteriormente ser usada como filtro de pesquisa;
* O acesso a console de gerenciamento deve ser realizado com o uso de um método de autenticação de dois fatores;
* O acesso a console deve ser por HTTPS (portas 8080 e 443) e seus certificados de segurança devem ser emitidos por entidades reconhecidas na Internet;
* A console de gerenciamento deve suportar a definição de contas de administrador com base em funções, relatar as alterações às mesmas em um log de eventos e alertas que podem ser consultados por meio da mesma console;
* O nível hierárquico de administradores da console deve conter:
* Administrador de Organização: Um administrador da organização deverá ter visibilidade em todas as redes dentro da organização. Deverão existir dois tipos de administradores da organização: (1) acesso total e (2) somente leitura.
* O administrador com acesso total pode efetuar as seguintes operações dentro da organização a qual ele pertence:
* Criar, editar e excluir contas de acesso total e somente leitura para a organização;
	+ Redefinição de senhas;
	+ Criar, editar e excluir redes;
	+ Adicionar novos dispositivos à rede da organização.
* Administrador de Rede: Terão visibilidade nas redes da organização para as quais tenham sido designados como um administrador. Deverão existir dois tipos de administradores de rede: (1) acesso total e (2) somente leitura. Um administrador de rede com acesso total será capaz de efetuar as seguintes operações dentro da organização a qual ele pertence:
* Criar, editar e excluir outras contas de administrador no âmbito da rede;
* Criar, editar e excluir redes em que possuam privilégios
* As alterações de configuração, remoção ou adição de equipamentos deve ser registrada com dia, hora, e nome do administrador que a realizou.
* Identificar tentativas, com sucesso, ou não de login na plataforma de gerencia.
* Funcionalidade de criação de templates a fim de facilitar a configuração de diversos equipamentos simultaneamente.
* Sistema automatizado de upgrade de firmware a fim dos equipamentos estarem sempre com a última versão estável de firmware.
* Definir período de expiração da senha do administrador.
* Forçar o administrador a não usar as mesmas senhas anteriores
* Bloquear o acesso a plataforma após falhas de login
* Configurar logout da plataforma após minutos sem atividade
* Permitir que a plataforma de gerenciamento seja acessível apenas de IP's permitidos
* Apresentar inventário de equipamentos da solução que estão, ou não, em utilização.
* A console de administração deve possuir ferramenta integrada para captura de pacotes que passam pelos equipamentos de segurança gerenciados. Caso não haja funcionalidade nativa será aceita solução externa.
* Capacidade de identificação de dispositivos que se conectam por meio do appliance, com fio ou sem fio através do endereço IP ou MAC
* Suporte para a criação e o gerenciamento de VLANs utilizando o protocolo IEEE 802.1Q.
* Suportar criação de rotas estáticas
* O acesso a rede através do equipamento deve poder ser feito após autenticação em captive portal. Os métodos para essa autenticação devem ser:
* Click-through
* servidor radius
* credenciais de redes sociais
* Deve possuir a definição de uma lista de URLs e IPs para que o usuário possa acessar antes de sua autenticação.
* O portal cativo deve ser personalizável
* Por meio da mesma console de administração, deve ser possível gerar os relatórios de funcionamento correspondente a todos os equipamentos de segurança da solução.
* A solução deve suportar atribuição de políticas de segurança, filtro e QoS de acordo com a identidade do usuário conectado à rede baseado em: endereço MAC, IP, nome do usuário no Active Directory, LDAP ou RADIUS.
* A solução deve entregar, de maneira integrada ou não, ferramentas de visibilidade da rede, usuários, aplicações. Essa ferramenta deve reportar ou permitir no mínimo:
* Listagem identificando cada um dos clientes conectados à rede, identificando no mínimo: status, descrição, utilização, IP, política, MAC address e VLAN;
* Listagem de principais aplicações utilizadas pela rede;
* Listagem dos usuários que mais acessaram determinada aplicação;
* Relatório de utilização por aplicativo, identificando o serviço consultado, a categoria a qual pertence (esporte, música, vídeo, e-mail, tempo real, etc) e a sua utilização em bits por segundo durante o tempo.
* Necessário identificar o usuário e grupo de usuários que fizeram uso desse aplicativo;
* Inventário de equipamentos da solução que estão, ou não, em utilização.
* A ferramenta da gerência deve apresentar status de cada um dos equipamentos tais como: status das interfaces WAN, LAN, utilização dos links WAN, latência dos links WAN, perda de pacotes nos links WAN.
* A ferramenta de gerencia deve apresentar funcionalidades de troubleshooting tais como ping, traceroute, DNS lookup, reiniciar os equipamentos.
* A solução deve gerar sob demanda um relatório de segurança da última hora, última semana, último mês ou em um período específico de acompanhamento.
* Gerar um gráfico no momento de eventos classificados pela sua gravidade (Alta, Média e Baixa), bem como uma lista de eventos de segurança detectadas no período de tempo selecionado.
* Apresentar os clientes afetados pelas ameaças de segurança, tipo de dispositivo, qual localidade ele se encontra, data em que foi afetado e quantidade de eventos.
* Apresentar as ameaças mais relevantes na rede e breve descritivo da mesma
* Apresentar os principais sistemas operacionais afetados na rede.
* Apresentar em detalhes as ameaças encontradas na rede, com no mínimo as seguintes informações: dia/hora, mecanismo que detectou a ameaça (IDS, IPS, Antimalware, filtro de conteúdo), origem, destino, ação tomada, e informações da ameaça
* Notificar os eventos de segurança aos administradores da rede.
* Caso a solução de gerencia ofertada seja baseada em hardware controlador, deve ser considerada solução de alta disponibilidade total do sistema, incluindo alta disponibilidade para configuração, relatórios e bancos de dados.
* O sistema de gestão/visibilidade/configuração deve ser acessível via web, e disponível a partir de qualquer dispositivo dentro ou fora da rede
* Capaz de acessar, configurar e monitorar qualquer dispositivo da solução.
* Implementar autenticação de dois fatores para acesso a administração do sistema, o acesso deve ser feito via HTTPS.
* Possuir sistema hierárquico de gerenciamento onde deve ser possível o administrador definir quais redes determinado usuário pode ter gerencia e visibilidade, deve ser possível definir usuários como "somente leitura" sem direito de alteração das configurações.
* Através do dashboard de gerência na nuvem, deve ser capaz de ativar ferramentas de monitoração de performance de aplicações WEB, baseadas nos protocolos HTTP e HTTPS, fazendo uma avaliação baseada nos fluxos das aplicações, apresentando informações como jitter, latência, perda de pacotes e utilização (em MB).
* Através do dashboard de gerência na nuvem, deve ser capaz de ativar ferramentas de monitoração de performance dos links de WAN, fazendo uma avaliação baseada nos fluxos das aplicações, apresentando informações como jitter, latência, perda de pacotes e utilização (em MB)
* Através do dashboard de gerência na nuvem, deve ser capaz de ativar ferramentas de monitoração de performance de aplicações de Voice Over IP, fazendo uma avaliação baseada nos fluxos das aplicações, apresentando informações como jitter, latência, perda de pacotes e utilização (em MB). As informações de fluxos devem ser agregadas e enviadas para gerencia na nuvem utilizando protocolo TLS-SYSLOG através de porta TCP 6514
* A solução SDWAN, composta por plataforma de gerência e dispositivos de SDWAN, deve suportar ambiente de gerenciamento de atualizações de firmware dos equipamentos SDWAN, de tal maneira que esse ambiente permita que, os administradores de rede agendem facilmente as atualizações de firmware em suas redes, aceitem as versões beta do firmware, visualizar notas de log de alteração de firmware, visualizar números de versão de firmware e reverter o firmware em uma rede atualizada recentemente, ou seja, possam automatizar todos o processo de atualizações de firmwares dos equipamentos em questão.
* Suportar mecanismo avançado de reconhecimento de aplicações camada 7, utilizando técnicas avançadas de classificação e cujas regras de classificação sejam facilmente atualizáveis através da plataforma de gerenciamento, sem a necessidade de intervenção local nos equipamentos de SDWAN. Esse mesmo mecanismo deve ser capaz de detectar pelo menos 1.500 aplicativos e subclassificações, com menos de 1% de falso-positivo em tráfego criptografado desconhecido, e menos de 1% não classificado. Uma vez classifica as aplicações, deve ser capaz de implementar mecanismos de controle de trafego baseados em "traffic-shapping" por aplicação, e por usuários da rede, permitindo também a visualização analítica das aplicações utilizadas pelos usuários.
* O sistema operacional dos equipamentos em questão deve suportar camada de abstração de software chamada de camada de administração. Usar Docker Engine ou similar. O Docker Engine é o componente principal da plataforma Docker, responsável por construir, executar e gerenciar contêineres. Trata-se de um "runtime" e ferramentas leves que gerenciam Containers, imagens, redes e volumes. Deve ser possível efetuar o download e ativação desses containers em todos os equipamentos da solução de SDWAN, a partir da plataforma de gerência dos equipamentos.
* Os equipamentos, ao serem conectados à internet, devem automaticamente estabelecer um canal seguro de comunicação com ambiente de gerenciamento em nuvem, e uma vez estabelecida esta conectividade, devem automaticamente se registrar na respectiva rede ou organização onde foram previamente associados, efetuando esse processo sem a necessidade de qualquer pré-configuração via interface de gerenciamento local do equipamento.
* Possuir mecanismo que não permita a utilização do equipamento em outras redes e ambientes, em caso de furto. A ferramenta de gerência na nuvem deve ser capaz de bloquear o equipamento, e caso ele seja reconectado a internet, detectar e rastrear o equipamento, baseado no endereço IP público utilizado pelo mesmo.
 |
| 7 | Instalação do item 6 |
| 8 | **FIREWALL/ROTEADOR TIPO II COM LICENÇA DE SOFTWARE PARA PLATAFORMA DE GERENCIAMENTO EM NUVEM POR PERÍODO DE 60 MESES.*** Novos e homologados pela ANATEL;
* Todos os hardwares e softwares devem ser do mesmo fabricante;
* Todas as features avançadas de segurança (URL Filtering, IPS e Antimalware) devem ser do mesmo fabricante e nativamente integradas aos equipamentos ofertados.
* O equipamento de segurança com capacidade de SD-WAN deve ser um sistema integrado UTM (Unified Threat Management) que inclua pelo menos as seguintes características:
* Firewall de estados (Stateful Firewall);
* Filtro de conteúdo com no mínimo oitenta (80) categorias pré-definidas;
* Antimalware;
* Concentrador VPN para gateways e clientes;
* IDS e IPS;
* Roteamento baseado em políticas;
* Balanceamento de, no mínimo, 02 (dois) links WAN e mecanismo para seleção de melhor caminho a ser definido por aplicação camada 7, automaticamente baseado em, no mínimo, jitter, perda de pacotes e delay.
* Suportar no mínimo 2Gbps de tráfego de IPSEC VPN com criptografia AES;
* Suportar no mínimo 6Gbps de tráfego de “stateful firewall”, com as todas as funcionalidades de segurança habilitadas;
* Possuir interface USB para conexão de modem 3G/4G;
* Possibilidade de ser configurado em alta disponibilidade;
* Implementar mínimo 02 (duas) interfaces 10Gigabit Ethernet SFP+ para segmento WAN/Internet, sendo necessário que no mínimo, as duas interfaces WAN estejam simultaneamente ativas
* Mínimo 08 (oito) interfaces Gigabit-Ethernet para segmento LAN com conectores padrão UTP.
* Mínimo 08 (oito) interfaces Gigabit-Ethernet para segmento LAN com conectores padrão SFP.
* Mínimo 08 (oito) interfaces 10 Gigabit-Ethernet para segmento LAN com conectores padrão SFP+.
* Implementar recurso de web-caching sem a necessidade de utilizar equipamento externo para tal.
* Acompanhado com fonte de alimentação AC 110/220v padrão ABNT;
* Implementar funcionalidade de Firewall Stateful camada 7;
* A solução deverá suportar a definição de regras de firewall de camada 3 e Camada 7;
* Regras de políticas de acesso de camada 3 definidas por:
* Protocolo (UDP ou TCP)
* Host, sub-rede ou rede de origem;
* Porta TCP ou UDP de origem;
* Host, sub-rede ou rede de destino;
* Porta TCP ou UDP de destino;
* Através das regras da camada 7, deve suportar a restrição de tráfego a partir de categorias definidas, incluindo:
	+ Blog;
	+ E-mail;
	+ Compartilhamento de arquivos;
	+ Jogos;
	+ Noticias;
	+ Backup on-line;
	+ Ponto a ponto;
	+ Redes sociais e compartilhamento de fotos;
	+ Atualizações de softwares e antivírus;
	+ Esportes;
	+ Videoconferência e VoIP;
	+ Compartilhamento de arquivos via Web;
	+ Hostname http;
	+ Por Países, GeoIP-Firewall;
* Suporte a NAT 1:1 e o redirecionamento de portas (Port Forwarding) para a publicação de sistemas específicos para a Internet.
* Implementar funcionalidade de criação automatizada de tuneis IPSEC VPN entre equipamentos dentro da mesma organização;
* Implementar a criação de VPNs para acesso remoto de usuários usando IPSec L2TP
* As VPNs site-to-site devem poder ser configuradas em modo hub-spoke ou full-mesh
* Suportar NAT-transversal
* Permitir a criação de tuneis IPSEC VPN site-to-site com equipamentos de terceiros.
* Permitir a conexão com client VPN
* Permitir a integração nativa com Active Directory
* SDWAN
* Implementar solução de SDWAN capaz de balancear trafego entre os links WAN;
* Quando a função de balanceamento de carga estiver desativada, todo o tráfego da WAN deve usar o link principal, com redundância para link secundário e como uma terceira opção a conexão 3G/4G em caso de falha dos links primário e secundário
* Configurar a largura de banda dos links principais e backup (celular) de maneira independente
* Definir qual o link principal do equipamento
* Habilitar ou desabilitar o balanceamento de trafego entre os links
* Configurar qual dos links WAN será utilizado para acessar a internet por determinada rede (IP e/ou porta TCP-UDP) para trafego encapsulado deve ser possível escolher qual link será utilizado para acessar a localidade central baseado em camada 3, 4 e 7 a escolha de qual link será utilizado deve ser automatizada e inteligente baseado em, no mínimo, condições do link como jitter, delay e perda de pacotes.
* O chaveamento entre os links deve ser automático uma vez atingido níveis não aceitáveis das características citadas acima.
* Decidir os níveis de qualidade do link e seu chaveamento por aplicação.
* A política de modelagem de tráfego deve permitir a atribuição de limites de largura de banda simétricos ou assimétricos por aplicativo, por usuários e por grupo de usuários.
* Suportar BGP, OSPF e roteamento estático para divulgar as rotas as localidades remotas.
* Através da política de modelagem de tráfego deve ser capaz de serem priorizados determinados tipos de tráfego e/ou associados com um rótulo de QoS usando DSCP com pelo menos 4 classes de serviço (Melhor esforço, background, vídeo e voz)
* Filtro de conteúdo
* A solução deverá implementar recursos de filtro de conteúdo:
* A solução de filtro de conteúdo deverá ter categorias pré-definidas para bloqueio.
* Permitir a habilitação da funcionalidade "safesearch" ou equivalente assegurando o conteúdo das páginas de busca como google, bing, etc.
* Criação de blacklist baseada em URL, para sites que nunca devem ser acessados.
* Criação de whitelist, onde estas URL não serão avaliadas pelo filtro de conteúdo
* Detecção e prevenção de intrusões IPS/IDS:
* A solução deve colocar à disposição da instituição a habilidade de ativar o módulo IDS e IPS.
* Ativação ou desativação do módulo IDS/IPS para grupos de usuários.
* Inclusão em whitelist de uma ou várias assinaturas de IDS/IPS para remover da ação de bloqueio.
* Habilitar o nível de proteção baseado em score CVSS
* As assinaturas devem ser atualizadas diariamente, automaticamente, diretamente com o serviço de segurança da fabricante;
* Detectar e bloquear exploits, vírus, rootkits entre outras ameaças;
* Antimalware
* A solução deve possuir antimalware protection;
* A funcionalidade de antimalware deve, no mínimo, avaliar os seguintes tipos de arquivos:
	+ MS OLE2 (.doc, .xls, .ppt)
	+ MS Cabinet (Microsoft compression type)
	+ MS EXE
	+ ELF (Linux executable)
	+ Mach-O/Unibin (OSX executable)
	+ Java (class/bytecode, jar, serialization)
	+ PDF
	+ ZIP (regular and spanned)
	+ EICAR (standardized test file)
	+ SWF (shockwave flash 6, 13, and uncompressed)
* Caso algum malware seja encontrado deve ser possível enviar um alerta ao administrador da rede.
* Características gerais de gerenciamento da solução:
* A solução proposta deve atender às seguintes especificações:
* Gestão centralizada a partir de uma console de administração baseada na Web e a partir da qual deve ser possível o acesso, configuração e monitoramento de todos os equipamentos de segurança contemplados na solução.
* Por meio da console de gerenciamento deve ser possível a configuração de todas as funcionalidades descritas anteriormente;
* Deve haver mecanismos para agrupar logicamente a administração de um certo número de dispositivos UTM para envio de modificações em suas configurações simultaneamente.
* A plataforma de gerencia deve ser possível identificar cada uma das localidades remotas com uma identificação administrativa para posteriormente ser usada como filtro de pesquisa.
* O acesso a console de gerenciamento deve ser realizado com o uso de um método de autenticação de dois fatores
* O acesso a console deve ser por HTTPS (portas 8080 e 443) e seus certificados de segurança devem ser emitidos por entidades reconhecidas na Internet.
* A console de gerenciamento deve suportar a definição de contas de administrador com base em funções, relatar as alterações às mesmas em um log de eventos e alertas que podem ser consultados por meio da mesma console.
* O nível hierárquico de administradores da console deve conter:
* Administrador de Organização: Um administrador da organização deverá ter visibilidade em todas as redes dentro da organização. Deverão existir dois tipos de administradores da organização: (1) acesso total e (2) somente leitura.
* O administrador com acesso total pode efetuar as seguintes operações dentro da organização a qual ele pertence:
* Criar, editar e excluir contas de acesso total e somente leitura para a organização;
* Redefinição de senhas;
* Criar, editar e excluir redes;
* Adicionar novos dispositivos à rede da organização.
* Administrador de Rede: Terão visibilidade nas redes da organização para as quais tenham sido designados como um administrador. Deverão existir dois tipos de administradores de rede: (1) acesso total e (2) somente leitura. Um administrador de rede com acesso total será capaz de efetuar as seguintes operações dentro da organização a qual ele pertence:
* Criar, editar e excluir outras contas de administrador no âmbito da rede;
* Criar, editar e excluir redes em que possuam privilégios.
* As alterações de configuração, remoção ou adição de equipamentos deve ser registrada com dia, hora, e nome do administrador que a realizou.
* Identificar tentativas, com sucesso, ou não de login na plataforma de gerencia.
* Criação de templates a fim de facilitar a configuração de diversos equipamentos simultaneamente.
* Sistema automatizado de upgrade de firmware a fim dos equipamentos estarem sempre com a última versão estável de firmware.
* Definir período de expiração da senha do administrador.
* Forçar o administrador a não usar as mesmas senhas anteriores
* Bloquear o acesso a plataforma após falhas de login
* Configurar logout da plataforma após minutos sem atividade
* Permitir que a plataforma de gerenciamento seja acessível apenas de IP's permitidos
* Apresentar inventário de equipamentos da solução que estão, ou não, em utilização.
* Ferramenta integrada para captura de pacotes que passam pelos equipamentos de segurança gerenciados. Caso não haja funcionalidade nativa será aceita solução externa.
* Capacidade de identificação de dispositivos que se conectam por meio do appliance, com fio ou sem fio através do endereço IP ou MAC
* Suporte para a criação e o gerenciamento de VLANs utilizando o protocolo IEEE 802.1Q.
* Criação de rotas estáticas;
* O acesso a rede através do equipamento deve poder ser feito após autenticação em captive portal. Os métodos para essa autenticação devem ser:
	+ Click-through;
	+ Servidor radius.
	+ Credenciais de redes sociais
* Possuir a definição de uma lista de URLs e IPs para que o usuário possa acessar antes de sua autenticação.
* O portal cativo deve ser personalizável;
* Por meio da mesma console de administração, deve ser possível gerar os relatórios de funcionamento correspondente a todos os equipamentos de segurança da solução.
* A solução deve suportar atribuição de políticas de segurança, filtro e QoS de acordo com a identidade do usuário conectado à rede baseado em: endereço MAC, IP, nome do usuário no Active Directory, LDAP ou RADIUS.
* A solução deve entregar, de maneira integrada ou não, ferramentas de visibilidade da rede, usuários, aplicações. Essa ferramenta deve reportar ou permitir no mínimo:
* Listagem identificando cada um dos clientes conectados à rede, identificando no mínimo: status, descrição, utilização, IP, política, MAC address e VLAN;
* Listagem de principais aplicações utilizadas pela rede;
* Listagem dos usuários que mais acessaram determinada aplicação;
* Contar com um relatório de utilização por aplicativo, identificando o serviço consultado, a categoria a qual pertence (esporte, música, vídeo, e-mail, tempo real, etc) e a sua utilização em bits por segundo durante o tempo. É necessário identificar o usuário e grupo de usuários que fizeram uso desse aplicativo;
* Inventário de equipamentos da solução que estão, ou não, em utilização.
* A ferramenta da gerencia deve apresentar status de cada um dos equipamentos tais como: status das interfaces WAN, LAN, utilização dos links WAN, latência dos links WAN, perda de pacotes nos links WAN.
* A ferramenta de gerencia deve apresentar funcionalidades de troubleshooting tais como ping, traceroute, DNS lookup, reiniciar os equipamentos;
* A solução deve gerar sob demanda um relatório de segurança da última hora, última semana, último mês ou em um período específico de acompanhamento.
* Gerar um gráfico no momento de eventos classificados pela sua gravidade (Alta, Média e Baixa), bem como uma lista de eventos de segurança detectadas no período de tempo selecionado.
* Apresentar os clientes afetados pelas ameaças de segurança, tipo de dispositivo, qual localidade ele se encontra, data em que foi afetado e quantidade de eventos.
* Apresentar as ameaças mais relevantes na rede e breve descritivo da mesma
* Apresentar os principais sistemas operacionais afetados na rede.
* Apresentar em detalhes as ameaças encontradas na rede, com no mínimo as seguintes informações: dia/hora, mecanismo que detectou a ameaça (IDS, IPS, Antimalware, filtro de conteúdo), origem, destino, ação tomada, e informações da ameaça
* Notificar os eventos de segurança aos administradores da rede.
* Caso a solução de gerencia ofertada seja baseada em hardware controlador, deve ser considerada solução de alta disponibilidade total do sistema, incluindo alta disponibilidade para configuração, relatórios e bancos de dados.
* O sistema de gestão/visibilidade/configuração deve ser acessível via web, e disponível a partir de qualquer dispositivo dentro ou fora da rede
* Acessar, configurar e monitorar qualquer dispositivo da solução.
* Implementar autenticação de dois fatores para acesso a administração do sistema, o acesso deve ser feito via HTTPS.
* Possuir sistema hierárquico de gerenciamento onde deve ser possível o administrador definir quais redes determinado usuário pode ter gerencia e visibilidade, deve ser possível definir usuários como "somente leitura" sem direito de alteração das configurações.
* Através do dashboard de gerencia na nuvem, deve ser capaz de ativar ferramentas de monitoração de performance de aplicações WEB, baseadas nos protocolos HTTP e HTTPS, fazendo uma avaliação baseada nos fluxos das aplicações, apresentando informações como jitter, latência, perda de pacotes e utilização (em MB).
* Através do dashboard de gerencia na nuvem, deve ser capaz de ativar ferramentas de monitoração de performance dos links de WAN, fazendo uma avaliação baseada nos fluxos das aplicações, apresentando informações como jitter, latência, perda de pacotes e utilização (em MB)
* Através do dashboard de gerencia na nuvem, deve ser capaz de ativar ferramentas de monitoração de performance de aplicações de Voice Over IP, fazendo uma avaliação baseada nos fluxos das aplicações, apresentando informações como jitter, latência, perda de pacotes e utilização (em MB). As informações de fluxos devem ser agregadas e enviadas para gerencia na nuvem utilizando protocolo TLS-SYSLOG através de porta TCP 6514.
* A solução SDWAN, composta por plataforma de gerencia e dispositivos de SDWAN, deve suportar ambiente de gerenciamento de atualizações de firmware dos equipamentos SDWAN, de tal maneira que esse ambiente permita que, os administradores de rede agendem facilmente as atualizações de firmware em suas redes, aceitem as versões beta do firmware, visualizar notas de log de alteração de firmware, visualizar números de versão de firmware e reverter o firmware em uma rede atualizada recentemente, ou seja, possam automatizar todos o processo de atualizações de firmwares dos equipamentos em questão.
* Suportar mecanismo avançado de reconhecimento de aplicações camada 7, utilizando técnicas avançadas de classificação e cujas regras de classificação sejam facilmente atualizáveis através da plataforma de gerenciamento, sem a necessidade de intervenção local nos equipamentos de SDWAN. Esse mesmo mecanismo deve ser capaz de detectar pelo menos 1.500 aplicativos e subclassificações, com menos de 1% de falso-positivo em tráfego criptografado desconhecido, e menos de 1% não classificado. Uma vez classifica as aplicações, deve ser capaz de implementar mecanismos de controle de trafego baseados em "traffic-shapping" por aplicação, e por usuários da rede, permitindo também a visualização analítica das aplicações utilizadas pelos usuários.
* Os equipamentos, ao serem conectados à internet, devem automaticamente estabelecer um canal seguro de comunicação com ambiente de gerenciamento em nuvem, e uma vez estabelecida esta conectividade, devem automaticamente se registrar na respectiva rede ou organização onde foram previamente associados, efetuando esse processo sem a necessidade de qualquer pre-configuração via interface de gerenciamento local do equipamento.

Possuir mecanismo que não permita a utilização do equipamento em outras redes e ambientes, em caso de furto. A ferramenta de gerencia na nuvem deve ser capaz de bloquear o equipamento, e caso ele seja reconectado a internet, detectar e rastrear o equipamento, baseado no endereço IP público utilizado pelo mesmo. |
| 9 | Instalação do item 8 |
| 10 | **GATEWAY DE VOZ COM GARANTIA DE 60 MESES.*** O gateway de voz deve oferecer conectividade de chamadas Voz sobre IP (VoIP), além de conectar ligações PSTN e ou chamadas digitais. O gateway de voz deve suportar modulo com 1 slots NIM.
* O equipamento deve possuir as seguintes conectorizações mínimas:
	+ 1 interface USB 3.0 – Tipo A;
	+ 1 interface USB 3.0 mini-Tipo C;
	+ 1 porta console RJ-45;
	+ 1 porta console micro USB;
	+ Possuir 4 interfaces do tipo E1 e 8 interfaces do tipo FXO, para suportar a demanda de chamadas do Sistema de Telefonia descritos neste Termo;
	+ Possuir 6 interfaces ethernet de 1 Gigabit.
* Possuir licença SIP TRUNK para, no mínimo,10 conexões.
* **FUNCIONALIDADES**
* Possuir capacidade de suportar conectividade WAN de no mínimo 1Gbps;
* Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas.
* Possuir configuração de Memória RAM de no mínimo 16GB, para a implementação de todas as funcionalidades descritas nesta especificação.
* Possuir módulo de processamento digital de sinal (módulo DSP) suficiente para suportar 4 interfaces E1 e 8 interfaces FXO, além de outras funcionalidades como a quantidade de sessões do Session Border Controller;
* Fornecer ao menos 1 cabo de console compatível com a porta de console do equipamento;
* Fornecer 4 Cabos padrão BNC, para conectar as interfaces E1 contempladas no Gateway de voz;
* Suportar simultaneamente em sua memória Flash (ou semelhante), duas imagens do sistema operacional entregue com a solução.
* **FONTE DE ALIMENTAÇÃO**
* Possuir fonte de alimentação interna AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e freqüência (de 50/60 Hz).
* Possuir cabo de alimentação para a fonte com, no mínimo, 1,80m (um metro e oitenta centímetros) de comprimento.
* **DIMENSÕES**
* Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.
* **VISUALIZAÇÃO**
* Possuir LEDs para a indicação do status das portas e atividade.
* **GERENCIAMENTO**
* Implementar os padrões abertos de gerência de rede SNMP,incluindo a geração de traps.
* Suportar SNMP sobre IPv6
* Possuir suporte a MIB II, conforme RFC 1213.
* Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.
* Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa.
* Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP.
* Possuir armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 2048 bytes.
* Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas.
* Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas.
* Permitir o gerenciamento via CLI e Web, utilizando SSH e HTTPS.
* Capacidade de gerenciar múltiplas conexões VoIP.
* Possuir uma porta auxiliar serial assíncrona para acesso gerencial remoto.
* Implementar nativamente 4 grupos RMON (History, Statistcs, Alarms e Events) conforme RFC 1757.
* O equipamento deve suportar a configuração com um único endereço IP para gerência e administração, para uso dos protocolos: SNMP, NTP, HTTPS, SSH, Telnet, TACACS+ e RADIUS, provendo identificação gerencial única ao equipamento de rede.
* Possibilidade de criação de versões de configuração e suporte à “rollback” da configuração para versões anteriores.
* **FACILIDADES**
* Implementar Telnet para acesso à interface de linha de comando.
* Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet e serial.
* Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, FTP, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes.
* Permitir a atualização de sistema operacional através do protocolo TFTP ou FTP.
* Permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP).
* Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES.
* Permitir que a sua configuração seja feita através de terminal assíncrono.
* Permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes Syslog gerados pelo switch.
* Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
* Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.
* Suportar IPv6.
* Suportar protocolo de coleta de informações de fluxos que circulam pelo equipamento contemplando no mínimo as seguintes informações:
* IP de origem/destino
* Parâmetro “protocol type” do cabeçalho IP
* Porta TCP/UDP de origem/ destino
* Interface de entrada do tráfego
* Especificar o uso de tal funcionalidade somente para tráfego de entrada, somente para tráfego de saída (e também para ambos os sentidos simultaneamente) em uma dada interface do roteador
* A informação coletada deve ser automaticamente exportável em intervalos pré definidos através de um protocolo ipfix (Net Flow ou SFlow ou JFlow ou HFlow) padronizado.
* **PROTOCOLOS**
* Implementar o protocolo NTP.
* Implementar DHCP Relay e DHCP Server.
* Implementar o protocolo VRRP (RFC 2338) ou mecanismo similar de redundância de gateway. Suportar mecanismo de autenticação MD5 entre os peers VRRP.
* **PROTOCOLOS WAN**
* No caso específico do encapsulamento Frame Relay devem ser suportadas, no mínimo, as seguintes funcionalidades:
* FRF.15 e FRF.16: Multilink Frame Relay
* Permitir compressão dos datagramas IP.
* Implementar PPP (Point to Point Protocol) sobre Ethernet (PPP Over Ethernet).
* Implementar Multiprotocol Label Switching (MPLS).
* Implementar Locator ID Separation Protocol (LISP).
* **ROTEAMENTO**
* Implementar roteamento estático.
* Implementar roteamento dinâmico RIPv2.
* Implementar protocolo de roteamento dinâmico OSPF.
* Implementar protocolo de roteamento BGP.
* Permitir o roteamento nível 3 entre VLANs.
* Permitir a virtualização das tabelas de roteamento camada 3. As tabelas virtuais deverão ser completamente segmentadas.
* Suporte ao protocolo de Tunelamento GRE (General Routing Encapsulation), contemplando, no mínimo, os seguintes recursos:
* Permitir a associação do túnel GRE a uma tabela virtual de roteamento específica, definida pelo administrador do equipamento.
* Possibilidade de configuração de “Keepalive” nos túneis.
* Suporte a QoS (qualidade de serviço) - deve ser possível a cópia da informação de classificação de tráfego existente no cabeçalho do pacote original para os pacotes transportados com encapsulamento GRE.
* Implementar roteamento baseado em origem, com possibilidade de definição do próximo salto camada 3, baseado em uma condição de origem.
* Implementar Enhanced Interior Gateway Routing Protocol (EIGRP).
* **ROTEAMENTO IPv6**
* Suportar roteamento estático para IPv6.
* Implementar roteamento dinâmico RIPng.
* Suportar protocolo de roteamento dinâmico OSPFv3 para IPv6.
* Implementar protocolo de roteamento Multiprotocol BGP com suporte a IPv6.
* Deve implementar, no mínimo 1.500.000 rotas IPv6 com possibilidade de ampliação para 4.000.000 de rotas;
* **DESEMPENHO**
* Suportar a capacidade de tráfego de IPv4 de, no mínimo, 19,7 Gbps considerando como tráfego pacotes de 1400 bytes.
* Suportar a capacidade de tráfego de IPsec, no mínimo, 1,9 Gbps considerando como tráfego pacotes de 1400 bytes.
* Suportar 4.000 (quatro mil) Tuneis IPsec SVTI.
* **SEGURANÇA**
* Implementar mecanismo de autenticação para acesso local ou remoto ao
* equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS e

RADIUS.* Implementar no mínimo 4.000 (quatro mil) lista de controle de acesso (ACL - Access Control List), para IPv4 e IPv6.
* Especificar o horário e dia da semana em que devem ser
* automaticamente ativadas as ACLs.
* Implementar listas de controle de acesso (ACLs), para filtragem de pacotes,
* baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e
* flags TCP.
* Proteger a interface de comando do equipamento através de senha.
* Implementar o protocolo SSH para acesso à interface de linha de comando.
* Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao gateway via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.
* Permitir a inserção de certificado, para autenticação do protocolo SSH e Tuneis IPSEC.
* Implementar mecanismos de AAA (Authentication, Authorization e Accounting)
* com garantia de entrega.
* Implementar a criptografia de todos os pacotes enviados ao servidor de controle de
* acesso e não só os pacotes referentes à senha.
* Permitir controlar e auditar quais comandos os usuários e grupos de usuários
* podem emitir em determinados elementos de rede.
* **FUNCIONALIDADES DE VPN**
* Suportar serviços de VPN baseados no padrão IPSec (IP Security Protocol)
* Suportar serviços de VPN baseados no padrão IKE (Internet Key Exchange)
* Suportar algorítmos de criptografia DES, 3DES, 128-bit AES e 256-bit AES para conexões com VPN IPSec.
* Reagrupar pacotes de sessão fragmentados para análise e entrega no destino.
* Suportar a criação de VPNS IPSEC baseada em políticas de segurança.
* Suportar criação de VPNs de acordo com o conjunto de padrões IPSEC em modo
* túnel.
* Modos de operação “tunnel mode” e “transport
* mode”.
* Suportar no mínimo as RFCs 1828, 1829, 2401, 2402, 2406, 2407, 2408 e 2409.
* Suportar as funcionalidades de gerenciamento de chaves para VPN.
* Suportar a utilização de clientes baseados em IPSEC.
* **PADRÕES**
* Implementar padrão IEEE 802.1q (Vlan Frame Tagging).
* Implementar padrão IEEE 802.1p (Class of Service) para cada porta.
* Implementar padrão IEEE 802.3ad.
* Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).
* Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control).
* **MULTICAST**
* Implementar mecanismo de controle de multicast através de IGMPv3.
* Implementar roteamento multicast PIM (Protocol Independent Multicast) nos modos “sparse-mode” (RFC 2362).
* **QUALIDADE DE SERVIÇO (QoS)**
* Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p.
* Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo).
* Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.
* Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" – nível 2) e DSCP ("Differentiated Services Code Poin\"- nivel 3), conforme definições do IETF (Internet Engineering Task Force).
* Suportar funcionalidades de QoS de “Traffic Shaping” e “Traffic Policing”.
* Possível a especificação de banda por classe de serviço.
* Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como: transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote.
* Suporte aos mecanismos de QoS WRED (Weighted Random Early Detection).
* Implementar RTP (Real-Time Transport Protocol) e a compressão do cabeçalho dos pacotes RTP (IP RTP Header Compression).
* Implementar priorização nível 2 IEEE 802.1p e priorização nível 3 dos tipos “IP precedence” e DSCP (Differentiated Services Code Point).
* O roteador deve suportar o mapeamento das prioridades nível 2 (IEEE 802.1p) em prioridades nível 3 (IP Precedence e DSCP) e vice-versa.
* Implementar política de enfileiramento nas linhas seriais (priorização de tráfego por tipo de protocolo trafegado).
* Suportar pelo menos as seguintes técnicas de enfileiramento: Priority Queuing, Weighted Fair Queuing, Class-Based Weighted Fair Queuing e Low Latency Queuing.
* Implementar RSVP (Resource Reservation Protocol).
* **INTERNET PROTOCOL VERSÃO 6 (IPV6)**
* Implementar IPv6.
* Permitir a configuração de endereços IPv6 para gerenciamento.
* Permitir consultas de DNS com resolução de nomes em endereços IPv6.
* Implementar ICMPv6 com as seguintes funcionalidades:
* Implementar protocolos de gerenciamento Ping, Traceroute, SSH, SNMP, SYSLOG e DNS sobre IPv6.
* **INTERCONEXÃO COM A ESTRUTURA ATUAL**
* A Solução de telefonia ofertada deverá permitir a interoperabilidade com o atual sistema de telefonia existente. Permitindo que com a aquisição de novos aparelhos, os ramais do sistema de telefonia atual possam ser migrados para a nova solução.
 |
| 11 | Instalação do item 10 |
| 12 | **PONTO DE ACESSO WIFI 6 COM LICENÇA DE SOFTWARE PARA PLATAFORMA DE GERENCIAMENTO EM NUVEM POR PERÍODO DE 60 MESES, INCLUINDO INSTALAÇÃO.*** Implementar terceiro rádio WIFI dedicado para análise de espectro e funcionalidades de segurança através da implementação de Sistema de prevenção de intrusão sem fio (WIPS). Esse rádio deverá ser capaz de atuar nas frequências de 2.4Ghz e 5Ghz
* Permitir configurar o SSID para trabalhar nos modos NAT e BRIDGE.
* A plataforma de gerência na nuvem, e conjunto com equipamentos de ponto de acesso, devem implementar mecanismo de controle de acesso de acordo com o padrão Hotspot 2.0, baseado no padrão 802.11u IEEE.
* A plataforma de gerência na nuvem deve implementar ferramenta de troubleshooting na console de gerência dos access points, permitindo realizar testes via protocolo ICMP (ex PING) utilizando endereços IPV4 e IPV6
* Suportar a conexão de, no mínimo, 512 dispositivos simultâneos por rádio;
* A plataforma de gerência na nuvem, e conjunto com equipamentos de ponto de acesso, devem implementar localização de ativos ("Asset Location") baseada no protocolo BLE (Bluetooth Low Energy) e WIFI. As informações apresentadas devem incluir capacidade de visualizar graficamente no mapa onde estão geograficamente distribuídos os ativos em questão.
* Implementar padrão IPV6, incluindo conectividade com a gerência na nuvem através de dual-Stack (IPv4 e IPv6) e regras de saída (outbound) de firewall de camada 3 com endereços IPv4 e IPv6 de destino.
* Possuir mecanismo que não permita a utilização do Access Point em outras redes e ambientes, em caso de furto. A ferramenta de gerência na nuvem deve ser capaz de bloquear o equipamento, e caso ele seja reconectado à internet, detectar e rastrear o equipamento, baseado no endereço IP público utilizado pelo mesmo
* Implementar recursos de deteção e filtro de aplicações, possuindo um base de reconhecimento de, no mínimo, 1500 tipos de aplicações, para reconhecimento e bloqueio de conteúdos relacionados a jogos, compartilhamento de arquivos, redes sociais, entre outros. Caso este recurso necessite de licença, a mesma deve ser fornecida pelo mesmo período de tempo coberto pela garantia solicitada neste ETP
* Implementar roaming de camada 3 distribuído, onde seja possível configurar VPN e/ou tunelamentos entre access points, sem a necessidade de um apiance e/ou concentrador externo para tal função
* Implementar solução segurança baseada em DNS com as seguintes características mínimas:
* Possuir no mínimo 50 categorias de URL Filtering; deve possuir logs de bloqueio e liberação de acessos a URLs;
* Bloquear domínios suspeitos de propagar ou implementar atividades que comprometam a segurança dos usuários, tais como propagação de malware, atividades de phishing, botnet e outros;
* Suportar multi-user MIMO bidirecional (fluxos espaciais de downlink e uplink simultâneos), otimizando dessa maneira a diversidade de fluxo de dados entre cliente e access point.
* Suporta e implementar padrão IEEE 802.1x e suportar suplicante na porta ethernet, de tal maneira que o equipamento deve usar o certificado digital para se autenticar na porta do switch onde será conectado, via 802.1X e ter permissão de acesso à rede mediante autenticação bem-sucedida.
* Suportar tráfego agregado de, no mínimo, 2.90 Gbps;
* Possuir no mínimo 01 (uma) porta MultiGigabit 1x 100/1,000/2.5G BASE-T Ethernet (RJ45)
* Deve implementar rádio para acesso de clientes na frequência de 2.4GHz, com no mínimo, suporte a MIMO 4x4 com 4 fluxos espaciais;
* Deve implementar rádio para acesso de clientes na frequência de 5GHz, com no mínimo, suporte a MIMO 4x4 com 4 fluxos espaciais;
* Deve possuir antenas internas integradas (embutidas) com ganho de, no mínimo, 5.4 dBi para 2,4 GHz e 6 dBi para 5 GHz, ou possuir conectores para instalação de antenas externas
* A solução de controladora em nuvem deverá ser do mesmo fabricante do ponto de acesso a fim de garantir uma perfeita interoperabilidade;
* Plataforma em nuvem, responsável pelas seguintes funções na rede sem fio: administração, configuração e gerenciamento completo centralizado dos pontos de acesso WiFi com funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Rádio Frequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários;
* A solução de Controladora sem fio em nuvem não deve ter restrição de licença que limite o número de Ponto de Acesso a ser controlado por ela, sendo escalável para gerenciar, no mínimo, 10.000 (dez mil) pontos de acesso;
* Disponibilizar uma Console de Gerenciamento Web acessível através de protocolo Criptografado, compatível com os principais browsers do mercado (Internet Explorer, Firefox e Chrome), permitindo também acesso a Console através de dispositivos móveis com sistema operacional IOS e Android;
* Possui a capacidade de habilitar e desabilitar os SSIDs de forma automática e com agendamento periódico;
* Realizar procedimentos automáticos de configuração, correção e aperfeiçoamento da cobertura e disponibilidade dos pontos de acesso;
* Possuir ferramenta de gerenciamento para múltiplas localidades integradas;
* Realizar otimização de radiofrequência, monitoramento e alertas;
* Realizar o upgrade de softwares dos pontos de acesso WiFi;
* Empregar criptografia de dados TLS ou SSL no canal de comunicação com os pontos de acesso WiFi;
* Implementar 2FA ou MFA para acesso administrativo a Console de Gerenciamento WEB;
* Implementar integração nativa via SAML para autenticação SSO de acesso a Console de Gerenciamento
* Implementar logoff automático de administradores que estiverem em idle timeout
* Implementar mecanismo que força a troca periódica de senhas dos administradores da console de gerenciamento Web;
* Implementar mecanismo que força a utilização de senha forte para acesso a console de gerenciamento Web;
* Implementar mecanismo que bloqueia o usuário administrativo que tiver mais de 3 Webhooks Wireless (APs)
* Possuir integração com Webhooks;
* Possível realizar abertura de chamados técnicos de suporte pela mesma interface de console de gerenciamento Web
* Integrar nativamente com APIs abertas e documentadas,
* Implementar relatório de compliance PCI, nativamente;
* Disponibilidade mínima de 99,9%;
* Infraestrutura de Data Center distribuídos globalmente,
* Data Centers com certificação ISO27001
* Replicação Real-Time entre seus Data Centers menor que 90 segundos;
* Efetuar backups diários das configurações e arquivos;
* Realizar auditorias de segurança semanais assim como testes intrusivos (PenTesting) feitos por empresa independente;
* Ter arquitetura de Storage Multi-Tier;
* Implementar segmentação de dados e criptografia de dados, garantindo que os dados são armazenados com segurança
* Compliance com GDPR
* Implementar solução nativa de captura de pacotes no Cabo (Ethernet) dos Acess poins, assim como dos clientes conectados nos SSIDs (captura de tráfego dos rádios);
* Implementar integração nativa com a solução Ekahau;
* Possibilitar desativar os leds dos acess points;
* Disponibilizar pelo menos 03 (três) níveis de acesso a Console de Gerenciamento Web, sendo:
	+ Administrador: acesso de leitura e escrita as configurações para o gerenciamento do sistema;
	+ Operador: acesso de apenas leitura as configurações para a monitoria, sem permissão para alterar configurações;
	+ Organizador de Visitantes: acesso e permissão exclusiva para criação de usuários temporários e visitantes para acesso a rede WiFi;
* Permitir a criação de múltiplas redes distintas e segregadas, mas administradas na mesma console, permitindo assim a segmentação e agrupamento de Access Points que tenham objetivos comuns, permitindo uma melhor organização do ambiente de equipamentos administrados;
* Permitir a criação de contas de usuários para acesso à rede WiFI. Estes usuários devem ficar armazenados na própria solução de controladora sem fio em nuvem;
* Implementar recursos que permitam mecanismo de autenticação através de portal Web customizável (cative portal customizável) para clientes visitantes, com usuário e senha. Este mecanismo deve permitir ainda que o cliente visitante crie a sua própria conta de usuário, cuja validação deve ser realizada por meio de mensagem a ser enviada para o e-mail informado pelo cliente visitante durante o cadastro. No caso de a solução gerar um usuário e/ou senha automaticamente, estes dados devem ser informados ao visitante através de e-mail ou sms, ou captive portal. Todo o processo deve ser realizado sem a intervenção do administrador da solução que controla a solução sem fio em nuvem;
* Permitir a visualização de um conjunto de informações de análise dos Access Points que fazem parte da rede sem fio, disponibilizando pelo menos as seguintes informações:
* Relação dos Access Points conectados, disponibilizando no mínimo as informações de Nome, MAC Adresse, Modelo de equipamento e endereço IP;
* Quantidade de dispositivos conectados em cada Access Point, volume de dados utilizado, tempo de disponibilidade e SSIDs;
* Localização dos Access Points em planta baixa inserida no sistema, incorporando informações sobre os equipamentos gerenciados; com integração nativa com GoogleMaps.
* Mapa de Calor;
* Estar licenciado e fornecer analíticos de presença, informando graficamente números relacionados a:
	+ Usuário passantes (Passer By ou Proximity), Visitantes (Visitor) e Engajamento (Engaged ou Loyalty)
	+ Os analíticos devem garantir histórico de dados retroativos de pelo menos 30 dias. Deve ser possível comparar analíticos de diferentes localidades (Sites ou Networks)
* Estar licenciado e fornecer monitoramento proativo com gráficos contendo telemetria informando porcentagem ou número absoluto do sucesso em: Associações, Autenticações, entrega de DHCP e respostas DNS. Os gráficos devem garantir histórico de dados retroativos de pelo menos 30 dias.
* Estar licenciado e fornecer monitoramento proativo com gráficos contendo telemetria informando porcentagem ou número absoluto referente à qualidade de comunicações unificadas (UC), Voz e Vídeo. Latências os gráficos devem garantir histórico de dados retroativos de pelo menos 30 dias.
* Deve permitir a visualização de um conjunto de informações dos dispositivos conectados à rede sem fio, disponibilizando pelo menos os dados abaixo especificados:
* Endereço IP, MAC Address, Hostname, Usuário;
* Sistema Operacional do dispositivo utilizado;
* Tempo de conexão;
* Informação do protocolo de conexão com a rede WiFi, SSID e Ponto de Acesso utilizados;
* Gráficos e Dados de utilização dos Usuários; gráfico com utilização de banda throughput desde as últimas duas horas até 30 dias.
* Exibição das capacidades do dispositivo de rede do cliente conectado: Largura de Banda, Maximum BitRate, Spatial Streams e nível de sinal de conexão.
* Informações de aplicações acessadas
* Disponibilizar um formato de relatório sintético, com o resumo das principais informações estatísticas de utilização dos Access Points, como por exemplo: SSIDs mais usados, usuários com maior consumo de dados, aplicações mais utilizadas, tipos de dispositivos mais usados (Sistema Operacional), Access Points mais utilizados, volume total de banda e quantidade total de usuários. Tal relatório ainda deve possibilitar ser enviado por e-mail, para usuários definidos pelo Administrador; O relatório deverá ter a possibilidade de agendamento e inserção de logotipo customizado no Email a ser enviado pelo sistema.
* Implementar DHCP mandatório impedindo que clientes com IP Fixo se conectem aos SSID;
* Possibilitar o agrupamento dos Access Points suportando a criação e o gerenciamento de grupos de Access Points simultâneos, permitindo assim criar nomenclaturas de organização como "Prédio Central", "Primeiro Andar" entre outros;
* Período de retenção de logs de clientes associados a rede wifi por um período de, no mínimo, 12 (doze) meses
* Fornecer pontos de acesso WiFi idênticos, novos e sem uso anterior. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento, na data de entrega da proposta.
* A configuração dos seus parâmetros operacionais, o gerenciamento das políticas de segurança e de radiofrequência devem ser gerenciadas por uma solução de Controladora sem fio em nuvem.
* Estar licenciado para permitir o controle e gerenciamento centralizado através da solução de controladora sem fio em nuvem por um período de, no mínimo, 60 (sessenta) meses;
* O Ponto de Acesso não deve possuir qualquer restrição ou licenciamento que limite o número de usuários;
* Fornecer, para cada Ponto de Acesso, suporte do fabricante, incluída na licença do equipamento, com tempo de duração equivalente ao tempo de subscrição da licença adquirida
* O Ponto-de-Acesso deve estar com a última e mais atualizada versão de firmware instalada no ato da entrega.
* O Ponto de Acesso deve estar acompanhado de todos os acessórios necessários para instalação, configuração e operacionalização do equipamento, tais como: softwares, cabos de console, kits para fixação, documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;
* Suportar kit antifurto com a finalidade de evitar o furto do equipamento;
* Possibilitar a fixação do equipamento em teto e parede. Devem ser fornecidos todos os acessórios necessários para que possa ser feita a fixação, juntamente com kit antifurto;
* O modelo do equipamento ofertado deve possuir, na data da entrega da proposta, homologação junto a ANATEL com certificado disponível publicamente no endereço eletrônico desta agencia, conforme a Resolução número 242 de 30 de novembro de 2000;
* Possuir todos os acessórios necessários para instalação, configuração e operação do equipamento, tais como: softwares, documentação técnica, acessórios completos de fixação para teto e parede originais do mesmo fabricante, etc;
* Fornecer todas as licenças necessárias para o pleno funcionamento do ponto de acesso em conjunto com a solução de controladora sem fio em nuvem, incluindo todos os recursos especificados neste Termo de Referência;
* permitir à CONTRATANTE a abertura de chamados direto no fabricante; porém a responsabilidade pelo chamado é da CONTRATADA.
* Suportar alimentação via interface de rede através de POE (Power over Ethernet) no padrão 802.3at ou através de fonte de alimentação externa de corrente continua DC-12V.
* Possuir *captive portal* web de autenticação do tipo splash page local ou em conjunto com a solução de controladora sem fio em nuvem. Este portal web de autenticação deve permitir customização e suportar integração com servidor RADIUS do cliente para autenticar os clientes Wi-Fi com informações de usuário e senha;
* Implementar, localmente ou em conjunto com a solução de controladora sem fio em nuvem, integração com AD, RADIUS e LDAP
* Implementar recursos de firewall stateful camada 7;
* Interpretar e encaminhar protocol Bonjour da Apple. As solicitações Bonjour de clientes no SSID especifico deverão ser encaminhadas para uma VLAN definida. Além disso deve ser possível escolher serviços específicos, bem como habilitar o encaminhamento do Bonjour para um subconjunto limitado de serviços, por exemplo, apenas para AirPlay, e outros.
* Implementar a visualização/identificação e marcação das aplicações para permitir o bloqueio ou marcação QoS via DSCP;
* Permitir a definição de endereços MAC para controle de acesso à rede Wi-Fi;
* Implementar controle e traffic shaping de aplicações por usuário reconhecendo no mínimo 1000 aplicações incluindo a disponibilização de relatórios; deve ser fornecido com todas as licenças necessárias para esta funcionalidade.
* Implementar, localmente ou na nuvem, análise de espectro de RF em 2.4GHz e 5gHZ para identificação de outros pontos de acesso intrusos e não autorizados (rogues), além de interferências no canal habilitado no ponto de acesso e nos demais canais configurados na rede WiFi, sem impacto no seu desempenho;
* Realizar, localmente ou na nuvem o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF. Ajustar automaticamente os canais 802.11 e realizar a detecção de interferências e reajustar os parâmetros de Rádio Frequência visando evitar problemas de cobertura e performance;
* Permitir operação simultânea nos padrões IEEE 802.11b/g/n/ax, na faixa de 2,4 GHz, e 802.11a/n/ac/ax, na faixa de 5 GHz, através de rádios independentes (dual radio), com padrão de irradiação omnidirecional;
* Implementar a tecnologia 802.11ax (Wi-Fi 6) e suportar SU-MIMO, DL-MU-MIMO e UL-MU-MIMO
* Possuir certificação Wi-Fi 6 Alliance;
* Suportar BSS-Coloring e TWT;
* Suportar WPA3;
* Implementar nativamente tunelamento IPSEC VPN;
* Implementar High-Throughput (HT): Canais de 20MHz, 40MHz para IEEE 802.11N e VHT20, VHT40 e VHT80 para IEEE 802.11ac;
* Implementar maximal-ratio combining (MRC) e Beamforming;
* Implementar DL-OFDMA e UL-OFDMA;
* Ser compatível com os padrões WMM e 802.1p para priorização de trafego;
* Possuir capacidade para operação em modo "repetidor ou mesh", permitindo a comunicação entre pontos de acesso WiFi sem a necessidade de cabeamento adicional permitindo desta forma o atendimento de usuários em locais isolados da localidade;
* Suportar Advanced Power Save (U-APSD);
* Possuir cliente DHCP, para configuração automática do endereço IP;
* Permitir a conexão a rede de usuários em IPv4 e IPv6;
* Gerenciável, no mínimo, através do protocolo SNMP versão 2;
* Possuir a capacidade de criação de no mínimo 15 (quinze) SSIDs em um único radio WI-FI
* Habilitar e desabilitar a divulgação do SSID com agendamento automático;
* O modelo de equipamento proposto deve possuir certificação da Wi-Fi Alliance
* Possuir no mínimo 01 (um) LED indicativo do seu estado de operação;
* O software interno e os arquivos de configuração devem ser armazenados em memória não volátil, permitindo a sua atualização via solução de controladora sem fio em nuvem;
* Permitir o uso do protocolo de autenticação IEEE 802.1X para no miminho EAP-TLS e EAP-TTLS/ EAP-MSCHAPV2 e EAP-SIM
* Compatível com WPA (WiFi Protected Access com algoritmo de criptografia TKIP e Message Integrity Check MIC);
* Implementar WPA3 com AES;
* Compatível com o padrão IEEE 802.11i;
* Permitir a implantação de VLANs segundo o padrão IEEE 802.1Q, permitindo a configuração de no mínimo 8 (oito) VLANs;
* Implementar a técnica de direcionamento de banda, permitindo que clientes com suporte a faixa de frequência de 5 GHz se conectem aos Pontos de Acesso utilizando, preferencialmente, a faixa de 5 GHz;
* Implementar o envio de eventos por meio do protocolo Syslog;
* Implementar controle de limite de uso de banda por SSID e por cliente;
* Detectar, classificar e gerar alarmes de interferências Wi-Fi provenientes de dispositivos padrão IEEE 802.11;
* Realizar o bloqueio da comunicação entre usuários que compartilhem um mesmo SSID, permitindo o isolamento dos usuários;
* Implementar o controle de trafego de broadcast evitando a degradação do serviço devido a propagação deste tipo de trafego;
* Implementar segurança sem fio ativa wIPS 24x7 com radio dedicado (não podendo ser o mesmo radio utilizado para prover serviço aos usuários) para identificar ataques de RF como Denial of Service, Flood Attack, Mapeamento de rede, Spectrum Analisys, entre outros;
* Implementar detecção e contenção de rogue APs e de redes AD-Hoc sem prejuízo aos clientes WiFi IEEE 802.11 conectados no ponto de acesso Wi-Fi;
* Possuir radio BLE integrado e ativado para uso;
* Possuir recurso de ser utilizado como equipamento de Site Survey;
* A plataforma de gerencia na nuvem deve implementar interface de software ("application program interface" ou API) que permita interagir diretamente com a plataforma e com os dispositivos gerenciados pela mesma. A API deve conter um conjunto de ferramentas conhecidas como endpoints para criar software e aplicativos que se comunicam com o painel de gerencia da nuvem, para casos de uso como provisionamento, alterações de configuração em massa, monitoramento e controles de acesso baseados em função. Essa API deve suportar arquitetura RESTful, utilizando protocolo HTTPS para requisições de URLs e JSON.
* A plataforma de gerencia na nuvem deve implementar apresentação de informações de localização dos usuários e dispositivos, utilizando informações coletadas dos pontos de acesso (APs), através da detecção de requisições e frames do protocolo 802.11 (Wifi), e também de informações coletadas via protocolo Bluetooth, incluindo anonimamente informações de dispositivos BLE (Bluetooh Low Energy) como parte de seu conjunto de dados de análise de localização. As informações apresentadas devem incluir capacidade de visualizar onde as pessoas estão gastando tempo dentro de um determinado local ao longo do dia (independentemente de seus dispositivos estarem ou não associados a rede sem fio).
* Implementar análise de espectro de RF nas bandas de 2.4Ghz e 5Ghz para identificação de outros Access Points intrusos e não autorizados (rogues), interferências no canal habilitado do AP e nos demais canais da rede Wi-Fi. A análise de espectro deve ser realizada de forma simultânea ao atendimento dos clientes do AP sem perda de desempenho.
* A console de gerencia na nuvem deve implementar captura de pacotes em tempo real, no equipamento em questão. Além disso, deve ser possível selecionar qual a interface onde será feita a coleta de pacotes, podendo ser a interface ethernet e a interface sem fio (wireless).
* Implementar firewall de camada 7.
 |
| 13 | **MÓDULO DE INTERFACE SFP, 1000BASE-LX, COM GARANTIA DE 36 MESES E INSTALAÇÃO.**Modulo transceivers SFP para fibras ópticas monomodo (SMF) com suporte ao padrão IEEE 802.3z, 1000BaseLX, autosensing de velocidade, conector duplo LC, hot-swappable, operação com comprimento de onda de 1310nm |
| 14 | **PATCH PANEL 24 PORTAS COM GARANTIA DE 36 MESES E INSTALAÇÃO.*** Possuir certificado Listed por laboratório de terceira parte, como UL, ETL ou Delta;
* Projetado para atender os sistemas de cabeamento estruturado, horizontal e secundário, em salas de telecomunicações, com a função de distribuir os serviços de voz, dados e imagens com segurança, baseando-se nas normas estabelecidas para Categoria 6, provendo suporte para aplicações até 250 MHz, Classe E;
* O corpo do produto deve ser fabricado em material metálico, com módulos de conectores em termoplástico de alto impacto termo resistente à chama (UL 94-V0);
* Possuir painel frontal metálico, com identificação das portas serigrafadas no produto;
* Os terminais de conexão devem ser produzidos em bronze fosforoso estanhado, padrão 110 IDC para suportar condutores de 22 a 24 AWG;
* Ser fornecido com guia traseiro metálico com fixação individual para organização dos cabos;
* Ser fornecido com acessórios para fixação (parafusos e arruelas);
* Projetado para instalação em Rack 19", conforme requisitos da norma EIA- 310D;
* Possuir 24 portas, utilizando apenas uma unidade de rack (UA);
* Ilustrar e atender aos padrões de crimpagem T568A e T568B estabelecidos pela NORMA;
* Possuir identificação da marca, categoria do produto e código de rastreabilidade de produção;
* Resistência de Contato: máx. 20m Ohm;
* Resistência DC: máx. 20m Ohm;
* Resistência de Isolamento: min. 500M Ohm;
* Prova de Tensão: 1000V (RMS, 60Hz, 1min);
* O guia traseiro deve fixar os cabos usando fitas do tipo Velcro não sendo permitido o uso de abraçadeiras plásticas que podem danificar o cabo quando mal instaladas.
* O Patch Panel deverá ser fornecido com Guia de Cabos (organizador) com tampa de 1U;
* Todos as portas deverão ser identificadas conforme a norma TIA/EIA-606A.
* **Patch Cord**
* Possuir certificado Listed por laboratório de terceira parte, como UL, ETL ou Delta;
* Possuir certificação Anatel, conforme divulgação pública no site www.anatel.gov.br, para o cordão de manobra (Patch Cord) e cabo de transmissão (Patch Cable).
* Deve ter capa externa em PVC CM e o fabricante deve disponibilizar duas opções de classe de flamabilidade: CM e LSZH. Esta informação deverá estar impressa na capa do cabo;
* Comprimento de 2,5m;
* Possuir disponibilidade de até 7 cores. (Azul, Vermelho, Cinza, Preto, Branco, Amarelo e Verde).
* Fornecido em embalagem individual, preservando as propriedades do produto até o uso efetivo;
* Montado e testado 100% em fábrica;
* Os condutores devem ser fabricados de cobre nu multifilar isolado por polietileno termoplástico de alta densidade. Os condutores (veias) são torcidos e reunidos formando o núcleo de 4 pares.
* Sobre o núcleo deve ser aplicada uma capa de material retardante a chama e nas pontas são aplicados os conectores de 8 vias do tipo RJ45;
* O condutor deve possuir diâmetro nominal de 24 AWG;
* Os conectores devem ser de policarbonato de alto impacto transparente retardante a chama UL94-V0 e logotipo do fabricante gravado no mesmo, com boot injetado e com protetor da trava do plug na mesma cor do patch cord.
* Suportar ciclo de inserção de até 1000 RJ45 e 200 RJ11 conexões;
* Montagem padrão T568A (outras sob consulta);
* Suportar instalação em ambientes internos, não agressivo;
* Suportar carga máxima de tração na instalação de 110N;
* Suportar temperatura de operação de -20°C a +60°C;
* Possuir nome do fabricante, marca do produto e dados de fabricação, impressos na capa do cabo;
* Possuir impedância característica de 100 Ohms;
* Atender às Diretivas RoHS 3 (UE) 2015;
* É necessário apresentar o catálogo correspondente, na apresentação da documentação inicial.
* É necessário a apresentação do certificado Anatel junto a documentação inicial;
* Todos os patches cords deverão ser identificados em ambas as extremidades, conforme a norma TIA/EIA-606A
 |
| 15 | **PATCH PANEL DESCARREGADO COM GARANTIA DE 36 MESES E INSTALAÇÃO.*** Acabamento em pintura epóxi de alta resistência a riscos na cor preta;
* Proteção contra corrosão para as condições especificadas de uso em ambientes internos (ANSI/TIA-569);
* Largura 19", conforme requisitos da norma EIA/ECA-310E;
* Painel de 1U de altura, largura 19”, com 24 posições descarregadas;
* Permite a inserção de ícones coloridos;
* Compatível com conectores CAT.6;
* Permitir escalabilidade no número de portas conforme crescimento da planta;
* Tipo de Pintura Epóxi pó de alta resistência a riscos;
 |
| 16 | **PONTO DE REDE TIPO I COM GARANTIA DE 36 MESES E INSTALAÇÃO.*** **Cabo U/UTP cat 6**
* Possuir certificado Listed por laboratório de terceira parte, como UL, ETL ou Delta;
* Possuir certificação Anatel, conforme divulgação pública no site www.anatel.gov.br;
* Possuir classe de flamabilidade LSZH. Esta informação deverá estar impressa na capa do cabo;
* Ser composto por condutores de cobre nu, possuir 23 AWG de diâmetro nominal isolados em polietileno termoplástico de alta densidade;
* Possuir testes comprobatórios das principais características elétricas em transmissão de altas velocidades, como atenuação, RL, NEXT, PSNEXT, ELFEXT, PSELFEXT, Velocidade de Propagação (Vel.Prop.), Prop. Delay, LCL/TCL, ELTCTL, para frequências da categoria 6 (classe E), com a apresentação dos resultados em catálogo;
* Suportar aplicações de transmissão de dados em alta velocidade, incluindo: Fast Ethernet 100BASE-TX, Gigabit Ethernet 1000BASE-T, 1000BASE-TX, 10GBASE-T, Comunicação de voz e vídeo analógico e Digital, Power Over Ethernet (PoE);
* Ser composto por condutores de cobre nu, possuir 23 AWG de diâmetro nominal isolados em polietileno termoplástico de alta densidade;
* Atender ao padrão de cores Azul/Branco, Laranja/Branco, Verde/Branco, Marrom/Branco, quanto à isolação dos pares;
* Suportar instalação em ambientes internos, não agressivo;
* Possuir diâmetro externo nominal máximo de 6,1mm;
* Suportar carga máxima de tração na instalação de 110N;
* Possuir raio mínimo de curvatura de 24 mm;
* Possuir gravação sequencial métrica decrescente na capa do cabo (305 a 0m);
* Possuir nome do fabricante, marca do produto e dados de fabricação, impressos na capa do cabo;
* Possuir impedância característica de 100 Ohms;
* Suportar temperatura de operação de -20ºC a +60ºC;
* Suportar temperatura de instalação de 0ºC a +50ºC;
* Possuir disponibilidade de até 7 cores. (Azul, Vermelho, Cinza, Preto, Branco, Amarelo e Verde);
* Atender à Diretiva RoHS 3 (UE) 2015/863;
* Todos os enlaces deverão ser identificados conforme a norma TIA/EIA-606A.
* Realizar identificação de cada ponto de rede, e fornecido e instalado todos os acessórios necessários à perfeita execução do serviço.
* **Conector modular RJ45 fêmea -** **cat 6**
* Corpo em termoplástico de alto impacto não propagante a chama (UL 94 V-0);
* Vias de contato produzidas em bronze fosforoso com camadas de 2,54μm de níquel e 1,27μm de ouro;
* Montado em placa de circuito impresso dupla face;
* Terminais de conexão em bronze fosforoso estanhado, padrão 110 IDC;
* Capa traseira e tampa de proteção frontal articulada.
* **Espelho 4x2 com 1 (um) módulo para 1 (uma) tomada RJ45 - cat 6**
* **Linecord (cordão de usuário)**
* Possuir certificado Listed por laboratório de terceira parte, como UL, ETL ou Delta;
* Possuir certificação Anatel, conforme divulgação pública no site www.anatel.gov.br, para o cordão de manobra (Patch Cord) e cabo de transmissão (Patch Cable).
* Possuir capa externa em PVC CM e o fabricante deve disponibilizar duas opções de classe de flamabilidade: CM e LSZH. Esta informação deverá estar impressa na capa do cabo;
* Comprimento de 2,5m;
* Possuir disponibilidade de até 7 cores. (Azul, Vermelho, Cinza, Preto, Branco, Amarelo e Verde).
* Fornecido em embalagem individual, preservando as propriedades do produto até o uso efetivo;
* Montado e testado 100% em fábrica;
* Os condutores devem ser fabricados de cobre nu multifilar isolado por polietileno termoplástico de alta densidade. Os condutores (veias) são torcidos e reunidos formando o núcleo de 4 pares.
* Sobre o núcleo deve ser aplicada uma capa de material retardante a chama e nas pontas são aplicados os conectores de 8 vias do tipo RJ45;
* O condutor deve possuir diâmetro nominal de 24 AWG;
* Os conectores devem ser de policarbonato de alto impacto transparente retardante a chama UL94-V0 e logotipo do fabricante gravado no mesmo, com boot injetado e com protetor da trava do plug na mesma cor do patch cord.
* Suportar ciclo de inserção de até 1000 RJ45 e 200 RJ11 conexões;
* Montagem padrão T568A (outras sob consulta);
* Suportar instalação em ambientes internos, não agressivo;
* Suportar carga máxima de tração na instalação de 110N;
* Suportar temperatura de operação de -20°C a +60°C;
* Possuir nome do fabricante, marca do produto e dados de fabricação, impressos na capa do cabo;
* Possuir impedância característica de 100 Ohms;
* Atender às Diretivas RoHS 3 (UE) 2015;
* É necessário apresentar o catálogo correspondente, na apresentação da documentação inicial.
* É necessário a apresentação do certificado Anatel junto a documentação inicial;
* Todos os Line Cords deverão ser identificados em ambas as extremidades, conforme a norma TIA/EIA-606A.
* **Certificação**
* Após o término da instalação da infraestrutura de cabeamento de rede, deverá ser executada a certificação da rede, por meio de uso de equipamento adequado aos testes de *link* e canal para todos os pontos.
* Apresentar a impressão da certificação e dos relatórios emitidos pelo equipamento de todos os enlaces metálicos, em meio magnético e impressos originais;
* A rede estruturada só será considerada como certificada após a aprovação em todos os testes;
* Considerar para a fase de testes de certificação a utilização dos mais modernos equipamentos de testes.
* O equipamento de teste deverá obrigatoriamente operar com a última versão do sistema operacional do fabricante para aquele modelo/versão, devendo possuir calibração vistoriada e comprovada com data inferior a 1 ano

A licitante deverá apresentar o catálogo correspondente ao produto quando do encaminhamento da documentação técnica. |
| 17 | **PONTO DE REDE TIPO II COM GARANTIA DE 36 MESES E INSTALAÇÃO.*** **Cabo U/UTP cat 6**
* Possuir certificado Listed por laboratório de terceira parte, como UL, ETL ou Delta;
* Possuir certificação Anatel, conforme divulgação pública no site www.anatel.gov.br;
* Possuir classe de flamabilidade LSZH. Esta informação deverá estar impressa na capa do cabo;
* Ser composto por condutores de cobre nu, possuir 23 AWG de diâmetro nominal isolados em polietileno termoplástico de alta densidade;
* Possuir testes comprobatórios das principais características elétricas em transmissão de altas velocidades, como atenuação, RL, NEXT, PSNEXT, ELFEXT, PSELFEXT, Velocidade de Propagação (Vel.Prop.), Prop. Delay, LCL/TCL, ELTCTL, para frequências da categoria 6 (classe E), com a apresentação dos resultados em catálogo;
* Suportar aplicações de transmissão de dados em alta velocidade, incluindo: Fast Ethernet 100BASE-TX, Gigabit Ethernet 1000BASE-T, 1000BASE-TX, 10GBASE-T, Comunicação de voz e vídeo analógico e Digital, Power Over Ethernet (PoE);
* Ser composto por condutores de cobre nu, possuir 23 AWG de diâmetro nominal isolados em polietileno termoplástico de alta densidade;
* Atender ao padrão de cores Azul/Branco, Laranja/Branco, Verde/Branco, Marrom/Branco, quanto à isolação dos pares;
* Suportar instalação em ambientes internos, não agressivo;
* Possuir diâmetro externo nominal máximo de 6,1mm;
* Suportar carga máxima de tração na instalação de 110N;
* Possuir raio mínimo de curvatura de 24 mm;
* Possuir gravação sequencial métrica decrescente na capa do cabo (305 a 0m);
* Possuir nome do fabricante, marca do produto e dados de fabricação, impressos na capa do cabo;
* Possuir impedância característica de 100 Ohms;
* Suportar temperatura de operação de -20ºC a +60ºC;
* Suportar temperatura de instalação de 0ºC a +50ºC;
* Possuir disponibilidade de até 7 cores. (Azul, Vermelho, Cinza, Preto, Branco, Amarelo e Verde);
* Atender à Diretiva RoHS 3 (UE) 2015/863;
* Todos os enlaces deverão ser identificados conforme a norma TIA/EIA-606A.
* Realizar identificação de cada ponto de rede, e fornecido e instalado todos os acessórios necessários à perfeita execução do serviço.
* **Conector modular RJ45 fêmea - cat 6**
* Corpo em termoplástico de alto impacto não propagante a chama (UL 94 V-0);
* Vias de contato produzidas em bronze fosforoso com camadas de 2,54μm de níquel e 1,27μm de ouro;
* Montado em placa de circuito impresso dupla face;
* Terminais de conexão em bronze fosforoso estanhado, padrão 110 IDC;
* Capa traseira e tampa de proteção frontal articulada.
* **Espelho 4x2 com 2 módulos para 2 tomadas RJ45 – cat6**
* **Linecord (cordão de usuário)**
* Possuir certificado Listed por laboratório de terceira parte, como UL, ETL ou Delta;
* Possuir certificação Anatel, conforme divulgação pública no site www.anatel.gov.br, para o cordão de manobra (Patch Cord) e cabo de transmissão (Patch Cable).
* Possuir capa externa em PVC CM e o fabricante deve disponibilizar duas opções de classe de flamabilidade: CM e LSZH. Esta informação deverá estar impressa na capa do cabo;
* Comprimento de 2,5m;
* Possuir disponibilidade de até 7 cores. (Azul, Vermelho, Cinza, Preto, Branco, Amarelo e Verde).
* Fornecido em embalagem individual, preservando as propriedades do produto até o uso efetivo;
* Montado e testado 100% em fábrica;
* Os condutores devem ser fabricados de cobre nu multifilar isolado por polietileno termoplástico de alta densidade. Os condutores (veias) são torcidos e reunidos formando o núcleo de 4 pares.
* Sobre o núcleo deve ser aplicada uma capa de material retardante a chama e nas pontas são aplicados os conectores de 8 vias do tipo RJ45;
* O condutor deve possuir diâmetro nominal de 24 AWG;
* Os conectores devem ser de policarbonato de alto impacto transparente retardante a chama UL94-V0 e logotipo do fabricante gravado no mesmo, com boot injetado e com protetor da trava do plug na mesma cor do patch cord.
* Suportar ciclo de inserção de até 1000 RJ45 e 200 RJ11 conexões;
* Montagem padrão T568A (outras sob consulta);
* Suportar instalação em ambientes internos, não agressivo;
* Suportar carga máxima de tração na instalação de 110N;
* Suportar temperatura de operação de -20°C a +60°C;
* Possuir nome do fabricante, marca do produto e dados de fabricação, impressos na capa do cabo;
* Possuir impedância característica de 100 Ohms;
* Atender à Diretiva RoHS;
* É necessário apresentar o catálogo correspondente, na apresentação da documentação inicial.
* É necessário a apresentação do certificado Anatel junto a documentação inicial;
* Todos os Line Cords deverão ser identificados em ambas as extremidades, conforme a norma TIA/EIA-606A.
* **Certificação**
* Após o término da instalação da infraestrutura de cabeamento de rede, deverá ser executada a certificação da rede, por meio de uso de equipamento adequado aos testes de *link* e canal para todos os pontos.
* Apresentar a impressão da certificação e dos relatórios emitidos pelo equipamento de todos os enlaces metálicos, em meio magnético e impressos originais;
* A rede estruturada só será considerada como certificada após a aprovação em todos os testes;
* Considerar para a fase de testes de certificação a utilização dos mais modernos equipamentos de testes.
* O equipamento de teste deverá obrigatoriamente operar com a última versão do sistema operacional do fabricante para aquele modelo/versão, devendo possuir calibração vistoriada e comprovada com data inferior a 1 ano
* A licitante deverá apresentar o catálogo correspondente ao produto quando do encaminhamento da documentação técnica.
 |
| 18 | **PONTO DE REDE TIPO III COM GARANTIA DE 36 MESES E INSTALAÇÃO.*** Cabo U/UTP cat 6
* Possuir certificado Listed por laboratório de terceira parte, como UL, ETL ou Delta;
* Possuir certificação Anatel, conforme divulgação pública no site www.anatel.gov.br;
* Possuir classe de flamabilidade LSZH. Esta informação deverá estar impressa na capa do cabo;
* Ser composto por condutores de cobre nu, possuir 23 AWG de diâmetro nominal isolados em polietileno termoplástico de alta densidade;
* Possuir testes comprobatórios das principais características elétricas em transmissão de altas velocidades, como atenuação, RL, NEXT, PSNEXT, ELFEXT, PSELFEXT, Velocidade de Propagação (Vel.Prop.), Prop. Delay, LCL/TCL, ELTCTL, para frequências da categoria 6 (classe E), com a apresentação dos resultados em catálogo;
* Suportar aplicações de transmissão de dados em alta velocidade, incluindo: Fast Ethernet 100BASE-TX, Gigabit Ethernet 1000BASE-T, 1000BASE-TX, 10GBASE-T, , Comunicação de voz e vídeo analógico e Digital, Power Over Ethernet (PoE);
* Ser composto por condutores de cobre nu, possuir 23 AWG de diâmetro nominal isolados em polietileno termoplástico de alta densidade;
* Atender ao padrão de cores Azul/Branco, Laranja/Branco, Verde/Branco, Marrom/Branco, quanto à isolação dos pares;
* Suportar instalação em ambientes internos, não agressivo;
* Possuir diâmetro externo nominal máximo de 6,1mm;
* Suportar carga máxima de tração na instalação de 110N;
* Possuir raio mínimo de curvatura de 24 mm;
* Possuir gravação sequencial métrica decrescente na capa do cabo (305 a 0m);
* Possuir nome do fabricante, marca do produto e dados de fabricação, impressos na capa do cabo;
* Possuir impedância característica de 100 Ohms;
* Suportar temperatura de operação de -20ºC a +60ºC;
* Suportar temperatura de instalação de 0ºC a +50ºC;
* Possuir disponibilidade de até 7 cores. (Azul, Vermelho, Cinza, Preto, Branco, Amarelo e Verde);
* Atender à Diretiva RoHS 3 (UE) 2015/863;
* Todos os enlaces deverão ser identificados conforme a norma TIA/EIA-606A.
* Realizar identificação de cada ponto de rede, e fornecido e instalado todos os acessórios necessários à perfeita execução do serviço.
* **Conector modular RJ45 fêmea - cat 6**
* Corpo em termoplástico de alto impacto não propagante a chama (UL 94 V-0);
* Vias de contato produzidas em bronze fosforoso com camadas de 2,54μm de níquel e 1,27μm de ouro;
* Montado em placa de circuito impresso dupla face;
* Terminais de conexão em bronze fosforoso estanhado, padrão 110 IDC;
* Capa traseira e tampa de proteção frontal articulada.
* **Espelho 4x2 com 2 (dois) módulos para duas (duas) tomada RJ45 - cat 6**
* **Linecord (cordão de usuário)**
* Possuir certificado Listed por laboratório de terceira parte, como UL, ETL ou Delta;
* Possuir certificação Anatel, conforme divulgação pública no site www.anatel.gov.br, para o cordão de manobra (Patch Cord) e cabo de transmissão (Patch Cable).
* Possuir capa externa em PVC CM e o fabricante deve disponibilizar duas opções de classe de flamabilidade: CM e LSZH. Esta informação deverá estar impressa na capa do cabo;
* Comprimento de 2,5m;
* Possuir disponibilidade de até 7 cores. (Azul, Vermelho, Cinza, Preto, Branco, Amarelo e Verde).
* Fornecido em embalagem individual, preservando as propriedades do produto até o uso efetivo;
* Montado e testado 100% em fábrica;
* Os condutores devem ser fabricados de cobre nu multifilar isolado por polietileno termoplástico de alta densidade. Os condutores (veias) são torcidos e reunidos formando o núcleo de 4 pares.
* Sobre o núcleo deve ser aplicada uma capa de material retardante a chama e nas pontas são aplicados os conectores de 8 vias do tipo RJ45;
* O condutor deve possuir diâmetro nominal de 24 AWG;
* Os conectores devem ser de policarbonato de alto impacto transparente retardante a chama UL94-V0 e logotipo do fabricante gravado no mesmo, com boot injetado e com protetor da trava do plug na mesma cor do patch cord.
* Suportar ciclo de inserção de até 1000 RJ45 e 200 RJ11 conexões;
* Montagem padrão T568A (outras sob consulta);
* Suportar instalação em ambientes internos, não agressivo;
* Suportar carga máxima de tração na instalação de 110N;
* Suportar temperatura de operação de -20°C a +60°C;
* Possuir nome do fabricante, marca do produto e dados de fabricação, impressos na capa do cabo;
* Possuir impedância característica de 100 Ohms;
* Atender à Diretiva RoHS;
* É necessário apresentar o catálogo correspondente, na apresentação da documentação inicial.
* É necessário a apresentação do certificado Anatel junto a documentação inicial;
* Todos os Line Cords deverão ser identificados em ambas as extremidades, conforme a norma TIA/EIA-606A.
* **Certificação**
* Após o término da instalação da infraestrutura de cabeamento de rede, deverá ser executada a certificação da rede, por meio de uso de equipamento adequado aos testes de link e canal para todos os pontos.
* Apresentar a impressão da certificação e dos relatórios emitidos pelo equipamento de todos os enlaces metálicos, em meio magnético e impressos originais;
* A rede estruturada só será considerada como certificada após a aprovação em todos os testes;
* Deverá considerar para a fase de testes de certificação a utilização dos mais modernos equipamentos de testes.
* O equipamento de teste deverá obrigatoriamente operar com a última versão do sistema operacional do fabricante para aquele modelo/versão, devendo possuir calibração vistoriada e comprovada com data inferior a 1 ano.
* **Conduto flexível**
* Infraestrutura em duto flexível de pvc de 1"e 2, com todos os acessórios de montagem;
* **Canaletas**
* Canaletas de pvc de 50x20 mm e 110x20 mm, com todos os acessórios de montagem, no interior das salas;
* **Eletrocalhas**
* Eletrocalhas perfuradas de chapa metálica de 100x50x3000 mm, com todos os acessórios de montagem;

A licitante deverá apresentar o catálogo correspondente ao produto quando do encaminhamento da documentação técnica. |
| 19 | **RACK DE 19" FECHADO DE 12U COM GARANTIA DE 36 MESES E INSTALAÇÃO*** Rack de 19", 12 UA, fixação em parede, estrutura em aço carbono SAE 1010 com espessura de 1,2 mm, pintura eletrostática na cor preta RAL 9011, com fechamentos laterais e traseiros removíveis com aletas de ventilação e fecho rápido tipo fenda, porta frontal com fechadura cilíndrica / 02 (duas) chaves e visor de acrílico fumê, profundidade não inferior a 570 mm, com entrada e saída de cabos pela sua base e acompanhado dos seguintes acessórios: 01 (uma) régua com 4 tomadas elétricas cada de 1 UA; sistema de ventilação de teto composto de 02 (dois) ventiladores; e conjunto porca gaiola e parafuso M5 em todas as posições "U.
 |
| 20 | **RACK DE PISO DE 19" FECHADO DE 42U COM GARANTIA DE 36 MESES E INSTALAÇÃO*** Ser confeccionado em aço carbono SAE 1010, 1,9mm;
* Possuir furação quádrupla para sistema ventilação, incluído;
* Possuir tampa lateral perfuradas, facilmente removível através de fecho cilíndrico tipo Yale com aleta de ventilação;
* Porta traseira em chapa de aço perfurada bipartida;
* Teto com ventiladores;
* *Top cable* superior para acomodação de cabos metálicos e fibras ópticas óticas;
* Passa cabos laterais, com alça de fixação e porta para melhor acesso aos cabos;
* Capacidade de carga de 20kg / *finger*;
* Organizadores laterais, com alça de fixação e porta para melhor acesso aos cabos;
* Organizadores laterais com *fingers* plásticos.
* Possuir porta frontal de vidro temperado fumê;
* Possuir plano de fixação frontal e traseiro em aço padrão 19” perfurado;
* Ser fornecido com um plano de fixação com furação a cada 1/2U;
* Fechamento da porta feito através de fechos tipo Yale escamoteáveis;
* Porta frontal reversível, com dobradiças de articulação interna que possibilitam uma abertura de 180°;
* Fornecido com pés niveladores para alinhamento no piso;
* Possuir carga estática máxima de 500Kg;
* Ter grau de proteção IP 20 quando utilizado furação colmeia ou IP30 quando não;
* Confeccionado em pintura epóxi-pó texturizada na cor preta;
* Largura de 800mm e profundidade de 670mm;
* Fornecido com duas réguas de tomadas com 6 tomadas 10A;
* Fornecido com duas réguas de tomadas com 8 tomadas 20A;
* Fornecido com todos os demais acessórios necessários.
 |
| 21 | **RACK DE PISO DE 19" FECHADO DE 44U COM GARANTIA 36 MESE E INSTALAÇÃO*** Ser confeccionado em aço carbono SAE 1010, 1,9mm;
* Possuir furação quádrupla para sistema ventilação, incluído;
* Possuir tampa lateral perfuradas, facilmente removível através de fecho cilíndrico tipo Yale com aleta de ventilação;
* Porta traseira em chapa de aço perfurada bipartida;
* Teto com ventiladores;
* *Top cable* superior para acomodação de cabos metálicos e fibras ópticas óticas;
* Passa cabos laterais, com alça de fixação e porta para melhor acesso aos cabos;
* Capacidade de carga de 20kg / *finger*;
* Organizadores laterais, com alça de fixação e porta para melhor acesso aos cabos;
* Organizadores laterais com *fingers* plásticos.
* Possuir porta frontal de vidro temperado fumê;
* Possuir plano de fixação frontal e traseiro em aço padrão 19” perfurado;
* Ser fornecido com um plano de fixação com furação a cada 1/2U;
* Fechamento da porta feito através de fechos tipo Yale escamoteáveis;
* Porta frontal reversível, com dobradiças de articulação interna que possibilitam uma abertura de 180°;
* Fornecido com pés niveladores para alinhamento no piso;
* Possuir carga estática máxima de 500Kg;
* Ter grau de proteção IP 20 quando utilizado furação colmeia ou IP30 quando não;
* Confeccionado em pintura epóxi-pó texturizada na cor preta;
* Largura de 800mm e profundidade de 1000mm;
* Fornecido com duas réguas de tomadas com 6 tomadas 10A;
* Fornecido com duas réguas de tomadas com 8 tomadas 20A;

Fornecido com todos os demais acessórios necessários. |
| 22 | **SENSOR IP DE TEMPERATURA E UMIDADE DO AR COM INTERFACE ETHERNET COM LICENÇA DE SOFTWARE PARA PLATAFORMA DE GERENCIAMENTO EM NUVEM POR PERÍODO DE 60 MESES E INSTALAÇÃO.*** Detectar a presença de produtos químicos, detritos, temperaturas extremas, umidade e ruído. Caso a qualidade do ar diminua, o sensor deve ser capaz de notificar imediatamente via e-mail, SMS, notificação por push ou webhook;
* Gerenciamento em nuvem, centralizado;
* Temperatura Faixa: 0°C a +55°C / +32°F a +131°F;
* Umidade Faixa: 0 a 95% UR;
* Recursos sem fio, Bluetooth;
* Frequência de operação 2,400–2,4835 GHz;
* Padrão IEEE 802.15.1 (Bluetooth Low Energy 4.2);
* Amostragem de dados - Temperatura: a cada dois minutos, Umidade: a cada dois minutos, PM 2.5: a cada cinco minutos, TVOC: a cada 90 segundos, Ruído ambiente: a cada 5 minutos;
* Relatório de dados para o gateway: a cada 20 minutos ou imediatamente após a violação do limite;
* Armazenamento de dados *on board*: até cinco dias de armazenamento de dados.
 |
| 23 | **SERVIDOR DE COMUNICAÇÃO UNIFICADA IP COM GARANTIA DE 60 MESES.*** **RECURSOS DE VOZ**
* A solução deverá ser entregue em forma de appliance físico.
* O appliance deverá ser instalado em rack de 19” e vir com todos os acessórios necessários para esta instalação.
* A solução deve ser composta por um conjunto de aplicações de comunicação unificada que implementem as seguintes funções:
	+ Controle e Processamento de chamadas;
	+ Mensageria Instantânea e Presença;
	+ Correio de Voz;
	+ Gateway de Voz.
* A solução deve ter seu hardware e software dimensionados para atender, no mínimo, 1000 usuários.
* A solução deve ser dimensionada de modo a suportar, no mínimo, 500 sessões simultâneas de música em espera e até 50 fontes de música em espera.
* **FUNCIONALIDADES DA SOLUÇÃO E CONTROLE DE CHAMADAS**
* A aplicação de Controle e Processamento de Chamadas deve suportar e implementar, no mínimo, as seguintes funcionalidades:
* Em caso de falha de um dos processadores de chamadas, chamadas em andamento continuem conectadas, de modo que a falha deste componente seja transparente para o usuário;
* Provisionar a configuração de telefones e softphones IP de modo automático;
* Efetuar a sinalização de controle para o estabelecimento e desconexão de chamadas;
* Efetuar a sinalização e interface com os gateways para integração da Rede de Telefonia Pública com o ambiente de telefonia IP.
* Manipulação de dígitos e tratamento de chamadas – inserção, remoção ou substituição de string de dígitos e códigos de acesso a discagem, tradução de string de dígitos e transformação de padrão de discagem.
* Possibilitar a criação de categorias distintas a serem aplicadas a cada usuário, permitindo restringir acesso a chamadas de emergência, internas, locais, DDD ou DDI conforme o perfil de cada usuário.
* Implementar mecanismos que restrinjam a transferência de chamadas externas para um dispositivo externo.
* Implementar IPv4 e IPv6, inclusive dual stack.
* Possuir capacidade de em conjunto com os terminais, utilizar a opção 150 do protocolo DHCP para identificar o TFTP server de onde a configuração de cada terminal está disponível. Caso não exista servidor DHCP disponível, deverá permitir a configuração manual dos terminais.
* Implementar serviço TFTP que deve disponibilizar para os terminais os seguintes arquivos:
	+ Firmware – permitindo atualização de firmware automática e remota;
	+ Configuração
	+ Certificados
	+ Definições de Softkeys
	+ Plano de Discagem
* Implementar os CODECs G.711 a-law e u-law, G.722, G.722.1, G.723.1 e G.729 e iLBC.
* Permitir a atribuição automática de CODECs individualmente, por chamada estabelecida.
* Permitir a seleção automática de aúdio de alto consumo de banda para chamadas entre dispositivos em um mesmo site enquanto selecionando aúdio de baixo consumo de banda para chamadas entre dispositivos em sites diferentes.
* Ser compatível com os protocolos H.323, MGCP, SIP (line-side) e tronco SIP.
* A implementação de SIP deve ser compatível com as seguintes RFCs:
* SIP Line Side: 3261, 3262, 3264, 3265, 3311,3515 e 3842.
* SIP Trunk Side: 2833, 2976, 3261, 3262, 3264, 3265, 3311, 3323, 3325, 3515, 3842, 3856 e 3891.
* Implementar QoS de acordo com o padrão 802.1p.
* Suportar VLANs de acordo com o padrão 802.1q.
* Permitir a criação e o gerenciamento do plano de discagem de forma centralizada.
* Disponibilizar ferramenta que análise o plano de discagem para número específicos, permitindo testar e verificar o correto funcionamento do plano de discagem.
* Implantar CDR – Call Detail Records.
* Disponibilizar ferramenta de relatórios baseados nos CDRs, incluindo relatórios de chamadas por usuários, chamadas através de gateways e qualidade das chamadas.
* Disponibilizar mecanismo de pesquisa de CDR.
* Permitir administração básica do banco de dados de CDR.
* Permitir a deleção de registros de acordo com o tamanho do banco de dados.
* Disponibilizar ferramenta de administração em massa, permitindo que os administradores realizem a inserção, a atualização ou a deleção de usuários e dispositivos em grandes blocos.
* Suportar SNMP para geração e envio de traps para sistemas de monitoração remotos.
* Implementar seleção automática de rota, de modo que em caso de indisponibilidade do link ou de insuficiência de recursos (banda) para realização da chamada por meio da rede WAN ou perda de comunicação com os appliances, a chamada deve ser automaticamente roteada para a rede de telefonia pública.
* Possibilitar a implementação de recursos de sobrevivência garantindo que telefones IP, localizados em redes remotas, continuem sua operação em caso de falha do circuito de WAN ou em caso de falhas dos servidores de telefonia.
* Permitir o compartilhamento dos recursos de mídia – transcodificadores, recursos para música em espera, MTPs (Media Termination Poin) e bridges de conferência - através do gerenciamento centralizado de tais recursos.
* Implantar Media termination point (MTP) em troncos SIP e em compliance com a RFC 2833
* Permitir a criação e o gerenciamento de audioconferências a partir dos terminais.
* Permitir a criação de no mínimo 5 audioconferências de 8 participantes em G.711.
* Permitir a criação de 1000 regiões administrativas para processamento de chamadas.
* Implementar mecanismos de Call Admission Control (CAC) entre as regiões administrativas, de modo a garantir que o QoS de voz seja mantido ao posicionar novas chamadas sobre a Rede Pública de Telefonia, de modo automático, quando não houver banda disponível nos links WAN.
* Implementar Hot Line e PLAR (Private Line Automated Ringdown).
* Suportar DNIS (Dialed Number Identification Service)
* Função Chefe-Secretária.
* Implementar Supressão de Silêncio e Voice Activity Detection (VAD).
* Implementar indicação de mensagem em espera (MWI).
* Possuir suporte a Fax sobre IP por meio de técnicas de Pass-through e Fax-Relay.
* Implementar DTMF in band de acordo com a RFC 2833 (RTP-NTE).
* Implementar DTMF out of band: KPML (RFC 4730); SIP Notify (RFC 3265); e SIP Info (RFC 2976).
* Atender aos padrões TAPI, JTAPI e WML ou XML.
* A solução deve permitir a criação de serviços por meio de linguagem XML ou WML de modo que os terminais tenham acesso a aplicações na intranet e na internet.
* Permitir a diferenciação de toques para chamadas internas e externas.
* Implementar funcionalidades de cobertura de chamadas, incluindo encaminhamento de chamada diferenciado baseada no número chamado ser interno ou externo, encaminhamento para um caminho de cobertura e roteamento baseado na hora do dia.
* Implementar grupos de captura: broadcast; circular; maior tempo em idle; e linear.
* Implementar códigos de autorização de acesso (Forced authorization code).
* Toda a interface para usuários deverá ser implementada na língua portuguesa.
* Permitir autenticação de dispositivos através de certificados X.509v3.
* 1.2.60. Permitir autenticação nos trunks SIP utilizando troca de certificados IPSec ou preshared key.
* Disponibilizar mecanismo para a instalação automática de certificados de significância local (LSC) para os dispositivos.
* Implementar criptografia de mídia utilizando SRTP.
* Implementar criptografia de sinalização utilizando TLS.
* Implementar HTTPS para todas as ferramentas e serviços baseados em web.
* Implementar SSL para diretórios.
* Implementar arquivos TFTP com certificados self-signed do TFTP Server.
* Implementar as seguintes funcionalidades para os usuários:
* Discagem abreviada.
* Atendimento automático e intercom.
* Chamada de retorno se o destino estiver ocupado ou se a chamada original não foi respondida.
* Cobertura de chamada
* Encaminhamento de chamadas: todas (on net e off net); se ocupado; se não responder; se não houver banda; e se não o dispositivo de destino não estiver registrado.
* Estacionamento e recuperação de chamada.
* Captura de chamada;
* Captura de chamada de grupo;
* Notificação de Captura de Chamada.
* Status de Chamada por linha: estado; duração e número.
* Chamada em Espera com alerta sonoro configurável.
* Identificação do Chamador.
* Encadeamento de Conferências.
* Visualização de Número Discado.
* Direct Inward dialing (DID) e direct outward dialing (DOD)
* Discagem por diretório a partir do telefone: pessoal e corporativo.
* Desvio de Chamadas
* Mobilidade de ramal por usuário.
* Mudança de PIN de mobilidade de usuário a partir do telefone.
* Indicação visual de mensagem em espera (caixa postal)
* Toque diferenciado para chamadas internas e externas.
* Não perturbe.
* Encaminhamento imediato a caixa postal.
* Rediscagem do último número (interno e externo)
* Login e logout de grupos de busca.
* Conferências: ad-hoc e meet me
* Múltiplas chamadas por linha.
* Música em Espera
* Transferência: cega e com consulta.
* Configuração de discagem rápida e encaminhamento de chamadas pelo usuário via portal web.
* **MENSAGERIA INSTANTÂNEA E PRESENÇA**
* A solução de Mensageria Instantânea e presença deve suportar e implementar, no mínimo, as seguintes funcionalidades:
* Permitir a coleta de informações do usuário, como atividade, disponibilidade e métodos de comunicação, para que sejam refletidos como “status” nas aplicações de comunicação IP (voz, mensageria instantânea, vídeo e colaboração)
* Implementar nativamente os padrões Extensible Messaging and Presence Protocol (XMPP), SIP e SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE).
* A solução deverá ser dimensionada de forma a suportar até 1.000 usuários.
* Refletir, no mínimo, os seguintes estados básicos para um determinado usuário:
* Disponível – quando o usuário está disponível para ser contatado;
* Ocupado – quando existe alguma atividade no calendário do usuário;
* Ao telefone – quando o usuário está utilizando o ramal que lhe foi assignado;
* Inativo – quando o usuário não tenha usado seus dispositivos de comunicação por um período de tempo pré-determinado.
* Através dos protocolos SIP e SIMPLE, o “status” de presença deverá poder ser, publicado e notificado aos diversos clientes de comunicação IP compatíveis.
* Interfaces de programação de aplicação (APIs) Simple Object Access Protocol (SOAP), Representational State Transfer (REST) e Bidirectional Streams over Synchronous HTTP (BOSH) para integração com aplicações baseadas em web.
* Integrar com soluções de calendário, de tal forma que a disponibilidade do usuário seja refletida automaticamente em seu “status” mesmo que o usuário não esteja logado no sistema.
* Permitir a troca de informação de presença entre diferentes organizações que estejam utilizando a mesma solução de presença e mensageria instantânea.
* Utilizar certificados digitais e TLS para a troca segura de informações.
* Ser administrado através de uma interface gráfica web segura, utilizando o protocolo HTTPS.
* Compatibilidade os seguintes padrões:
* RFC3261 – SIP: Session Initiation Protocol
* RFC3265 – SIP – Specific Event Notification
* RFC3428 – SIP Extension for Instant Message
* RFC3856 – A Presence Event Package for SIP
* RFC3863 – Presence Information Data Format (PIDF)
* RFC3903 – SIP Extension for Event State Publication
* RFC4479 – A Data Model for Presence
* RFC4480 – RPID: Rich Presence: Extensions to the Presence Information Data Format (PIDF)
* Draft-ietf- simple-prescaps-ext-03 – User Agent Capability Extension to Presence Information Data Format (PIDF)
* RFC4662 – A SIP Event Notification Extension for Resource Lists
* Draft-ietf-sip-subnot-etags-02 – An Extention to SIP Events for Conditional Event Notification
* **CORREIO DE VOZ**
* A solução de Correio de Voz deve suportar e implementar, no mínimo, as seguintes funcionalidades:
* Permitir redundância ativa 1+1 do appliance virtual, somando-se as capacidades individuais de portas de conexão com sistema de sinalização e controle durante situação normal;
* Atender a uma chamada direcionada pelo sistema de sinalização e controle e direcioná-la automaticamente para a caixa postal do usuário de destino valendo-se do número discado;
* Permitir através do telefone do usuário reproduzir e processar mensagens (repetir, responder, encaminhar, deletar, salvar, marcar como não lida, ouvir o registro de data e hora e pular para a próxima mensagem);
* Permitir ao usuário, durante a execução de uma chamada, pausar, voltar e avançar a reprodução de uma mensagem;
* Permitir controlar o volume e velocidade da reprodução da mensagem;
* Permitir a gravação de uma mensagem para ser endereçada à vários destinatários ou lista de distribuição;
* Permitir ao usuário fazer busca por mensagens utilizando-se de referência campos como call-id, nome ou ramal nas mensagens salvas;
* Ao gravar uma mensagem de voz ao usuário será permitido marcar a mensagem como comum, urgente, privada ou segura;
* Ao gravar uma mensagem de voz deverá ser permitido ao usuário solicitar confirmação da entrega da mensagem;
* Permitir gravar uma chamada em andamento e enviar o arquivo de gravação para a caixa;
* Permitir ao usuário visualizar no display do seu telefone IP uma lista com todas as mensagens de voz armazenadas em sua caixa postal. O usuário poderá selecionar quais das mensagens ele irá reproduzir, baseando-se em campos como remetente, data e número chamador;
* Auto-atendendor com no mínimo 3 sub-níveis de árvore de atendimento;
* Implementar regras de roteamento de chamadas entrantes a partir do número chamador;
* Implementar regras de roteamento de chamadas entrandes a partir do dia da semana;
* Permitir regras de roteamento de chamadas entrantes a partir da disponibilidade no aplicativo de correio eletrônico Microsoft Exchange;
* Oferecer ao usuário acesso à sua caixa de voz através de página web, autenticando-se utilizando as mesmas credenciais disponíveis no diretório corporativo;
* Permitir ao usuário customizar saudações de atendimento para chamadas internas, externas, ocupado, fora do horário e férias;
* Permitir ao usuário a criação de listas de distribuição e endereçar mensagens de voz a estas listas através da interface de telefone (TUI – Telephony User Interface) ou da interface gráfica (GUI - Graphical User Interface);
* Notificação de novas mensagens para os usuários através de SMTP, SMS e telefones a serem discados;
* Busca por mensagens atavés de aplicativos de leitura RSS;
* Reproduzir, compor, responder e encaminhar mensagens através de aplicativos de correio eletrônico através de IMAP;
* Enviar mensagens de voz para o mesmo inbox do usuário no Microsoft Exchange;
* Implementar regras de níveis de acesso e restrição de usuários ou grupos de usuários para os quais uma chamada não poderá ser encaminhada;
* Integrar com servidores de fax externos utilizando protocolos padrões de mercado;
* Permitir se configurar o período máximo que uma mensagem poderá ficar armazenada na caixa de um usuário. O usuário deverá receber notificação da proximidade do expiro deste período;
* Conectar-se ao sistema de sinalização e controle através de protocolo SIP, sem a adição de hardware externo ou conversores de protocolo;
* Sincronizar informações de usuário, incluindo credenciais, através de protocolo LDAP com o Diretório Corporativo;
* Permitir que os clusters de servidores estejam geograficamente dispersos em Data Centers distintos;
* Ser compatível com protocolo VPIM para o estabelecimento de networking com outros sistemas de correio de voz;
* Administração através de interface Web bem como possuir interface de linha de comando para suporte 3º nível;
* Plano de numeração baseado no formato E.164;
* Classes de Serviços de usuários para a definição das funcionalidades disponíveis para um usuário ou grupos de usuários;
* Permitir a criação de usuários em lote;
* Permitir a importação dos usuários configurados no sistema de sinalização e controle;
* Utilizar sRTP e TLS na integração SIP com o sistema de sinalização e controle;
* SNMP versões 1, 2 e 3;
* Permitir a configuração de lista de feriados;
* Message Waiting Indication – MWI nos telefones que também tiverem suporte a esta funcionalidade para a notificação de novas mensagens de voz;
* Alerta sonoro de novas mensagens para os telefones que não suportarem MWI;
* Permitir a configuração de diferentes níveis administrativos;
* Permitir a auto-configuração de um novo usuário onde este possa gravar o seu nome e configurar a sua nova senha;
* Possuir relatórios administrativos informando o status de ocupação das portas de voz do servidor;
* Permitir o broadcast de mensagens;
* Permitir a customização das saudações da solução;
* Permitir o ajuste automático às mudanças de horário de verão;
* Possuir logging e relatórios de logins sem sucesso;
* Permitir configurar mensagens como privadas, evitando que as mesmas sejam encaminhadas para fora da empresa;
* Implementar os codecs G.711, G.729, G.722 e iLBC;
* Possuir ferramenta de transcoding interno, sem necessidade de hardware adicional;
* Possuir relatórios administrativos com informações sobre: Usuários, ocupação de portas, configuração de sistema, capacidade de storage do mailstore, plano de numeração;

**LICENCIAMENTO*** O Licenciamento do sistema ofertado deverá ser conforme o modelo de Subscrição.
* O licenciamento deverá ser pelo período de 60 meses.
* O licenciamento deverá suportar, no mínimo, 1000 dispositivos registrados na Central Telefônica.
 |
| 24 | Instalação do item 23 |
| 25 | **SERVIDOR DE HIPERCONVERGÊNCIA COM GARANTIA DE 60 MESES.*** Serão aceitos *appliances* ou nós certificados, desde que garantida a compatibilidade com a ferramenta de gestão e atualização dos firmwares e softwares relacionados à infraestrutura hiperconvergente (virtualização e armazenamento definidos por software) de maneira centralizada, automatizada e orquestrada. Todos os componentes de hardware deverão ser totalmente compatíveis com os softwares especificados neste termo de referência.
* Deverá ser ofertado com pelo menos dois processadores, cada processador com pelo menos 16 (dezesseis) núcleos (cores) operando a uma frequência mínima de 2.5GHz, devendo ser da geração mais recente ofertada pelo fabricante do equipamento. Caso o requisito mínimo para atender ao SDS seja superior, deverão ser considerados os núcleos adicionais na proposta.
* Deverá ser ofertado com pelo menos 8 (oito) módulos de memória idênticos com capacidade individual mínima de 64GB (sessenta e quatro gigabyte) do tipo DDR5 com velocidade mínima de 4600 MT/s.
* Suportar expansão de até 8 TB (oito terabytes) de RAM.
* Gabinete para rack padrão 19” (dezenove polegadas) com altura máxima de 2U acompanhado dos respectivos kits de instalação em rack com trilhos deslizantes; Resiliência a falhas de componentes físicos como discos, fontes e o próprio nó de Hiper convergência.
* Possuir uma placa de rede com pelo menos duas portas 10/25/50GbE compatíveis com transceptores SFP+ e SFP28 e cabos de conexão direta tipo DAC ou twinax.
* Cada equipamento deverá prover 20TiB (vinte tebibytes – base 2) de capacidade de armazenamento útil, provida por drives SSD.
* Cada módulo (“nó”) deverá conter no mínimo 20 (vinte) baias dianteiras para discos SSD de 2,5.
* As unidades dedicadas para inicialização do sistema operacional e outras finalidades necessárias para a operação e manutenção do nó não serão consideradas como armazenamento.
* Possuir internamente, no mínimo, 1 (uma) controladora de discos rígidos padrão SAS, que possua, no mínimo: Canais suficientes para o controle de todos os discos suportados pelo chassi; Taxa de transferência de dados de no mínimo 12 Gb/s.
* Permitir a troca de discos avariados, sem interrupção das operações de I/O das aplicações que estão acessando os dados (hot-plug ou hot-swap).
* Os equipamentos deverão ser fornecidos com todos os acessórios necessários para sua instalação, incluindo, mas não se limitando a: trilhos para montagem em rack, cabos de alimentação elétrica e cabos para conexões de rede 10 (dez)/25 (vinte e cinco) Gigabit Ethernet SFP+ / SPF28 por nó.
* Interface de rede dedicada ao gerenciamento remoto, que possibilite o gerenciamento “out-of-band” através de porta RJ-45 dedicada, não sendo essa nenhuma das interfaces da controladora de rede.
* Solução por hardware e/ou software de gerenciamento remoto, independente do sistema operacional e do estado do computador, possibilitando acesso a console gráfica do servidor, mesmo em falha de sistema operacional (virtual KVM).
* Possuir fontes de alimentação em redundância (N+N) com potência individual mínima de 1200 Watts.
* Fontes de alimentação deverão permitir a substituição sem interrupção do funcionamento do equipamento, sendo capazes de suprir individualmente as necessidades do gabinete em sua configuração máxima com no mínimo 50% das fontes instaladas.
* Possuir subsistema de ventilação redundante e hot-swappable.
* Subsistema de alimentação deverá operar em tensões de 100 a 240 VCA (cem a duzentos e quarenta volts de corrente alternada) com seleção automática.
* O subsistema de alimentação deverá vir acompanhado dos cabos de ligação elétrica necessários à sua instalação e ao seu perfeito funcionamento.
* O subsistema deverá implementar de forma nativa mecanismo que viabilize a detecção de falhas em suas fontes de alimentação e ventiladores.
* Será aceita proposta com dimensionamento considerando até 30% de ganhos com desduplicação e compressão (1.43:1). O dimensionamento deverá descontar todas as perdas com formatação, configuração de RAID (quando aplicável) em nível para prover o melhor desempenho para o SDS, fator de replicação (dado original e uma réplica em equipamentos distintos no mesmo cluster e no mesmo site), alta-disponibilidade (HA), área de manobra (*slack space*) e, quando aplicável, grupos de discos em número máximo conforme estabelecido nos manuais do fabricante da solução de armazenamento definida por software, para reduzir impacto durante operações de reconstrução e re-sincronização. Além disso, deverá considerar as perdas relativas à soma de verificação (*checksum*) para garantia de integridade dos dados e quaisquer outras perdas / overhead da solução de armazenamento definida por software, inclusive perdas decorrentes do emprego de tecnologias para ganhos de eficiência como desduplicação e compressão. Caso a solução requeira evacuação dos dados e/ou reformatação dos discos para ativar ou desativar desduplicação/compressão de dados, a área de manobra (*slack space*) deverá ser de pelo menos 30% (trinta por cento), conforme recomendação expressa no manual do fabricante da solução de armazenamento definida por software. Se a solução não for capaz de otimizar os dados no nível do cluster (global), a licitante deverá considerar 30% (trinta por cento) de capacidade de armazenamento útil adicional a fim de compensar a ineficiência da solução por manter cópias redundantes no cluster. Caso a solução perca a eficiência de otimização com desduplicação ou compressão ao utilizar criptografia dos dados, não poderá considerar quaisquer ganhos no dimensionamento da configuração ofertada.
 |
| 26 | Instalação do item 25 |
| 27 | **SOLUÇÃO DE BACKUP COM LICENÇA DE SOFTWARE E GARANTIA DE 60 MESES.*** + Solução de proteção de dados, backup e replicação composta por hardware e software.
	+ Os produtos ofertados devem ser do mesmo fabricante ou homologados pelo mesmo para garantir a completa interoperabilidade do hardware com o software ofertado;
	+ A solução deve ser baseada em Hardware físico, com no mínimo as seguintes configurações:
		- Baseado em rack padrão 19” com altura máxima de 2Rus; Deve suportar processadores Intel Xeon; Possuir no mínimo 2 processadores Intel Xeon 4310 ou superior.; Possuir no mínimo 128GB de RAM DDR4 3200MHz, com módulos de memória de tamanho mínimo de 16GB; Possuir no mínimo 16 slots de discos de 3,5” hot-swappable; Possuir 2x unidades SSD de 480GB 3x DWPD, Possuir no mínimo 16(dezesseis) discos NL-SAS ou SATA superior de 8TB cada; Possuir controladora de disco com suporte a RAID 0, 1, 5, 6, 10, 50, e 60 e com no mínimo 4GB de cache; Deve possuir no mínimo uma placa de rede com 4 portas de 10/25Gbps SFP/SFP28.
	+ Suportar no mínimo os seguintes protocolos:
		- VXLAN e NVGRE; Fibre Channel over Ethernet (FCoE); IEEE 802.1p; IEEE 802.1Qaz; DPDK; N-Port ID Virtualization (NPIV)
	+ A solução deverá possuir fontes de alimentação redundantes e vir equipado com todos os cabos e acessórios para a correta instalação do equipamento;
	+ A solução de backup deve estar licenciada para todos os servidores hypervisors que compõem solução hyperconvergente deste Termo de Referência. O licenciamento não deverá ter limite de máquina virtual ou por volumetria protegida.
	+ A solução deverá ter direito de atualização do software por no mínimo 60 meses.
	+ O licenciamento fornecido deverá ser no mínimo de 60 meses.
	+ A solução deve incluir recursos de backup e replicação integrados em uma única solução; incluindo replicação e reversão da replicação de e para a infraestrutura virtualizada.
	+ A solução não deve precisar da instalação de agentes para realizar suas tarefas de backup, recuperação e replicação de máquinas virtuais.
	+ Fornecer uma estratégia de recuperação rápida, que permita aos usuários prover/restabelecer o serviço quase imediatamente e de maneira simples. Esta estratégia deve consistir em iniciar e ligar a máquina virtual, que falhou, diretamente do arquivo de backup no armazenamento usual do backup.
	+ A recuperação instantânea das máquinas virtuais deve permitir mais de uma máquina virtual e/ou ponto de restauração simultâneo para a disponibilidade do ponto de recuperação funcional, permitindo ter vários pontos no tempo de uma ou mais máquinas virtuais em execução.
	+ Após uma recuperação rápida, deve ser possível realizar uma restauração total sem interrupções de serviço. A ferramenta deve garantir que o trabalho feito pelos usuários não seja afetado ao migrar suas máquinas virtuais do repositório de backup para o armazenamento de produção, sem impor uma restrição de tempo na execução da máquina durante o processo de recuperação instantânea.
	+ A capacidade de executar backup completo (backup) de qualquer máquina virtual deve ser fornecida dentro de uma janela de manutenção mínima, permitindo processos de recuperação completos em interrupções de serviço mais curtas e menos frequentes. A estratégia deve ser replicar ou copiar a quente o backup (backup) da máquina virtual que está em um armazenamento desduplicado para o armazenamento em produção onde a máquina virtual é executada. Além disso, deve poder transferir deste estado de recuperação através de mais de um método tecnológico.
	+ Opção de recuperação instantânea de arquivos que estão dentro dos backups e réplicas das máquinas virtuais. O que deve permitir o acesso ao conteúdo dos discos virtuais dessas máquinas, sem a necessidade de recuperar o backup completo e reiniciar a máquina virtual a partir dele.
	+ Incluir um assistente de recuperação instantânea em nível de arquivo nos sistemas de arquivos mais utilizados do Windows – FAT, FAT32, NTFS, ReFS. Linux – ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs. Solaris – UFS e ZFS (exceto qualquer versão pool do Oracle Solaris). BSD – UFS e UFS2. MacOS – HFS e HFS+.
	+ Criar um índice (catálogo) de todos os arquivos gerenciados pelos sistemas operacionais Windows ou Linux, sem um agente, quando este for o sistema operacional executado dentro de uma máquina virtual cujo backup foi feito.
	+ Realizar pesquisas rápidas através de índices de arquivos que são manipulados por um sistema operacional Windows ou Linux, quando este for o sistema operacional executado dentro de uma máquina virtual cujo backup foi feito.
	+ Garantir a consistência das aplicações transacionais automaticamente por meio da integração com o Microsoft VSS, nos sistemas operacionais Windows.
	+ Realizar backup, logs transacionais (logs de transação) para máquinas virtuais com Microsoft Exchange, SQL Server e Oracle sem utilização de agentes.
	+ Enviar notificações por correio eletrônico (e-mail), SNMP ou através dos atributos da máquina virtual do resultado da execução de suas tarefas.
	+ Incluir ferramentas de recuperação fácil e assistida, através das quais os administradores de servidores de correio como o Microsoft Exchange, nas versões 2010 (SP1, SP2, SP3), 2013, 2016 e 2019, possam comparar os backups realizados com a produção e recuperar objetos individuais, como e-mails e contatos, sem precisar recuperar os arquivos da máquina virtual como um todo e reiniciá-la. Sem exigir uma infraestrutura intermediária ("staging").
	+ Incluir ferramentas de recuperação fácil e assistida, através das quais os administradores de servidores de serviços de diretório, como o Microsoft Active Directory a partir de sua versão 2008-R2 ou superiores, possam comparar os backups realizados com a produção e recuperar objetos individuais, como usuários, grupos, diretivas de grupo (GPOs), registros DNS, partições de configuração, além de outros objetos do AD. Não havendo a necessidade de recuperar os arquivos da máquina virtual como um todo e reiniciá-la.
	+ Incluir ferramentas de recuperação fáceis, por meio das quais os administradores dos servidores de banco de dados do Microsoft SQL Server a partir de sua versão 2005 SP4 e superiores, possam recuperar objetos individuais, como tabelas e registros. Não havendo a necessidade de recuperar os arquivos da máquina virtual como um todo e reiniciar a mesma. Também deverá ser possível a publicação das bases protegidas para servidores SQL de destino, respeitando a versão dos backups.
	+ Incluir ferramentas de recuperação fáceis, através das quais os administradores dos servidores de banco de dados Oracle possam recuperar os bancos de dados. Não havendo a necessidade de recuperar os arquivos da máquina virtual como um todo e reiniciar a mesma.
	+ Oferecer visibilidade instantânea, recursos avançados de pesquisa e recuperação rápida de itens individuais para o Sharepoint 2010, 2013, 2016, 2019 ou superior sem o uso de agentes.
	+ Oferecer 100% de confiabilidade na inicialização correta de todas as suas máquinas virtuais protegidas e no funcionamento do serviço/função dessas máquinas virtuais (servidor DNS, controlador de domínio, servidor de correio, servidor SQL, Oracle, etc.) no momento da recuperação, sendo capaz de realizar testes de recuperabilidade automaticamente a partir das máquinas copiadas.
	+ Criar uma cópia de trabalho do ambiente de produção de qualquer estado anterior para solução de problemas, teste de procedimentos, treinamento etc; executando uma ou várias máquinas virtuais a partir do arquivo de backup em um ambiente isolado, sem a necessidade de mais espaço de armazenamento e sem modificar o backup.
	+ A solução deve permitir a migração de máquinas virtuais entre clusters e datacenters do VMware vSphere.
	+ A solução deve monitorar o espaço livre das LUNs e, se não houver espaço, não deverá executar o snapshot no ambiente virtual.
	+ Oferecer capacidade de recuperação granular do Microsoft Active Directory, Microsoft SQL Server, do Microsoft Exchange Server, do Microsoft SharePoint, do Oracle e dos arquivos do sistema operacional.
	+ Oferecer arquivamento em fita, suporte a VTL (Virtual Tape Libraries), biblioteca de fitas e unidades independentes.
	+ Oferecer trabalhos de cópia de segurança com a implementação de políticas de retenção; com o objetivo de manter uma cópia ou réplica dos arquivos de backup em caso de desastre.
	+ Oferecer aceleração de rede "WAN" integrada e obter uma cópia remota no local por meio da rede "WAN" otimizada e rápida, sem o uso de agentes ou configurações especiais de rede em nenhuma de suas versões.
	+ Incluir a capacidade de realizar backups a partir de snapshots de armazenamento incluído na solução.
	+ Incluir um VMware Plug-in para o vSphere Web Client e monitorar a infraestrutura de backup diretamente do vSphere Web Client, com exibições detalhadas e gerais do status das tarefas e dos recursos de backup.
	+ A solução deve ter um mecanismo de recuperação de emergência dos backups criptografados em caso de perda da senha, podendo ser recuperada com uma senha mestra gerada através do portal web.
	+ A solução deve ter um mecanismo de pesquisa de arquivos global entre os backups.
	+ Oferecer suporte às últimas versões disponíveis dos hipervisores mais populares no mercado: VMWare vSphere e Microsoft Hyper-V em todas as versões compatíveis com o respectivo fabricante.
	+ Não deve exigir hardware específico para obter a desduplicação e a compactação de informações fora dos requisitos padrão de qualquer software (appliance desduplicadora).
	+ Não deve exigir licenças independentes para atividades de backup, recuperação e replicação. Não deverá exigir licenças separadas de software para backup e recuperação granular assistida e consistente das seguintes aplicações:
	+ Microsoft Active Directory 2008 R2 em diante; Microsoft Exchange Server 2010 SP1 em diante; Microsoft SQL Server 2005 SP4 em diante; Oracle Database 11.x e superior para Windows / Linux; Microsoft Sharepoint 2010 em diante.
	+ Permitir a recuperação granular sem a necessidade de configurar ambientes temporários para:
	+ Realizar réplicas em outros sites ou infraestruturas a partir dos backups previamente realizados.
	+ Apresentar um método de recuperação fácil para ambientes de contingência, com ações pré-configuradas para evitar ações manuais em caso de desastre, semelhante a um botão de emergência.
	+ Oferecer a possibilidade de armazenar backups de forma criptografada, bem como garantir o trânsito de informações sob esse esquema a partir do arquivo de backup, sem exigir criptografia do sistema de armazenamento
	+ Permitir a delegação de tarefas de recuperação, no nível de elementos de aplicação, para outros usuários, a fim de baixar o número de processos a serem executados pelo administrador da plataforma.
	+ Recursos internos que permitam selecionar um destino de armazenamento de backup que possa ser hospedado por um provedor de serviços em nuvem (BaaS).
	+ Funcionalidades integradas que permitam a seleção de um destino de replicação que possa ser hospedado em um provedor de serviços em nuvem (DRaaS).
	+ Funcionalidade para gerar armazenamento de backup global, que pode incluir vários e diferentes tipos de armazenamento, e direcionar tarefas de backup para ele como se fosse um, permitindo também crescimento em escala dos mesmos, sem impacto sobre o meio ambiente de backup já configurado.
	+ Integração com hardware de desduplicação EMC Data Domain, HP StoreOnce, Quantum DXi e ExaGrid, além de otimizações para o uso de qualquer sistema de armazenamento desduplicado.
	+ Integração com plataformas de desduplicação na origem – EMC DataDomain Boost e HP StoreOnce Catalyst e Quantum Accent.
	+ Possuir um número de produto exclusivo, de acordo com a versão ou edição, fornecido pelo fabricante para a aquisição do pacote de software que inclui todas as funcionalidades mencionadas acima.
	+ Capacidade de definir grupos de fitas magnéticas para serem utilizadas em uma única sessão de armazenamento em fita (Media Pool) para maximizar o desempenho e a velocidade de transferência.
	+ A solução deve suportar e armazenar os arquivos de fita desduplicados, obtendo maior eficiência do espaço da fita.
	+ Capacidade de processar o envio de dados em várias unidades de fita, em paralelo para maximizar a largura de banda e minimizar o tempo de transferência.
	+ Capacidade de desvincular a função do servidor da infraestrutura da solução que permite acesso a unidades de fita, evitando a necessidade de essa função se sobrepor a outras funções na solução.
	+ Ter a capacidade de leitura direta do sistema de armazenamento central, quando em um ambiente de infraestrutura VMWare, apresentado através do protocolo NFS, evitando assim o tráfego de informações através das interfaces de controle do hipervisor.
	+ Ser capaz de diferenciar, nas máquinas virtuais com sistema operacional MS Windows, os blocos de disco que contêm dados irrelevantes (blocos sujos) e evitar sua transferência para os backups, bem como a exclusão arbitrária de arquivos nas máquinas virtuais com sistema operacional MS Windows instalado no sistema de arquivos NTFS.
	+ A solução deve fornecer mecanismos de proteção para evitar sobrecarga nos sistemas de armazenamento da plataforma virtual, através de monitoramento próativo dos datastores, permitindo a auto-regulação do sistema de backups e da função de replicação, em função dos limites definidos. Deverá ter a capacidade de diferenciar por unidade lógica ou LUN e definir limites diferenciados para cada um deles.
	+ Capacidade de aproveitar o subsistema de rastreio de blocos alterados (CBT) do ambiente virtual, também para operações de retorno (failback), acelerando a transferência de dados para o datacenter produtivo.
	+ Suporte para backups nativos (integrados) no VMWare Cloud na AWS.
	+ Integração com armazenamento de objetos como o Amazon S3, Azure Blob Storage, IBM Cloud Object Storage, bem como com provedores de serviços compatíveis com o protocolo S3 e armazenamento local compatível com o protocolo S3.
	+ Eficiência no uso da largura de banda quando integrada ao armazenamento em nuvem pública, permitindo a recuperação granular de dados, a partir dos blocos do arquivo de backup, economizando significativamente o custo da operação em largura de banda.
	+ Quando integrado ao armazenamento em nuvem pública, ele deve ser autossuficiente e não depender de qualquer catálogo externo, permitindo, em caso de desastre, a recuperação completa dos arquivos armazenados na nuvem pública.
	+ Permitir recuperações futuras a qualquer momento sem exigir uma licença paga. Ou seja, você pode usar a versão gratuita do produto para esses fins.
	+ Permitir a conformidade com padrões como o GDPR para dados ou registrar exclusões de maneira automatizada usando scripts (feitos pelo cliente) nos arquivos de backup antes de restaurar uma máquina virtual no ambiente produtivo. Além disso, deverá permitir que os administradores façam alterações no sistema operacional, instalação ou remoção de aplicações para estar em conformidade com diretriz corporativa ao restaurar uma máquina virtual.
	+ Integrada com diferentes antivírus para realizar análises de infecção nos backups existentes na plataforma, por exemplo, backups anteriores da mesma solução, análise antes de fazer uma recuperação instantânea ou completa da máquina virtual. Além de estar integrado no mecanismo de teste automatizado das máquinas virtuais e/ou conteúdo da máquina virtual, para realizar proativamente a análise prévia.
	+ Identificar e excluir automaticamente as máquinas virtuais que possuem o recurso "Multi-Writer" habilitado.
	+ Prover suporte para plataformas de servidor Microsoft Windows Server 2019 ou superior.
	+ A solução deve oferecer suporte aos ambientes Oracle RAC (versões 11 e superior) usando o RMAN e deve ser certificada.
	+ A solução deve ter suporte para SAP HANA (versões 2.0 SPS 02 - SPS 03) via BACKINT e deve ser certificada.
	+ A solução deve permitir que a integração com as funções do VMware vSphere forneça um mecanismo de autoatendimento via Web, que permitirá o gerenciamento dos backups atribuídos aos usuários configurados.
* A solução também deve permitir a recuperação apenas dos blocos de disco da máquina virtual que foram alterados usando o CBT.
 |
| 28 | Instalação do item 27 |
| 29 | **SUBSCRIÇÃO DE SOFTWARE HCI E GARANTIA DE 60 MESES**.* + Deverá ser fornecida unidade de subscrição de software hiperconvergente por núcleo de processamento (core).
	+ O software hiperconvergente deverá incluir virtualização de infraestrutura (computação, rede e armazenamento) e o respectivo gerenciamento configurado de maneira a garantir alta disponibilidade e sem ponto único de falha.
	+ O software HCI deverá permitir a configuração de um cluster com todos os equipamentos deste termo de referência, mesmo com as diferentes especificações de seus componentes internos, sendo permitida também a adição de novos equipamentos futuramente com novas gerações de processadores, diferentes configurações de discos, memória RAM e a inclusão de novos equipamentos com GPU para atender demandas de virtualização de desktops para equipe de engenharia.
	+ Permitir a realização de snapshots e clones através da solução de armazenamento de dados definida por software (SDS), independente do Hipervisor, utilizando algoritmo redirect-on-write para maior eficiência na utilização de storage bem como no tempo necessário para conclusão do snapshot ou clone.
	+ Quando da inclusão online e não disruptiva de novos equipamentos com mais de uma camada de armazenamento (NVMe/SSD/HDD), o software deverá realizar a movimentação dos dados entre as camadas para favorecer o desempenho necessário aos dados mais acessados, garantindo a gestão do ciclo de vida dos dados (ILM) no nível do cluster.
	+ A solução deverá permitir a definição do número de réplicas dos dados no mesmo cluster, sendo o dado original e uma réplica, em equipamentos distintos no mesmo cluster, para aplicações menos críticas e o dado original mais duas réplicas, em equipamentos distintos no mesmo cluster, para aplicações mais críticas.
	+ A solução deverá permitir a configuração de domínios de disponibilidade de modo a tolerar a falha de equipamentos e racks. A falha de um disco não deve interromper ou impactar o funcionamento de outros discos na solução.
	+ A subscrição de software deverá permitir a compressão de dados durante a sua ingestão e após o seu armazenamento na camada de capacidade.
	+ O SDS deverá permitir a desduplicação global dos dados, tanto na camada de desempenho quanto na camada de capacidade, de modo que até a replicação dos dados para outro cluster seja otimizada para reduzir o uso de banda.
	+ Deverá permitir a configuração de QoS de armazenamento para máquinas virtuais (VMs) a fim de limitar a utilização demasiada de recursos que pudesse interferir no funcionamento de outras VMs no mesmo cluster.
	+ Permitir a priorização do uso da camada de maior desempenho do storage para determinadas VMs e seus respectivos discos virtuais através da interface gráfica de gestão.
	+ Deverá permitir a configuração de armazenamento através de volumes iSCSI para VMs em execução no cluster HCI e para aplicações externas ao cluster, inclusive bare-metal.
	+ A subscrição deverá permitir a configuração de planos de proteção com retenção de snapshots locais e a replicação de dados otimizada (desduplicação e compressão) para outro cluster com objetivo de ponto de recuperação (RPO) de pelo menos 1h (uma hora).
	+ Deverá permitir a realização de snapshots através do SDS com consistência para os dados da aplicação (application-consistent), tanto para VMs com sistema operacional Windows como para VMs com sistema operacional Linux, através de tecnologia VSS e semelhantes.
	+ Permitir que o próprio administrador da máquina virtual realize a recuperação granular de arquivos sem a necessidade de envolvimento da equipe responsável pela gestão das cópias de segurança (backup).
	+ Deverá permitir a autenticação do cliente para que o cluster HCI obtenha um certificado válido do usuário garantindo uma autenticação bidirecional em que o servidor também verifica a autenticidade do usuário através de um certificado válido fornecido por ele ao acessar a console de gestão.
	+ Para aumento de segurança, a subscrição deverá permitir o bloqueio do cluster HCI para restringir o acesso administrativo ao Hipervisor e SDS somente através do uso de chaves SSH, sem a utilização de senhas.
	+ O software deverá permitir o uso da funcionalidade de segurança Windows Defender Credential Guard para isolamento das credenciais em máquinas virtuais com sistema operacional Windows, evitando ataques como Pass-the-Hash e Pass-The-Ticket.
	+ O software HCI deverá permitir o emprego de tecnologias como vGPU para compartilhamento de GPU entre desktops virtualizados e GPU passthrough para aplicações de inteligência artificial e aprendizagem de máquina virtualizadas e conteinerizadas.
	+ O software HCI deverá permitir o provisionamento automatizado, operações e a gestão do ciclo de vida de um cluster Kubernetes pronto para ambiente de produção com alta disponibilidade utilizando mais de um master node, permitindo integração com balanceador de carga existente. O cluster Kubernetes deverá ser implantado com armazenamento persistente em modo de acesso Read-Write-Once para aplicativos em contêineres através de integração nativa com CSI driver para Volumes iSCSI e compartilhamento NFS, e Read-Write-Many para compartilhamento NFS. Também deverá ser possível a integração com o serviço de armazenamento de objetos através de protocolo S3. Deverá permitir operações de escalabilidade para aumento do número de worker nodes sem interrupção para os aplicativos e com a simplicidade de um clique através da interface gráfica. Permitir atualização de software dos nodes e do Kubernetes sem interrupção para os aplicativos de produção. Deverá prover ferramentas para monitoramento, registro e alerta utilizando pilha EFK (Prometheus, ElasticSearch, Fluent Bit e Kibana) ou semelhantes.
	+ A solução deverá permitir a gestão centralizada de múltiplos clusters no mesmo centro de dados e em centros distantes geograficamente para que seja possível gestão da infraestrutura, monitoramento de alertas e saúde destes clusters.
	+ Deverá permitir a autenticação em nível empresarial utilizando Role Based Access Control (RBAC), sendo possível atribuir diferentes níveis de permissão para usuários e grupos de usuários.
	+ Deverá permitir a integração com outras tecnologias através de APIs do tipo REST.
	+ A interface de gerenciamento web deverá possuir uma ferramenta de busca contextualizada para acelerar as pesquisas na interface gráfica.
	+ O fabricante da solução deverá disponibilizar um portal de suporte para abertura de chamados, upload de logs e dados de diagnóstico relevantes para o chamado, acesso a documentação, base de conhecimento, download de atualizações, verificação de alertas relacionados à infraestrutura e compatibilidade de firmwares e softwares.
	+ A solução deverá possuir uma ferramenta para automatizar e orquestrar todos os procedimentos necessários para atualização dos firmwares e softwares relacionados com um assistente para elaborar todo o planejamento e sequenciamento dos procedimentos de atualização.
 |
| 30 | Instalação do item 29 |
| 31 | **SWITCH L2, 24 PORTAS GIGABIT ETHERNET, STACKABLE (EMPILHÁVEL), POE +, COM LICENÇA DE SOFTWARE PARA PLATAFORMA DE GERENCIAMENTO EM NUVEM POR PERÍODO DE 60 MESES.*** Composto de um único equipamento, padrão 19 polegadas e 1U de altura, acompanhado dos devidos acessórios para montagem em rack;
* Possuir garantia por toda vida util (lifetime warranty)
* Possuir fluxo de ventilacao frente-para-tras ( front to back);
* Possuir 01 porta 10/100/1000 BASET exclusiva para gerenciamento;
* Todas as portas deverao estar devidamente habilitadas e licenciadas;
* Possuir portas especificas de empilhamento, com, no minimo 80 Gbps de capacidade por switch;
* Permitir empilhamento de até 08 Switches;
* Tipo arquitetura non-blocking ;
* Possuir capacidade de suportar 4.094 VLANs 802.1Q
* Implementar spanning tree 802.1d e 802.1w
* Implementar controle sobre broadcast storm
* Implementar protocolo LLDP 802.1AB
* Implementar LACP 802.3ad com no minimo 8 portas agregadas
* Implementar port mirroring
* Implementar priorização de tráfego via CoS 802.1p com 8 filas por porta
* Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP)
* Implementar IGMP snooping
* Implementar 802.1x, com configuração automatizada de vlans de usuários
* Implementar controle de acesso baseado em endereço MAC
* Implementar funcionalidade BPDU guard
* Implementar funcionalidade root guard
* Implementar funcionalidade DHCP snooping
* Implementar bypass de autenticação via endereço MAC
* Implementar roteamento estático
* Implementar roteamento entre VLAN's
* Implementar DHCP relay
* Possuir recursos de "zero touch provisioning" a fim de facilitar e agilizar a instação
* Implementar autenticação baseada em MAC address
* Implementar VLANs para trafego de voz de forma automatica, Voice VLAN;
* Implementar isolação de portas para impedir a comunicação de hosts dentro da mesma VLAN;
* Implementar a criação de ACLs baseadas em IP origem, porta de origem, IP destino, porta de destino, protocolo ou VLAN;
* Implementar os seguintes padrões:
* IEEE 802.1D MAC Bridges;
* IEEE 802.1p Priority;
* IEEE 802.1Q VLANs;
* IEEE 802.1w Rapid Reconfiguration of Spanning Tree;
* IEEE 802.3ad Link Aggregation Control Protocol (LACP);
* IEEE 802.1AB Link Layer Discovery Protocol (LLDP);
* IEEE 802.1D (STP);
* IEEE 802.1p (CoS);
* IEEE 802.1X Port Based Network Access Control;
* Login de rede baseado no protocolo IEEE 802.1x, permitindo que a porta do Switch seja automaticamente associada a VLAN definida para o usuário no Servidor RADIUS;
* RADIUS CoA;
* Autenticação baseada em web, com suporte a SSL, através de RADIUS;
* Autenticação baseada em endereço MAC, através de RADIUS;
* Possuir tabela MAC com entrada para no minimo 32.000 endereços MAC
* Identificar as principais aplicações de camada 7, que trafegam nas interfaces do switch, sem a necessidade de equipamentos externos para tal.
* Solução de gerenciamento centralizado, capaz de realizar operações de atualização de software, configuração, e extração de relatórios de todos os equipamentos. Essa solução de gerenciamento deve ser redundante, em niveis de hardware e software, ativo-ativo e ter seu licenciamento completo, opcionalmente pode ser entregue uma solução de gerenciamento em nuvem;
* A solução de gerenciamento deve ser baseada em nuvem, não podendo ser On-Premises;
* Possuir certificacao ISO27001
* A solução de gerenciamento deve ser capaz de gerenciar dispositivos em localidades diferentes;
* Interface de gerência com disponibilidade de 99,99% ou melhor;
* Implementar a atualização de imagens de software de maneira agendada;
* Implementar a atualização de imagens de software sem a necessidade de intervenção manual;
* Implementar Syslog;
* A solução de gerenciamento deve ser capaz de mostrar logs de alterações na configuração, juntamente com a data, usuário e alteração realizada;
* Implementar visualização de informações através de SNMPv1/v2c/v3;
* Implementar gerenciamento via web com suporte a HTTPS/SSL, permitindo visualização gráfica da utilização das portas;
* Apresentar relatórios das principais aplicações (camada 7) que estão sendo usadas na rede;
* Implementar recurso de "template" a fim de configurar diversos equipamentos e grupos de equipamentos simultaneamente
* Os equipamentos deverão fornecer para a plataforma de gestão estatísticas históricas detalhadas de uso por interface e por dispositivo conectado;
* Os equipamentos deverão incluir mecanismos de classificação e profiling dos dispositivos conectados a eles, identificando características, como fabricante e sistema operacional;
* Contar com mecanismos para garantir que o sistema operacional seja íntegro, consistente e atualizado em todos os switches de maneira automatizada;
* Os equipamentos deverão ser configurados e monitorados de maneira unificada, tendo a capacidade de aplicar configurações a distintas interfaces de distintos equipamentos de forma simultânea, inclusive para dispositivos em localidades diferentes;
* Os equipamentos deverão suportar o envio de alertas sobre seu estado via e-mail, tais como: se o switch está disponível para a plataforma de gestão por 5 ou mais minutos, se uma interface se desabilitar por um determinado tempo, seja por mudança de velocidade na interface, seja por problemas no cabo, dentre outros;
* Capacidades para fazer capturas de pacotes de forma remota usando a plataforma de gestão para fins de diagnóstico de falhas; Será aceita solução externa caso a platarforma não tenha nativamente
* A solução de gerenciamento deve mostrar automaticamente uma topologia da rede com os dispositivos conectados;
* A solução de gerenciamento deve apresentar no minimo os seguintes relatórios e funcionalidades:
* Identificar todos usuários da rede, por nome, autenticação ou dispositivo dos ultimos 30 dias;
* Identificar os os IPs de todos usuários;
* Identificar os MAC address de todos usuários;
* Identificar VLANs de todos usuários;
* Identificar as principais aplicações que esses usuários trafegaram na rede;
* Identificar as aplicações que mais consomem a rede nos ultimos 30 dias;
* Identificar os equipamentos que mais consomem a rede;
* Identificar os usuários que mais consomem a rede;
* A solução de gerenciamento deve listar graficamente todos os equipamentos da rede, identificando quais estão online, ou não;
* A solução de gerenciamento deve identificar o serial number de cada dispositivo;
* A solução de gerenciamento deve identificar graficamente quais portas do switch estão ou não sendo utilizadas, inclusive com PoE ou não;
* A solução de gerenciamento deve identificar quais clientes estão conectados do switch;
* A solução de gerenciamento deve mostrar graficamente onde cada switch está fisicamente instalado; independente da localidade
* A ferramenta de gerência deve permitir visualizar o tráfego geral da rede, separado por aplicação, incluindo quantidade de dados trafegados(UP/DOWN), duração da conexão e quantidade de clientes que utilizou a aplicação;
* Permitir a criação de políticas para desativação e ativação de portas baseado em horário de forma a economizar energia em momentos ociosos.
* Manter log de alteraçoes de configuração. E usuário responsavel pela alteração
* A ferramenta de gerencia deve ter capacidade de configurar diversas portas, de diversos equipamentos de forma simultanea
* Sistema de login deverá suportar autenticação de 2 fatores por SMS e Google Authenticator;
* Diferentes níveis de acesso a ferramenta de gerenciamento devem ser disponibilizados
* Ferramenta de gerencia deverá permitir que os equipamentos sejam separados em grupos, e apresentar esses grupos independentemente;
* Possuir 24 portas ethernet UTP padrão 10/100/1000 BASE-T
* Possuir no minimo 04 slots/portas do tipo SFP+ fixas ao equipamento para instalação de transceivers 10Gbps Multimodo ou Monomodo;
* Possuir switching capacity de no minimo 128 Gbps
* Possuir taxa de encaminhamento de pacotes de no minimo 130 Mpps
* Possuir um MTBF (Tempo médio entre falhas) de, no mínimo 320 mil horas;
* Implementar IEEE 802.3af suportando ao menos 370 Watts dedicados ao PoE;
* Implementar IEEE 802.3at PoE+;
* Implementar alimentação em todas as 24 interfaces RJ45 simultaneamente considerando IEEE 802.3af (15,4W) e/ou, no mínimo, 4 interfaces simultaneamente para IEEE 802.3at (30W).
* Permitir ativação e desativação manual (via console de gerencia) do POE, em cada porta.
* Possuir mecanismo que não permita a utilização do Switch em outras redes e ambientes, em caso de furto. A ferramenta de gerencia na nuvem deve ser capaz de bloquear o equipamento, e caso ele seja reconectado a internet, detectar e rastrear o equipamento, baseado no endereco IP publico utilizado pelo mesmo
* Implementar padrão IPV6 para conectividade com a gerencia na nuvem .Caso o equipamento não suporte IPV6 para gereciamento, essa função pode ser implementada em um equipamento externo tipo firewall camada 7, que devera ser fornecido junto com cada switch do projeto.

Apresentar as informações sobre as principais aplicações de camada 7 que passaram pelo equipamento, correlacionando estas informações com as informações de usuários, e apresentando de maneira clara, gráficos de consumo de aplicações camada 7, por usuário. Essas informacoes devem ser apresentadas e visualizadas no plataforma de gerencia. |
| 32 | Instalação do item 31 |
| 33 | **SWITCH L2, 48 PORTAS GIGABIT ETHERNET, STACKABLE (EMPILHÁVEL), POE +, COM LICENÇA DE SOFTWARE PARA PLATAFORMA DE GERENCIAMENTO EM NUVEM POR PERÍODO DE 60 MESES.*** Equipamento único, padrão 19 polegadas e 1U de altura, acompanhado dos devidos acessórios para montagem em rack;
* Além das 48 portas UTP. Possuir pelo menos 4 portas com conectores padrão SFP.
* Possuir garantia por toda vida util (lifetime warranty)
* Possuir fluxo de ventilacao frente-para-tras ( front to back);
* Possuir 01 porta 10/100/1000 BASET exclusiva para gerenciamento;
* Todas as portas deverão estar devidamente habilitadas e licenciadas;
* Possuir portas especificas de empilhamento, com, no mínimo 80 Gbps de capacidade por switch;
* Permitir empilhamento de até 08 Switches;
* Arquitetura non-blocking;
* Possuir capacidade de suportar 4.094 VLANs 802.1Q
* Implementar as seguintes funcionalidades:
	+ DHCP relay
	+ Spanning tree 802.1d e 802.1w
	+ Controle sobre broadcast storm
	+ Protocolo LLDP 802.1AB
	+ LACP 802.3ad com no minimo 8 portas agregadas
	+ Port mirroring
	+ Priorização de tráfego via CoS 802.1p com 8 filas por porta
	+ Leitura, classificação e remarcação de QoS (802.1p e DSCP)
	+ IGMP snooping
	+ 802.1x, com configuração automatizada de vlans de usuários
	+ Controle de acesso baseado em endereço MAC
	+ Funcionalidade BPDU guard
	+ Funcionalidade root guard
	+ Funcionalidade DHCP snooping
	+ Bypass de autenticação via endereço MAC
	+ Roteamento estático
	+ Roteamento entre VLAN's
* Possuir recursos de "zero touch provisioning" a fim de facilitar e agilizar a instação
* Implementar autenticação baseada em MAC address
* Implementar VLANs para trafego de voz de forma automatica, Voice VLAN;
* Implementar isolação de portas para impedir a comunicação de hosts dentro da mesma VLAN;
* Implementar a criação de ACLs baseadas em IP origem, porta de origem, IP destino, porta de destino, protocolo ou VLAN;
* Deve implementar os seguintes padrões:
	+ IEEE 802.1D MAC Bridges;
	+ IEEE 802.1p Priority;
	+ IEEE 802.1Q VLANs;
	+ IEEE 802.1w Rapid Reconfiguration of Spanning Tree;
	+ IEEE 802.3ad Link Aggregation Control Protocol (LACP);
	+ IEEE 802.1AB Link Layer Discovery Protocol (LLDP);
	+ IEEE 802.1D (STP);
	+ IEEE 802.1p (CoS);
	+ IEEE 802.1X Port Based Network Access Control;
	+ Login de rede baseado no protocolo IEEE 802.1x, permitindo que a porta do Switch seja automaticamente associada a VLAN definida para o usuário no Servidor RADIUS;
	+ RADIUS CoA;
	+ Autenticação baseada em web, com suporte a SSL, através de RADIUS;
	+ Autenticação baseada em endereço MAC, através de RADIUS;
* Possuir tabela MAC com entrada para, no mínimo, 32.000 endereços MAC
* Identificar as principais aplicações de camada 7, que trafegam nas interfaces do switch, sem a necessidade de equipamentos externos para tal.
* Solução de gerenciamento centralizado, capaz de realizar operações de atualização de software, configuração, e extração de relatórios de todos os equipamentos. Essa solução de gerenciamento deve ser redundante, em níveis de hardware e software, ativo-ativo e ter seu licenciamento completo, opcionalmente pode ser entregue uma solução de gerenciamento em nuvem;
* A solução de gerenciamento deve ser baseada em nuvem, não podendo ser On-Premises;
* Possuir certificacao ISO27001
* A solução de gerenciamento deve ser capaz de gerenciar dispositivos em localidades diferentes;
* Interface de gerência com disponibilidade de 99,99% ou melhor;
* Implementar a atualização de imagens de software de maneira agendada;
* Implementar a atualização de imagens de software sem a necessidade de intervenção manual;
* Implementar Syslog;
* A solução de gerenciamento deve ser capaz de mostrar logs de alterações na configuração, juntamente com a data, usuário e alteração realizada;
* Implementar visualização de informações através de SNMPv1/v2c/v3;
* Implementar gerenciamento via web com suporte a HTTPS/SSL, permitindo visualização gráfica da utilização das portas;
* Apresentar relatórios das principais aplicações (camada 7) que estão sendo usadas na rede;
* Implementar recurso de "template" a fim de configurar diversos equipamentos e grupos de equipamentos simultaneamente
* Os equipamentos deverão fornecer para a plataforma de gestão estatísticas históricas detalhadas de uso por interface e por dispositivo conectado;
* Os equipamentos deverão incluir mecanismos de classificação e profiling dos dispositivos conectados a eles, identificando características, como fabricante e sistema operacional;
* Deverá contar com mecanismos para garantir que o sistema operacional seja íntegro, consistente e atualizado em todos os switches de maneira automatizada;
* Os equipamentos deverão ser configurados e monitorados de maneira unificada, tendo a capacidade de aplicar configurações a distintas interfaces de distintos equipamentos de forma simultânea, inclusive para dispositivos em localidades diferentes;
* Os equipamentos deverão suportar o envio de alertas sobre seu estado via e-mail, tais como: se o switch está disponível para a plataforma de gestão por 5 ou mais minutos, se uma interface se desabilitar por um determinado tempo, seja por mudança de velocidade na interface, seja por problemas no cabo, dentre outros;
* Deverão ser inclusas capacidades para fazer capturas de pacotes de forma remota usando a plataforma de gestão para fins de diagnóstico de falhas; Será aceita solução externa caso a platarforma não tenha nativamente
* A solução de gerenciamento deve mostrar automaticamente uma topologia da rede com os dispositivos conectados
* A solução de gerenciamento deve apresentar, no mínimo, os seguintes relatórios e funcionalidades:
	+ Identificar todos usuários da rede, por nome, autenticação ou dispositivo dos ultimos 30 dias;
	+ Identificar os os IPs de todos usuários;
	+ Identificar os MAC address de todos usuários;
	+ Identificar VLANs de todos usuários;
	+ Identificar as principais aplicações que esses usuários trafegaram na rede;
	+ Identificar as aplicações que mais consomem a rede nos ultimos 30 dias;
	+ Identificar os equipamentos que mais consomem a rede;
	+ Identificar os usuários que mais consomem a rede.
* Listar graficamente todos os equipamentos da rede, identificando quais estão online, ou não
* Identificar o serial number de cada dispositivo
* Identificar graficamente quais portas do switch estão ou não sendo utilizadas, inclusive com PoE ou não
* Identificar quais clientes estão conectados do switch
* Mostrar graficamente onde cada switch está fisicamente instalado; independente da localidade
* A ferramenta de gerência deve permitir visualizar o tráfego geral da rede, separado por aplicação, incluindo quantidade de dados trafegados(UP/DOWN), duração da conexão e quantidade de clientes que utilizou a aplicação;
* Permitir a criação de políticas para desativação e ativação de portas baseado em horário de forma a economizar energia em momentos ociosos.
* Manter log de alterações de configuração. E usuário responsavel pela alteração
* A ferramenta de gerencia deve ter capacidade de configurar diversas portas, de diversos equipamentos de forma simultânea
* Sistema de login deverá suportar autenticação de 2 fatores por SMS e Google Authenticator;
* Diferentes níveis de acesso a ferramenta de gerenciamento devem ser disponibilizados
* Ferramenta de gerência deverá permitir que os equipamentos sejam separados em grupos, e apresentar esses grupos independentemente;
* Possuir 48 portas ethernet UTP padrão 10/100/1000 BASE-T
* Possuir, no mínimo, 04 slots/portas do tipo SFP+ fixas ao equipamento para instalação de transceivers 10Gbps Multimodo ou Monomodo;
* Possuir switching capacity de, no mínimo, 176 Gbps
* Possuir taxa de encaminhamento de pacotes de, no mínimo, 130 Mpps
* Possuir um MTBF (Tempo médio entre falhas) de, no mínimo 320 mil horas;
* Implementar IEEE 802.3af suportando ao menos 740 Watts dedicados ao PoE;
* Implementar IEEE 802.3at PoE+;
* Implementar alimentação em todas as 48 interfaces RJ45 simultaneamente considerando IEEE 802.3af (15,4W) e/ou, no mínimo, 4 interfaces simultaneamente para IEEE 802.3at (30W).
* Permitir ativação e desativação manual (via console de gerência) do POE, em cada porta.
* Possuir mecanismo que não permita a utilização do Switch em outras redes e ambientes, em caso de furto. A ferramenta de gerencia na nuvem deve ser capaz de bloquear o equipamento, e caso ele seja reconectado a internet, detectar e rastrear o equipamento, baseado no endereco IP publico utilizado pelo mesmo
* Implementar padrão IPV6 para conectividade com a gerencia na nuvem .Caso o equipamento não suporte IPV6 para gereciamento, essa função pode ser implementada em um equipamento externo tipo firewall camada 7, que devera ser fornecido junto com cada switch do projeto
* Apresentar as informações sobre as principais aplicações de camada 7 que passaram pelo equipamento, correlacionando estas informações com as informações de usuários, e apresentando de maneira clara, gráficos de consumo de aplicações camada 7, por usuário. Essas informações devem ser apresentadas e visualizadas no plataforma de gerência.
 |
| 34 | Instalação do item 33 |
| 35 | **TELEFONE IP TIPO I COM LICENÇA DE SOFTWARE, GARANTIA DE 36 MESES E INSTALAÇÃO.*** **PROTOCOLOS E CODEC**
* Implementar protocolo SIP
* Implementar os padrões de codificação G.711a, G.711μ, G.729, G729a e G729ab.
* Capacidade de identificar de forma dinâmica a Vlan de Voz, e permitir que o tráfego de dados e de voz utilizem VLANs distintas;
* **FUNCIONALIDADES DE CHAMADA**
* Deve possuir funções do display em idioma Português Brasil
* Devem implementar a configuração do toque de chamada.
* Devem permitir o ajuste de volume de chamada diretamente no aparelho.
* Devem permitir que se efetue transferência de chamadas internas e externas.
* **CARACTERISTICAS FISICAS**
* Possuir suporte a 1 linha.
* Possuir display de cristal líquido com resolução mínima de 128 por 32 pixels.
* Possuir duas portas switch 10/100 ethernet integradas internas, permitindo a conexão de um computador diretamente ao telefone IP fixo, nas velocidades de 10/100 Mbps, autosensing.
* Possuir alto falante e microfone específicos para a função de viva-voz.
* Implementar PoE (Power Over Ethernet) para alimentação direta via interface Ethernet (IEEE 802.3af);
* Possuir teclas físicas dedicadas para mute, ajuste de volume, viva-voz, espera, transferência e rediscagem.
* Possuir teclas para ajuste de volume do monofone, alto-falante e toque.
 |
| 36 | **TELEFONE IP TIPO II COM LICENÇA DE SOFTWARE, GARANTIA DE 36 MESES E INSTALAÇÃO*** **PROTOCOLOS E CODEC**
* Implementar protocolo SIP
* Implementar os padrões de codificação G.711a, G.711μ, G.729, G729a e G729ab.
* Capacidade de identificar de forma dinâmica a Vlan de Voz, e permitir que o tráfego de dados e de voz utilizem VLANs distintas;
* **FUNCIONALIDADES DE CHAMADA**
* Possuir funções do display em idioma Português Brasil
* Implementar a configuração do toque de chamada.
* Permitir o ajuste de volume de chamada diretamente no aparelho.
* Permitir que se efetue transferência de chamadas internas e externas.
* **CARACTERISTICAS FISICAS**
* Possuir suporte a 2 linha.
* Possuir display de cristal líquido com resolução mínima de 396 por 162 pixels.
* Possuir duas portas switch 10/100 ethernet integradas internas, permitindo a conexão de um computador diretamente ao telefone IP fixo, nas velocidades de 10/100 Mbps, autosensing.
* Possuir alto falante e microfone específicos para a função de viva-voz.
* Implementar PoE (Power Over Ethernet) para alimentação direta via interface Ethernet (IEEE 802.3af);
* Possuir teclas físicas dedicadas para mute, ajuste de volume, viva-voz, espera,

transferência e rediscagem.* Possuir teclas para ajuste de volume do monofone, alto-falante e toque.
 |
| 37 | **TELEFONE IP TIPO III COM LICENÇA DE SOFTWARE, GARANTIA DE 36 MESES E INSTALAÇÃO*** **PROTOCOLOS E CODEC**
* Implementar protocolo SIP
* Implementar os padrões de codificação G.711a-law, G.711mu-law, G.722, G.729a, iLBC, e iSAC.
* Capacidade de identificar de forma dinâmica a Vlan de Voz e permitir que o tráfego de dados e de voz utilizem VLANs distintas;
* **FUNCIONALIDADES DE CHAMADA**
* Possuir funções do display em idioma Português Brasil
* Implementar a configuração do toque de chamada.
* Permitir o ajuste de volume de chamada diretamente no aparelho.
* Permitir que se efetue transferência de chamadas internas e externas.
* **CARACTERISTICAS FÍSICAS**
* Possuir 5 teclas de linhas programáveis.
* Possuir display de 5 polegadas, colorido de com resolução mínima de 800 por 480 widescreen.
* Possuir câmera que permita vídeo bidirecional de 720p HD.
* Suportar Bluetooth 4.1.
* Possuir porta AUX RJ-9, para conexão de headset analógico.
* Possuir duas portas switch 10/100/1000 ethernet integradas internas, permitindo a conexão de um computador diretamente ao telefone IP fixo, nas velocidades de 10/100/1000 Mbps, autosensing.
* Possuir teclas para ajuste de volume do fone e do toque.
* Possuir alto falante e microfone específicos para a função de viva-voz.
* Implementar PoE (Power Over Ethernet) para alimentação direta via interface Ethernet (IEEE 802.3af) e (IEEE 802.3at);
* Possuir teclas físicas dedicadas para ajuste de volume, viva-voz, mute, espera, transferência, conferencia e headset.
* Suportar modulo de expansão.
* Possuir 2 portas USB.
 |
| 38 | Suporte Técnico e Manutenção |

Maricá, 01 de abril de 2024.

**Responsáveis técnicos,**

|  |  |
| --- | --- |
| **Walter Matoso Rosa Junior**Assistente - Mat.: 3.300.352Superintendência de Infraestrutura Diretoria Administrativa | **Alessandra Lopes Rangel** Mat.: 3.300.020Superintendente de Infraestrutura Diretoria Administrativa |

**Conferido e de acordo,**

**Daniel Ferreira da Silva**

Mat.:3.300.002

Diretor Administrativo

**ANEXO B**

**LOCAIS DE EXECUÇÃO DO OBJETO**

|  |  |  |
| --- | --- | --- |
| **TIPO DE UNIDADE**  | **USF** | **ENDEREÇO** |
| A | Carlos Alberto Soares (MCMV Inoã) | Estrada do Bosque Fundo, S/N BOSQUE FUNDO (LOT BSQ FUNDO) CEP: 24.943-060 |
| Carlos Marighella (MCMV Itaipuaçu) | Rua R, S/N CHÁCARAS DE INOÃ CEP: 24.940-640 |
| Marques/Condado | Rua Babaçu, S/N CONDADO DE MARICÁ CEP: 24.905-180 |
| Jacaroá Caju | Rua Ovídio Moreira de Souza - S/N JACAROÁ CEP: 24.902-430 |
| Jaconé | Estrada Ponta Negra-Sampaio Correia, S/N JACONÉ (PONTA NEGRA) CEP: 24.923-500 |
| Barra | Rua Francisco Ferreira da Costa, S/N, BARRA DE MARICÁ CEP: 24.915-428 |
| B | Bambuí | Estrada Antônio Calado, S/N BALNEÁRIO BAMBUÍ (PONTA NEGRA) Cep: 24.920-710 |
| CAXITO | Caxito | Rua Carmem Miranda, S/N. ITAPEBA CEP: 24.912-340 |
| Mumbuca | Rua Manoel Marins S/N, Mumbuca. CEP: 24.913-205 |
| C | Jardim Atlântico | Rua Van Lerberg, S/N (antiga rua 34) esquina com a rua Alice Maximino de Souza JARDIM ATLÂNTICO CENTRAL (ITAIPUAÇU) CEP: 24.934-165 |
| Santa Rita (Ponta Do Francês) | Rua Cento e Dezenove, S/N JARDIM ATLÂNTICO LESTE (ITAIPUAÇU) CEP: 24.933-150 |
| Jardim Atlântico / Cajueiro | Rua Hélio Guapyassu de Sá, JARDIM ATLÂNTICO CENTRAL (ITAIPUAÇU) CEP: 24.934-050 |
| Barroco | Rua João Toledo Gualberto, S/N BARROCO - ITAIPUAÇU CEP: 24.936-060 |
| Ponta Negra | Rua Vereador Alípio Manoel de Oliveira – S/N PONTA NEGRA (PONTA NEGRA) CEP: 24.922-268 |
| São José (I e II) | Rua Vinte e Dois, S/N (LOTO MAR) SÃO JOSÉ DE IMBASSAI - CEP: 24.931-375 |
| **Total** | **15** |
|  | Sede FEMAR | Rua Clímaco Pereira nº 367— Araçatiba — Maricá — RJ. 24.902-035 |
|  | Galpões | Rodovia Ernani do Amaral Peixoto, Km 37 – Manoel Ribeiro, – Maricá/RJ, CEP. 24.927-420 |

Maricá, 01 de abril de 2024.

**Responsáveis técnicos,**

|  |  |
| --- | --- |
| **Walter Matoso Rosa Junior**Assistente - Mat.: 3.300.352Superintendência de Infraestrutura Diretoria Administrativa | **Alessandra Lopes Rangel** Mat.: 3.300.020Superintendente de Infraestrutura Diretoria Administrativa |

**Conferido e de acordo,**

**Daniel Ferreira da Silva**

Mat.:3.300.002

Diretor Administrativo