

CONTRATO Nº 014 /2022/SCCC/ALMT

**CONTRATO QUE ENTRE SI
CELEBRAM A ASSEMBLEIA
LEGISLATIVA DO ESTADO DE
MATO GROSSO, ATRAVÉS DA
MESA DIRETORA E A EMPRESA
AVANT TECNOLOGIA E
INFORMÁTICA LTDA.**

A **ASSEMBLEIA LEGISLATIVA DO ESTADO DE MATO GROSSO**, doravante denominada **CONTRATANTE**, com sede no Centro Político Administrativo - Cuiabá-MT, inscrita no CNPJ sob nº 03.929.049/0001-11, na Avenida André Antônio Maggi, Lote 06, Setor A, Centro Político Administrativo - CPA, Edifício Governador Dante Martins de Oliveira, Cuiabá – MT., CEP 78049-901, Cuiabá – MT neste ato representado pelo Senhor Presidente Deputado Eduardo Botelho e o Primeiro Secretário, Ordenador de Despesas – Deputado Max Russi, e de outro lado à Empresa **AVANT TECNOLOGIA E INFORMÁTICA LTDA**, no CNPJ nº. 30.649.749/0001-25, com sede no SHC Norte, CL, Quadra 108, Bloco B, Lojas 46 e 50, CEP: 70.744-520, Brasília – DF., neste ato representada pelo Senhor Lucas Ribeiro Ganem, CNH nº. 00177279769, expedida pelo DETRAN/DF e CPF nº. 866.374.951-15, doravante denominada **CONTRATADA**, considerando o que consta no Processo Licitatório Pregão Eletrônico Registro de Preços nº 03/2022/ALMT (SGED. nº. 2021/1447.1397-5) e sujeitando-se, ainda, às normas da Lei nº 8.666, de 21 de junho de 1993 e suas alterações, e a Lei Complementar Federal nº 101, de 04 de maio de 2.000, demais normas que regem a espécie, **RESOLVEM** celebrar o presente contrato, nos seguintes termos e condições:

1/73

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O presente contrato tem por objeto a contratação de empresa especializada no fornecimento de soluções de TI, contemplando infraestrutura de rede de dados (switches), bem como serviços de instalação, configuração, migração, repasse de conhecimento, atualização e manutenção para atender as demandas da Assembleia Legislativa do Estado de Mato Grosso, conforme especificações do Termo de Referência nº 019/2021/STI, constante no Processo Licitatório Pregão Eletrônico Registro de Preços nº. 03/2022/ALMT (Protocolo SGED nº. 2021/1447.1397-5).

CLÁUSULA SEGUNDA – DA DESCRIÇÃO DA SOLUÇÃO, ESPECIFICAÇÕES TÉCNICAS, QUANTIDADES E PREÇOS PRATICADOS

2.1. As especificações técnicas dos itens que compõem o objeto deste Contrato, incluindo as normas e padrões de qualidade a serem observados, estão descritas na tabela abaixo:

Item	Descrição do item	Unidade	Quantidade	Valor Unitário	Valor Total
1	SWITCH TIPO 1 (32P 40/100 GBE)	UN	2	R\$ 279.900,00	R\$ 559.800,00
2	SWITCH TIPO 2 (48P 1/10/25 GBE + 4P 100 GBE)	UN	6	R\$ 244.890,00	R\$ 1.469.340,00
3	SWITCH TIPO 3 (48P 10/100/1000BASE-T POE + 4P 10 GBE)	UN	67	R\$32.820,00	R\$ 2.198.940,00
4	CABO UPLINK DAC/AOC QSFP28 100G 5M	UN	24	R\$ 4.300,00	R\$ 103.200,00
5	CABO DAC AOC 100G 10M	UN	8	R\$ 22.550,00	R\$ 180.400,00
6	CABO DAC AOC 25G 10M	UN	40	R\$ 4.100,00	R\$ 164.000,00
7	TRANSCEIVER SFP+ 10GBASE-SR	UN	320	R\$ 2.200,00	R\$ 704.000,00
8	SOLUÇÃO DE GERENCIAMENTO DOS ATIVOS DE REDE	UN	1	R\$ 39.900,00	R\$ 39.900,00
9	LICENÇA PARA GERENCIAMENTO DOS DISPOSITIVOS SWITCHS TIPO 1, 2 E 3	UN	75	R\$ 770,00	R\$ 57.750,00

2/73

10	LICENÇA PARA GERENCIAMENTO DOS DISPOSITIVOS PONTO DE ACESSO 1 E 2	UN	55	R\$ 789,00	R\$ 43.395,00
11	PONTO DE ACESSO INDOOR TIPO 1	UN	40	R\$ 5.590,00	R\$ 223.600,00
12	PONTO DE ACESSO INDOOR TIPO 2	UN	15	R\$ 8.300,00	R\$ 124.500,00
13	FONTE DE ALIMENTAÇÃO POE	UN	30	R\$ 270,00	R\$ 8.100,00
14	INSTALAÇÃO FÍSICA E CONFIGURAÇÃO BÁSICA	SERVIÇO	75	R\$ 2.870,00	R\$ 215.250,00
15	OPERAÇÃO ASSISTIDA	SERVIÇO	1	R\$ 890.000,00	R\$ 890.000,00
16	TREINAMENTO PARA TURMA DE 10 (DEZ) ALUNOS	SERVIÇO	1	R\$ 69.000,00	R\$ 69.000,00
Valor Total dos Itens: R\$ 7.051.175,00 (sete milhões, cinquenta e um mil e cento e setenta e cinco reais)					

2.3. O valor global do presente contrato é de **R\$ 7.051.175,00 (sete milhões, cinquenta e um mil e cento e setenta e cinco reais).**

CLÁUSULA TERCEIRA – DOS RECURSOS ORÇAMENTÁRIOS

3.1. As despesas decorrentes do presente procedimento licitatório correrão pela dotação orçamentária – Exercício de 2022 da Assembleia Legislativa do Estado de Mato Grosso, a seguir:

	Número	Histórico
Reduzida	36	-
Projeto/Atividade	2.009	Manutenção de Ações de Informática
Elemento de Despesa	3.3.90.39.00.00	Outros Serviços de Terceiros – Pessoa Jurídica
Fonte de Recurso	100	Recursos do Tesouro - Ordinários

3.2. No(s) exercício(s) seguinte(s), as despesas correspondentes correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

3/73

CLÁUSULA QUARTA – DOS PRAZOS DE VIGÊNCIA E EXECUÇÃO

4.1. O presente Instrumento de Contrato terá a vigência de 12 (doze) meses, a contar da data de sua assinatura, tendo validade e eficácia legal após a publicação de seu extrato no Diário Oficial Eletrônico da ALMT.

4.2. A **CONTRATANTE** providenciará a publicação do presente Contrato, em extrato, no Diário Oficial Eletrônico da Assembleia Legislativa do Estado de Mato Grosso, conforme determina o Parágrafo Único, do artigo 61, da Lei nº 8.666/93.

CLÁUSULA QUINTA – DAS CONDIÇÕES DE FORNECIMENTO E RECEBIMENTO DO OBJETO

5.1. A **CONTRATADA** deverá entregar os produtos conforme cronograma abaixo, sendo que os prazos estabelecidos serão contados a partir da data de assinatura do Contrato:

Etapa	Descrição	Prazo em dias
1	Entrega dos equipamentos	45 dias
2	Instalação e entrega do termo de garantia	15 dias (após entrega dos equipamentos)

5.2. O fornecimento deverá ser realizado das 08h00min às 12h00min e das 14h00min às 18h00min, de segunda à sexta-feira.

5.3. A **CONTRATADA** deverá fornecer o objeto em estrita conformidade com disposições e especificações do edital da licitação, de acordo com o Contrato, Termo de Referência e a proposta de preços apresentada.

5.4. A entrega do objeto será na forma do cronograma de execução, definido no Item 5.1.

5.5. Todo o equipamento e/ou material fornecido deverá estar acondicionado em embalagens apropriada, e em perfeitas condições de armazenamento e uso, de forma que garanta a sua integridade e não sejam danificados durante as operações de transporte, carga e descarga, conforme determina a Legislação vigente, podendo, os produtos serem devolvidos sem quaisquer ônus ao município, caso as exigências não sejam atendidas.

5.6. Os produtos deverão estar de acordo com as exigências do Código de Defesa do Consumidor, especialmente no tocante aos vícios de qualidade ou quantidade que os tomem impróprios ou inadequados ao uso a que se destinam ou lhes diminuam o valor, conforme diploma legal.

4/73

5.7. No ato da entrega, os materiais serão analisados em sua totalidade, sendo que aquele(s) que não satisfazer(em) à especificação exigida ser(ão) devolvido(s) à **CONTRATADA**.

5.8. Verificada alguma falha no fornecimento, a **CONTRATADA** obriga-se a reparar, corrigir, remover, reconstruir, ou substituir, os produtos entregues e não aceitos pelo **CONTRATANTE**, em função da existência de irregularidades, incorreções, no prazo de 48 (quarenta e oito) horas, contados da notificação que lhe for entregue oficialmente, sem ônus adicional para a **CONTRATANTE**, sem o que será convocada a segunda classificada, sem prejuízo da aplicação das sanções previstas nos artigos 86 a 88 da Lei 8.666/93 e artigos 20 e 56 a 80 do Código de Defesa do Consumidor.

5.9. O objeto deste Contrato será entregue na Secretaria de Tecnologia da Informação – Edifício Dante Martins de Oliveira, Piso Térreo, Avenida André Antônio Maggi, Lote 06, Setor A, CPA, CEP 78049-901 – Cuiabá, Mato Grosso, Brasil, das 08h00min às 12h00min e das 14h00min às 18h00min, de segunda à sexta-feira, com “pré-agendamento” pelo telefone (65) 3313-6450.

5.10. O objeto deste Contrato será recebido e avaliado com o escopo de verificar sua conformidade quanto à quantidade, qualidade e especificações descritas e nos termos dos artigos 69 e 73 a 76 da Lei n.º 8.666, de 21 de junho de 1993 e suas alterações, da seguinte forma:

5.10.1. **Provisório**, rigorosamente conforme descrito na especificação, deste Contrato, conforme o quantitativo da Nota de Empenho e Requisição (Nota de Autorização de Despesa), dentro do prazo estabelecido pela Assembleia Legislativa do Estado de Mato Grosso.

a) O Almoxarifado da Secretaria de Tecnologia da Informação da **CONTRATANTE**, limitar-se-á a verificar a sua conformidade com o discriminado na Nota Fiscal, fazendo constar na mesma a data de recebimento dos equipamentos e, se for o caso, as irregularidades observadas;

b) A simples assinatura do servidor em canhoto de fatura ou conhecimento de transporte implica apenas recebimento provisório.

5.10.2. **Definitivo**, no prazo de até 05 (cinco) dias corridos, contados a partir do recebimento provisório, um servidor designado pela **CONTRATANTE**, como Gestor e/ou Fiscal do Contrato, procederá ao recebimento definitivo, verificando a quantidade e a conformidade com o exigido neste Contrato, no Termo de Referência, Edital e com o constante na respectiva proposta de preço da licitante vencedora.

5.11. Em caso de divergência entre as quantidades, dimensões e qualidades, a fiscalização, sob consulta prévia, definirá o procedimento correto.

5/73

- a) Caso satisfatório as verificações deste inciso, o servidor atestará a efetivação da entrega do serviço ou material na Nota Fiscal e a encaminhará a Secretaria de Planejamento, Orçamento e Finanças, para fins de pagamento;
- b) Caso insatisfatório as verificações, o material deverá ser substituído, no prazo de até 10 (dez) dias contados da comunicação formal desta Administração;
- c) Caso a substituição não ocorra no prazo acima determinado, ou caso o novo material também seja rejeitado, estará à contratada incorrendo em atraso na entrega, sujeita à aplicação de penalidades;
- d) Os custos de substituição do produto rejeitado correrão exclusivamente a expensas da **CONTRATADA**.

5.12. Não será definitivamente recebido e, conseqüentemente, será colocado à disposição do fornecedor, o objeto que não for compatível com as características exigidas neste Contrato e no Termo de Referência, ou ainda, que apresente qualquer tipo de avaria e/ou falha.

5.13. A **CONTRATADA** deverá, obrigatoriamente, entregar os materiais em sua totalidade para cada localidade solicitada, não sendo admitido objeto incompleto ou parcelado, sob pena das sanções legais cabíveis.

5.14. O objeto deverá observar as discriminações contidas neste Contrato, sem defeitos ou avarias, sendo aplicadas todas as normas e exigências do Código de Defesa do Consumidor.

5.15. O aceite do objeto pelo setor competente da **CONTRATANTE** não exclui a responsabilidade do fornecedor por vícios de qualidade ou técnicos, aparentes ou ocultos, ou por desacordo com as especificações estabelecidas neste Contrato, e verificadas posteriormente.

5.16. Demais condições de fornecimento (omissas na ata de registro de preços, no termo de referência, e neste contrato) deverão estar de acordo com o que prevê o código do consumidor.

5.17. A **CONTRATANTE** não caberá qualquer ônus pela rejeição dos produtos ou serviços considerados inadequados ou em desconformidade com a especificação registrada neste Contrato.

5.18. O prazo de entrega do produto poderá ser prorrogado, desde que devidamente justificado o motivo, nos termos do art. 57, §1º e seus incisos, da Lei n.º 8.666/1993.

5.19. Após recebidos, os objetos serão conferidos pelo setor competente. Se constatada qualquer irregularidade, a empresa deverá substituí-los, no prazo máximo de 10 (dez) dias, a contar do recebimento da notificação formal emitida pela **CONTRATANTE**.

5.20. Em caso de divergência entre as quantidades, dimensões e qualidades, a fiscalização, sob consulta prévia, definirá o procedimento correto, com a devida aprovação e autorização da Secretaria de Tecnologia da Informação.

CLÁUSULA SEXTA – DO SWITCH TIPO 1 (32P 40/100 GBE)**6.1. CARACTERÍSTICAS GERAIS:**

- 6.1.1. Deve permitir instalação em rack de 19” padrão Telco EIA;
- 6.1.2. Deve possuir altura máxima 1 (um) *rack unit* (RU);
- 6.1.3. Deve possuir fonte de alimentação interna, do tipo *auto-sense*, para operar de 100 a 240 VAC;
- 6.1.4. Deve possuir fonte de alimentação redundante interna e hot-swappable;
- 6.1.5. Deve possuir capacidade de processamento igual ou superior a 2.000 (dois mil) Mpps;
- 6.1.6. Deve possuir capacidade de *switching* igual ou superior a 6.400 (seis mil e quatrocentos) Gbps;
- 6.1.7. Deve possuir latência média de, no mínimo, 0,8 microssegundos.
- 6.1.8. Deve possuir, no mínimo, 32 (trinta e duas) portas 40/100GbE utilizando QSFP+/QSFP28;
- 6.1.9. Todas as portas 40/100GbE devem permitir operação em modo *breakout* 4x10GbE ou 4x25GbE.
- 6.1.10. Deve ser compatível com QSFP+ 40GBASE-SR4, 40GBASE-LR4 e 40G-BiDi;
- 6.1.11. Deve ser compatível com QSFP28 100GBASE-SR4, 100GBASE-LR4 e 100GBASE-CWDM4;
- 6.1.12. Deve possuir pelo menos 32MB de buffer de pacotes;
- 6.1.13. Deve possuir, no mínimo, 4GB de memória DRAM e 32GB de memória NVRAM (flash);
- 6.1.14. Deve permitir empilhamento de até 09 (nove) unidades outros equipamentos em topologia linear e em anel, e permitir gerenciar a pilha com um único endereço IP;
- 6.1.15. Deve possuir banda agregada de empilhamento mínima de 800 (quatrocentos) Gbps, podendo ser através de 4 (duas) portas de 100 (cem) Gbps operando em full-duplex;

7/73

6.1.16. As interfaces de empilhamento podem ser compartilhadas com as 32 (trinta e duas) portas 40/100GbE supracitadas;

6.1.17. O equipamento deve permitir empilhamento através de cabos de fibra óptica com distância de pelo menos 10 (dez) km entre cada uma das unidades da pilha;

6.1.18. Deve possuir ventilação *front to back*, isto é, o fluxo de ar deve seguir no sentido das portas de interface para as fontes de energia;

6.1.19. Deve suportar a inversão do fluxo de ar de ventilação para o modo “*back to front*” através de pelo menos um dos seguintes métodos: troca de ventiladores e fontes, atualização de firmware ou alteração do arquivo de configuração.

6.1.20. Deve possuir porta de gerenciamento “out-of-band” operando a 10/100/1000 Mbps;

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

6.1.22. Possui slot USB para inserção de uma mídia de armazenamento removível para fazer upgrade de imagem do switch e backup da configuração;

6.1.23. Deve possuir LEDs indicativos de energização, status de slot USB, atividade do link e velocidade das portas;

6.1.24. Deve possuir LED de indicação de atividade, velocidade das portas mesmo em modo *breakout* de forma individual de cada “*lane*”;

6.1.25. Deve permitir realizar troubleshooting visual da unidade na pilha, identificando através de LEDs se o switch é master ou *slave* da pilha, e sua identificação na pilha;

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

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

6.1.28. A **CONTRATADA** deve apresentar carta oficial de revenda autorizada pelo fabricante do equipamento ofertado;

6.1.29. A proposta comercial deve discriminar o fabricante e o modelo do equipamento ofertado bem como seus respectivos “P/Ns”;

6.1.30. Deve ser novo e em plena fabricação. Não serão aceitos equipamentos com avisos de “End of Life” emitidos pelo fabricante;

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

8/73

6.2. FUNÇÕES DE CAMADA 2:

6.2.1. Deve suportar capacidade de no mínimo 290.000 (duzentos mil) endereços MAC;

6.2.2. Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad. Deve permitir a configuração de pelo menos 250 (duzentos e cinquenta) grupos de LACP com pelo menos 16 (dezesseis) portas dentro de um mesmo grupo;

6.2.3. Deve permitir a configuração de grupos de portas agregadas (*LAGs*) com balanceamento simétrico, garantindo que o tráfego de um mesmo origem e destino passe pela mesma porta de um LAG de forma bidirecional;

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

6.2.5. Deve implementar o protocolo IEEE 802.1s (*Multiple Spanning Tree*), IEEE 802.1w (*Rapid Spanning Tree*) e IEEE 802.1D (*Spanning Tree*);

6.2.6. Deve ser compatível com o protocolo PVST+;

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

6.2.8. Deve implementar BPDU Guard e Root Guard;

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

6.2.10. Deve permitir a criação VLANs privadas;

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

6.2.12. Deve implementar selective QinQ;

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

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

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

6.2.16. Deve implementar VPC (*Virtual Port Channel*), MCT (*Multi-Chassis Trunk*) ou funcionalidade similar que permita a formação de grupos de portas agregadas com o

9/73

protocolo IEEE 802.3ad utilizando simultaneamente portas locais e portas de outro equipamento idêntico;

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

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

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

6.2.20. Deve implementar MLD *snooping* v1 e v2;

6.2.21. Deve implementar MVRP (*Multiple VLAN Registration Protocol*);

6.2.22. Deve possuir funcionalidade de refletir a tráfego de entrada de uma porta Ethernet, retornando para um gerador de teste para permitindo medir a continuidade da rede e o desempenho da porta ethernet;

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

6.2.24. Deve implementar VXLAN;

6.2.25. Deve implementar *Precision Timing Protocol (PTP) Transparent Clock* baseado no padrão IEEE1588v2;

6.3. FUNÇÕES DE CAMADA 3:

6.3.1. Deve permitir roteamento local entre VLANs utilizando interfaces virtuais ou SVIs;

6.3.2. Deve permitir a configuração de rotas estáticas usando endereços IPv4 e IPv6;

6.3.3. Deve permitir a configuração de endereço IPv6 com prefixo de 127 bits para links point-to-point;

6.3.4. Deve implementar roteamento IP usando os protocolos RIPv1/v2 e RIPng;

6.3.5. Deve implementar roteamento IP usando os protocolos OSPFv2 e OSPFv3;

6.3.6. Deve implementar roteamento usando o protocolo BGP4 e BGP4+;

6.3.7. Deve implementar BFD (*bidirectional forwarding detection*) para rotas estáticas, OSPFv2, OSPFv3, BGP4 e BGP4+;

6.3.8. Deve implementar criação de túneis GRE;

10/73

6.3.9. Deve implementar VRF ou VRF-lite, com suporte a pelo menos 128 (cento e vinte e oito) instâncias;

6.3.10. Deve implementar os protocolos VRRP e VRRPv3;

6.3.11. Deve implementar ECMP com no mínimo 32 (trinta e dois) caminhos;

6.3.12. Deve implementar os protocolos de roteamento de *multicast* PIM-S, PIM-SSM e PIM-DM;

6.3.13. Deve suportar PIM-Passive para reduzir e minimizar tráfego de controle.

6.3.14. Deverá possuir no mínimo 500 (quinhentas) interfaces virtuais para roteamento entre VLANs

6.3.15. Deve suportar a configuração de pelo menos 2.000 (duas mil) rotas estáticas IPv4;

6.3.16. Deve suportar a configuração de pelo menos 1.000 (mil) rotas estáticas IPv6;

6.3.17. Deverá suportar a capacidade pelo menos 300.000 (trezentas mil) entradas em sua tabela de roteamento IPv4;

6.3.18. Deverá suportar a capacidade de pelo menos 35.000 (trinta e cinco mil) entradas em sua tabela de roteamento IPv6;

6.3.19. Deve implementar DHCP Server para IPv4 e IPv6;

6.3.20. Deve permitir a configuração de DHCP Relay;

6.3.21. Deve implementar PBR (*Policy-Based Routing*) para IPv4 e IPv6;

6.3.22. Deve implementar IPv6 *router advertisement* (RA) *preference* na mensagem de RA com informações de múltiplos roteadores para a escolher a rota default apropriada pelo host IPv6;

6.4. QUALIDADE DE SERVIÇO:

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

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

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

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

11/73

6.4.5. Deve permitir a configuração de *Rate Limiting* de entrada;

6.4.6. Deve permitir a configuração de *Rate Shaping* de saída;

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

6.5. SEGURANÇA:

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

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

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

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

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

6.5.5.1. 02 (dois) dispositivos que suportam o padrão IEEE 802.1x;

6.5.5.2. 02 (dois) dispositivos MAC que não suportam o padrão IEEE 802.1x;

6.5.5.3. 01 (um) dispositivo que suporta o padrão IEEE 802.1x e 1 (um) dispositivo MAC que não suporta o padrão IEEE 802.1x;

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

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

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

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

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

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

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

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

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

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

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

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

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

6.5.19. Deve permitir a configuração de *Dynamic ARP Inspection* em pelo menos 500 vlans;

6.5.20. Deve implementar IP *Source Guard*;

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

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

6.5.23. Deve implementar IPv6 RA guard e IPv6 ND *inspection*;

6.5.24. Deve implementar RADsec conforme RFC6614;

6.5.25. Deve implementar *unicast Reverse Path Forwarding* (uRPF) como ferramenta para evitar ataques do tipo source IP spoofing;

6.6. GERENCIAMENTO:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.6.15. Deve implementar o protocolo OpenFlow 1.3 com suporte para portas híbridas em Camada 2 e Camada 3;

- 6.6.16.** Deve permitir o monitoramento de tráfego através dos protocolos sFlow, NetFlow ou IPFIX. Deve ser possível exportar o tráfego de redes IPv4 e IPv6;
- 6.6.17.** Deve permitir a configuração de seu relógio interno de forma automática através do protocolo NTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
- 6.6.18.** Deve permitir armazenamento simultâneo de duas imagens de firmware em memória flash.
- 6.6.19.** Deve permitir atualização de imagem de firmware através de mídia de armazenamento externa conectado ao slot USB;
- 6.6.20.** Deve permitir o envio de mensagens de *syslog* à pelo menos 2 servidores distintos. Deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
- 6.6.21.** Deve permitir o envio de *syslog* com formato conforme RF5424 para prover mais informações no seu header;
- 6.6.22.** Deve possuir suporte a automação com Ansible.

CLÁUSULA SÉTIMA – DO SWITCH TIPO 2 (48P 1/10/25 + 4P 100 GBE)
--

7.1. CARACTERÍSTICAS GERAIS:

- 7.1.1.** Deve permitir instalação em rack de 19” padrão Telco EIA;
- 7.1.2.** Deve possuir altura máxima 1 (um) *rack unit* (RU);
- 7.1.3.** Deve possuir fonte de alimentação interna, do tipo *auto-sense*, para operar de 100 a 240 VAC;
- 7.1.4.** Deve possuir fonte de alimentação redundante interna e *hot-swappable*;
- 7.1.5.** Deve possuir capacidade de processamento igual ou superior a 2000 (dois mil) Mpps;
- 7.1.6.** Deve possuir capacidade de *switching* igual ou superior a 4000 (quatro mil) Gbps;
- 7.1.7.** Deve possuir latência média de, no mínimo, 0,8 microssegundos.
- 7.1.8.** Deve possuir, no mínimo, 48 (quarenta e oito) interfaces 1/10/25GbE compatíveis com SFP, SFP+ e SFP28 usando conectores LC;
- 7.1.9.** Deve possuir, no mínimo, 08 (oito) portas 40/100GbE utilizando QSFP+/QSFP28;

15/73

- 7.1.10. Todas as portas 40/100GbE devem permitir operação em modo breakout 4x10GbE ou 4x25GbE.
- 7.1.11. Deve ser compatível com SFP 1000BASE-SX, 1000BASE-LX e 1000Base-T;
- 7.1.12. Deve ser compatível com SFP+ 10GBASE-SR, 10GBASE-LR, 10GBASE-ER;
- 7.1.13. Deve ser compatível com SFP28 25GBASE-SR, 25GBASE-LR;
- 7.1.14. Deve ser compatível com QSFP+ 40GBASE-SR4, 40GBASE-LR4 e 40G-BiDi;
- 7.1.15. Deve ser compatível com QSFP28 100GBASE-SR4, 100GBASE-LR4 e 100GBASE-CWDM4;
- 7.1.16. Deve possuir pelo menos 32MB de buffer de pacotes;
- 7.1.17. Deve possuir, no mínimo, 4GB de memória DRAM e 32GB de memória NVRAM (flash);
- 7.1.18. Deve permitir empilhamento de até 9 (nove) unidades outros equipamentos em topologia linear e em anel, e permitir gerenciar a pilha com um único endereço IP;
- 7.1.19. Deve possuir banda agregada de empilhamento mínima de 800 (quatrocentos) Gbps, podendo ser através de 4 (duas) portas de 100 (cem) Gbps operando em full-duplex;
- 7.1.20. As interfaces de empilhamento podem ser compartilhadas com as 8 (oito) portas 40/100GbE supracitadas;
- 7.1.21. O equipamento deve permitir empilhamento através de cabos de fibra óptica com distância de pelo menos 10 (dez) km entre cada uma das unidades da pilha;
- 7.1.22. Deve possuir ventilação *front to back*, isto é, o fluxo de ar deve seguir no sentido das portas de interface para as fontes de energia;
- 7.1.23. Deve suportar a inversão do fluxo de ar de ventilação para o modo “*back to front*” através de pelo menos um dos seguintes métodos: troca de ventiladores e fontes, atualização de firmware ou alteração do arquivo de configuração;
- 7.1.24. Deve possuir porta de gerenciamento “out-of-band” operando a 10/100/1000 Mbps;
- 7.1.25. Deve possuir porta de console para gerenciamento utilizando conector RJ-45, USB, mini-USB ou USB Tipo C;
- 7.1.26. Possui slot USB para inserção de uma mídia de armazenamento removível para fazer upgrade de imagem do switch e backup da configuração;

7.1.27. Deve possuir LEDs indicativos de energização, status de slot USB, atividade do link e velocidade das portas;

7.1.28. Deve possuir LED de indicação de atividade, velocidade das portas mesmo em modo *breakout* de forma individual de cada “lane”;

7.1.29. Deve permitir realizar troubleshooting visual da unidade na pilha, identificando através de LEDs se o switch é master ou *slave* da pilha, e sua identificação na pilha;

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

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

7.1.32. O proponente deve apresentar carta oficial de revenda autorizada pelo fabricante do equipamento ofertado;

7.1.33. A proposta comercial deve discriminar o fabricante e o modelo do equipamento ofertado bem como seus respectivos “P/Ns”;

7.1.34. Deve ser novo e em plena fabricação. Não serão aceitos equipamentos com avisos de “End of Life” emitidos pelo fabricante;

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

7.2. FUNÇÕES DE CAMADA 2:

7.2.1. Deve suportar capacidade de no mínimo 290.000 (duzentos mil) endereços MAC;

7.2.2. Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad. Deve permitir a configuração de pelo menos 250 (duzentos e cinquenta) grupos de LACP com pelo menos 16 (dezesesseis) portas dentro de um mesmo grupo;

7.2.3. Deve permitir a configuração de grupos de portas agregadas (LAGs) com balanceamento simétrico, garantindo que o tráfego de um mesmo origem e destino passe pela mesma porta de um LAG de forma bidirecional;

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

7.2.5. Deve implementar o protocolo IEEE 802.1s (Multiple Spanning Tree), IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1D (*Spanning Tree*);

7.2.6. Deve ser compatível com o protocolo PVST+;

17/73

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

7.2.8. Deve implementar BPDU Guard e Root Guard;

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

7.2.10. Deve permitir a criação VLANs privadas;

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

7.2.12. Deve implementar *selective QinQ*;

7.2.13. Deve implementar para o protocolo UDLD (*Uni-Directional Link Detection*) ou DLDLP (*Device Link Detection Protocol*) ou similar;

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

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

7.2.16. Deve implementar VPC (*Virtual Port Channel*), MCT (*Multi-Chassis Trunk*) ou funcionalidade similar que permita a formação de grupos de portas agregadas com o protocolo IEEE 802.3ad utilizando simultaneamente portas locais e portas de outro equipamento idêntico;

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

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

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

7.2.20. Deve implementar MLD *snooping* v1 e v2;

7.2.21. Deve implementar MVRP (*Multiple VLAN Registration Protocol*);

7.2.22. Deve possuir funcionalidade de refletir a tráfego de entrada de uma porta Ethernet, retornando para um gerador de teste para permitindo medir a continuidade da rede e o desempenho da porta ethernet;

18/73

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

7.2.24. Deve implementar VXLAN;

7.2.25. Deve implementar *Precision Timing Protocol* (PTP) *Transparent Clock* baseado no padrão IEEE1588v2;

7.3. FUNÇÕES DE CAMADA 3:

7.3.1. Deve permitir roteamento local entre VLANs utilizando interfaces virtuais ou SVIs;

7.3.2. Deve permitir a configuração de rotas estáticas usando endereços IPv4 e IPv6;

7.3.3. Deve permitir a configuração de endereço IPv6 com prefixo de 127 bits para links point-to-point;

7.3.4. Deve implementar roteamento IP usando os protocolos RIPv1/v2 e RIPv6;

7.3.5. Deve implementar roteamento IP usando os protocolos OSPFv2 e OSPFv3;

7.3.6. Deve implementar roteamento usando o protocolo BGP4 e BGP4+;

7.3.7. Deve implementar BFD (*bidirectional forwarding detection*) para rotas estáticas, OSPFv2, OSPFv3, BGP4 e BGP4+;

7.3.8. Deve implementar criação de túneis GRE;

7.3.9. Deve implementar VRF ou VRF-lite, com suporte a pelo menos 128 (cento e vinte e oito) instâncias;

7.3.10. Deve implementar os protocolos VRRP e VRRPv3;

7.3.11. Deve implementar ECMP com no mínimo 32 (trinta e dois) caminhos;

7.1.12. Deve implementar os protocolos de roteamento de *multicast* PIM-S, PIM-SSM e PIM-DM;

7.3.13. Deve suportar PIM-Passive para reduzir e minimizar tráfego de controle.

7.3.14. Deverá possuir no mínimo 500 (quinhentas) interfaces virtuais para roteamento entre VLANs

7.3.15. Deve permitir a configuração de pelo menos 2.000 (duas mil) rotas estáticas IPv4;

7.3.16. Deve permitir a configuração de pelo menos 1.000 (mil) rotas estáticas IPv6;

7.3.17. Deverá suportar a capacidade pelo menos 300.000 (trezentas mil) entradas em sua tabela de roteamento IPv4;

19/73

7.3.18. Deverá suportar a capacidade de pelo menos 35.000 (trinta e cinco mil) entradas em sua tabela de roteamento IPv6;

7.3.19. Deve possuir DHCP Server para IPv4 e IPv6;

7.3.20. Deve permitir a configuração de DHCP Relay;

7.3.21. Deve implementar PBR (*Policy-Based Routing*) para IPv4 e IPv6;

7.3.22. Deve implementar IPv6 *router advertisement* (RA) *preference* na mensagem de RA com informações de múltiplos roteadores para a escolher a rota default apropriada pelo host IPv6;

7.4. QUALIDADE DE SERVIÇO:

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

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

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

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

7.4.5. Deve permitir a configuração de *Rate Limiting* de entrada;

7.4.6. Deve permitir a configuração de *Rate Shaping* de saída;

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

7.5. SEGURANÇA:

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

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

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

20/73

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

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

7.5.5.1. 02 (dois) dispositivos que suportam o padrão IEEE 802.1x;

7.5.5.2. 02 (dois) dispositivos MAC que não suportam o padrão IEEE 802.1x;

7.5.5.3. 01 (um) dispositivo que suporta o padrão IEEE 802.1x e 1 (um) dispositivo MAC que não suporta o padrão IEEE 802.1x;

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

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

7.5.8. Deve implementar "Change of Authorization" de acordo com a RFC 5176;

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

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

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

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

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

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

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

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

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

21/73

- 7.5.18. Deve possuir funcionalidade de proteção contra-ataques do tipo “ARP Poisoning”;
- 7.5.19. Deve permitir a configuração de *Dynamic ARP Inspection* em pelo menos 500 vlans;
- 7.5.20. Deve implementar *IP Source Guard*;
- 7.5.21. Deve implementar proteção contra-ataques do tipo TCP SYN e ataques do tipo Smurf;
- 7.5.22. Deve permitir o monitoramento da movimentação de um endereço MAC de uma porta para outra, facilitando a distinção entre um movimento legítimo com um movimento malicioso de um ataque de *MAC spoofing*;
- 7.5.23. Deve implementar IPv6 RA guard e IPv6 ND inspection;
- 7.5.24. Deve implementar RADsec conforme RFC6614;
- 7.5.25. Deve implementar *unicast Reverse Path Forwarding* (uRPF) como ferramenta para evitar ataques do tipo *source IP spoofing*;

7.6. GERENCIAMENTO:

- 7.6.1. Deve permitir monitoração e configuração usando SNMP v1, v2 e v3;
- 7.6.2. Deve permitir o gerenciamento via SNMPv3 com as seguintes opções: sem autenticação e sem privacidade, com autenticação e sem privacidade e com autenticação e com privacidade;
- 7.6.3. Deve ser possível enviar “traps” e realizar o gerenciamento via SNMP através das redes IPv4 e IPv6;
- 7.6.4. Deve permitir a configuração de porta para espelhamento de tráfego, para a coleta de pacotes em analisadores de protocolo ou detecção de intrusão;
- 7.6.5. Deve permitir espelhamento de tráfego baseado em Porta, VLAN, Filtro MAC e ACL;
- 7.6.6. Deve permitir a configuração de porta para espelhamento de tráfego para uma porta em um switch remoto;
- 7.6.7. Deve implementar gerenciamento usando SSH v2 utilizando os algoritmos de criptografia 3DES e AES. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;
- 7.6.8. Deve implementar gerenciamento via Telnet. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;
- 7.6.9. Deve implementar pelo menos 4 (quatro) grupos de RMON;

22/73

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

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

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

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

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

7.6.15. Deve implementar o protocolo OpenFlow 1.3 com suporte para portas híbridas em Camada 2 e Camada 3;

7.6.16. Deve permitir o monitoramento de tráfego através dos protocolos sFlow, NetFlow ou IPFIX. Deve ser possível exportar o tráfego de redes IPv4 e IPv6;

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

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

7.6.19. Deve permitir atualização de imagem de firmware através de mídia de armazenamento externa conectado ao slot USB;

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

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

7.6.22. Deve possuir suporta a automação com Ansible.

CLÁUSULA OITAVA – DO SWITCH TIPO 3 (48P 10/100/1000BASE-T POE + 4P 10 GBE)**8.1. CARACTERÍSTICAS GERAIS:**

- 8.1.1. Deve permitir instalação em rack de 19” padrão Telco EIA;
- 8.1.2. Deve possuir altura máxima 1 (um) *rack unit* (RU);
- 8.1.3. Deve possuir fonte de alimentação interna, do tipo *auto-sense*, para operar de 100 a 240 VAC;
- 8.1.4. Deve possuir 48 (quarenta e oito) portas 10/100/1000 Mbps, usando conectores RJ-45;
- 8.1.5. As portas 10/100/1000 BASE-T devem ser do tipo MDI/MDIX automático;
- 8.1.6. Deve possuir, no mínimo, 4 (quatro) portas 1/10 Gbps SFP/SFP+, as quais não devem operar em modo “combo” com as portas 10/100/1000 BASE-T em par trançado;
- 8.1.7. Deve possuir capacidade de processamento igual ou superior a 130 (cento e trinta) Mpps;
- 8.1.8. Deve possuir capacidade de *switching* igual ou superior a 180 (cento e oitenta) Gbps;
- 8.1.9. Deve possuir, pelo menos, 4 MB de buffers de pacotes;
- 8.1.10. Deve possuir, pelo menos, 1 GB de memória DRAM;
- 8.1.11. Deve possuir, pelo menos, 2 GB de memória flash;
- 8.1.12. Deve implementar os protocolos IEEE 802.3af Power over Ethernet (PoE) e IEEE 802.3at Power over Ethernet Plus (PoE+);
- 8.1.13. Deve possuir PoE *power* budget de pelo menos 370 (trezentos e setenta) watts;
- 8.1.14. Deve ser do tipo *fanless* ou permitir operação com os ventiladores internos desligados;
- 8.1.15. Deve permitir empilhamento de até 9 (nove) unidades outros equipamentos em topologia linear e em anel;
- 8.1.16. Deve permitir o empilhamento com switches de 12 portas, switches 24 portas, switches multi-gigabit e switches PoE+ e permitir o gerenciar a pilha com um único endereço IP;

24/73

8.1.17. Deve suportar banda agregada de empilhamento de no mínimo 80Gbps full-duplex, podendo ser através de agregação de portas de 10G. Essas portas podem ser formadas pelas portas do item 8.1.6.;

8.1.18. O equipamento deve permitir empilhamento através de cabos de fibra óptica com distância de pelo menos 10 (dez) km entre cada uma das unidades da pilha;

8.1.19. Deve possuir porta de gerenciamento “out-of-band” operando a 10/100/1000 Mbps;

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

8.1.21. Possui slot USB para inserção de uma mídia de armazenamento removível para fazer upgrade de imagem do switch e backup da configuração;

8.1.22. Deve possuir LEDs indicativos de energização, status de slot USB, atividade do link e velocidade das portas;

8.1.23. Deve permitir realizar troubleshooting visual da unidade na pilha, identificando através de LEDs se o switch é master ou *slave* da pilha, e sua identificação na pilha;

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

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

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

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

8.2. FUNÇÕES DE CAMADA 2:

8.2.1. Deve possuir capacidade de no mínimo 16.000 (dezesseis mil) endereços MAC;

8.2.2. Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad. Deve permitir a configuração de pelo menos 120 (cento e vinte) grupos de LACP com pelo menos 8 (oito) portas dentro de um mesmo grupo;

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

8.2.4. Deve implementar o protocolo IEEE 802.1s (*Multiple Spanning Tree*), IEEE 802.1w (*Rapid Spanning Tree*) e IEEE 802.1D (*Spanning Tree*);

8.2.5. Deve ser compatível com o protocolo PVST+;

25/73

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

8.2.7. Deve implementar BPDU Guard e Root Guard;

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

8.2.9. Deve permitir a criação VLANs privadas;

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

8.2.11. Deve implementar selective QinQ;

8.2.12. Deve implementar para o protocolo UDLD (*Uni-Directional Link Detection*) ou DLDLP (*Device Link Detection Protocol*) ou similar;

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

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

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

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

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

8.2.18. Deve implementar MLD *snooping* v1 e v2;

8.2.19. Deve implementar MVRP (Multiple VLAN Registration Protocol);

8.2.20. Deve possuir funcionalidade de refletir a tráfego de entrada de uma porta Ethernet, retornando para um gerador de teste para permitindo medir a continuidade da rede e o desempenho da porta ethernet;

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

8.3. FUNÇÕES DE CAMADA 3:

8.3.1. Deve permitir roteamento local entre VLANs utilizando interfaces virtuais ou SVIs;

26/73

- 8.3.2. Deve permitir a configuração de rotas estáticas usando endereços IPv4 e IPv6;
- 8.3.3. Deve permitir a configuração de endereço IPv6 com prefixo de 127 bits para links *point-to-point*;
- 8.3.4. Deve implementar roteamento IP usando os protocolos RIPv1/v2 e RIPv6;
- 8.3.5. Deve implementar roteamento IP usando os protocolos OSPFv2 e OSPFv3;
- 8.3.6. Deve implementar os protocolos VRRP e VRRPv3;
- 8.3.7. Deve implementar ECMP com no mínimo 8 caminhos;
- 8.3.8. Deve implementar os protocolos de roteamento de multicast PIM-S, PIM-SSM e PIM-DM;
- 8.3.9. Deve suportar PIM-Passive para reduzir e minimizar tráfego de controle.
- 8.3.10. Deverá possuir no mínimo 350 (trezentos e cinquenta) interfaces virtuais para roteamento entre VLANs
- 8.3.11. Deve permitir a configuração de pelo menos 500 (quinhentas) rotas estáticas IPv4;
- 8.3.12. Deve permitir a configuração de pelo menos 500 (quinhentas) rotas estáticas IPv6;
- 8.3.13. Deverá suportar a capacidade de pelo menos 1.000 (mil) entradas na sua tabela de IPv4;
- 8.3.14. Deverá suportar a capacidade de pelo menos 1.000 (mil) entradas em sua tabela de roteamento IPv6;
- 8.3.15. Deve possuir DHCP Server para IPv4 e IPv6;
- 8.3.16. Deve permitir a configuração de DHCP Relay;
- 8.3.17. Deve implementar PBR (*Policy-Based Routing*) para IPv4 e IPv6;
- 8.3.18. Deve implementar IPv6 *router advertisement* (RA) *preference* na mensagem de RA com informações de múltiplos roteadores para a escolher a rota default apropriada pelo host IPv6;

8.4. QUALIDADE DE SERVIÇO:

- 8.4.1. Deve permitir priorização de tráfego usando 8 (oito) filas de priorização por porta;
- 8.4.2. Deve permitir priorização de tráfego baseado no padrão IEEE 802.1p e no campo DSCP do protocolo Diffserv;

27/73

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

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

8.4.5. Deve permitir a configuração de *Rate Limiting* de entrada;

8.4.6. Deve permitir a configuração de *Rate Shaping* de saída;

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

8.5. SEGURANÇA:

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

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

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

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

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

8.5.5.1. 02 (dois) dispositivos que suportam o padrão IEEE 802.1x;

8.5.5.2. 02 (dois) dispositivos MAC que não suportam o padrão IEEE 802.1x;

8.5.5.3. 01 (um) dispositivo que suporta o padrão IEEE 802.1x e 1 (um) dispositivo MAC que não suporta o padrão IEEE 802.1x;

8.5.6. O equipamento deve permitir a configuração de re-autenticação 802.1x periódica;

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

8.5.8. Deve implementar "*Change of Authorization*" de acordo com a RFC 5176;

28/73

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

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

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

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

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

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

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

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

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

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

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

8.5.20. Deve permitir a configuração de *Dynamic ARP Inspection* em pelo menos 500 vlans;

8.5.21. Deve implementar *IP Source Guard*;

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

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

8.5.24. Deve implementar IPv6 *RA guard* e IPv6 *ND inspection*;

8.5.25. Deve implementar RADsec conforme RFC6614;

8.6. GERENCIAMENTO:

29/73

- 8.6.1.** Deve permitir monitoração e configuração usando SNMP v1, v2 e v3;
- 8.6.2.** Deve permitir o gerenciamento via SNMPv3 com as seguintes opções: sem autenticação e sem privacidade, com autenticação e sem privacidade e com autenticação e com privacidade;
- 8.6.3.** Deve ser possível enviar “traps” e realizar o gerenciamento via SNMP através das redes IPv4 e IPv6;
- 8.6.4.** Deve permitir a configuração de porta para espelhamento de tráfego, para a coleta de pacotes em analisadores de protocolo ou detecção de intrusão;
- 8.6.5.** Deve permitir espelhamento de tráfego baseado em Porta, VLAN, Filtro MAC e ACL;
- 8.6.6.** Deve permitir a configuração de porta para espelhamento de tráfego para uma porta em um switch remoto;
- 8.6.7.** Deve implementar gerenciamento usando SSH v2 utilizando os algoritmos de criptografia 3DES e AES. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;
- 8.6.8.** Deve implementar gerenciamento via Telnet. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;
- 8.6.9.** Deve implementar pelo menos 4 (quatro) grupos de RMON;
- 8.6.10.** Deve permitir o monitoramento dos *transceivers* óticos, retornando informação de temperatura, potência de transmissão (dBm), potência de recepção (dBm) e status;
- 8.6.11.** Deve implementar funcionalidade de diagnóstico do cabo de par trançado, retornando informação de comprimento do cabo, status do link;
- 8.6.12.** Deve permitir a atualização de arquivos de configuração e imagens de firmware usando TFTP ou FTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
- 8.6.13.** Deve permitir a atualização de imagens de firmware dos equipamentos de uma pilha sem a necessidade de reinicialização simultânea de todos os equipamentos da pilha, permitindo a continuidade do tráfego de dados durante o processo de atualização;
- 8.6.14.** Deve permitir configuração automática do seu próprio endereço IP e a seguir carga automática de um arquivo de configuração pré-definido, usando um servidor DHCP e um servidor TFTP ou FTP;

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

8.6.16. Deve implementar o protocolo OpenFlow 1.3 com suporte para portas híbridas em Camada 2 e Camada 3;

8.6.17. Deve permitir o monitoramento de tráfego através dos protocolos sFlow, NetFlow ou IPFIX. Deve ser possível exportar o tráfego de redes IPv4 e IPv6;

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

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

8.6.20. Deve permitir atualização de imagem de firmware através de mídia de armazenamento externa conectado ao slot USB;

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

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

8.6.23. Deve possuir suporte a automação com Ansible.

CLÁUSULA NONA – DO CABO UPLINK DAC/AOC QSFP28 100G 5M

9.1. CARACTERÍSTICAS GERAIS:

9.1.1. Cabo DAC com conectores QSFP28 100GB – 5 m

9.1.2. Cabo de cobre DAC com dois *transceiver*/conectores QSFP28 soldados ao cabo.

9.1.3. Deve ter comprimento de, no mínimo, 5 (cinco) metros.

9.1.4. Deve possuir velocidade de operação de 100 Gigabit Ethernet.

9.1.5. Deve ser do mesmo fabricante, homologado e compatível com os switches especificados neste lote.

31/73

CLÁUSULA DÉCIMA – DO CABO DAC AOC 100G 10M**10.1. CARACTERÍSTICAS GERAIS:**

- 10.1.1. Deve ser do mesmo fabricante dos switches ofertados;
- 10.1.2. Cabo *Direct Attach* ativo QSFP28 para QSFP28;
- 10.1.3. Dever ser compatível com interfaces 100G QSFP28;
- 10.1.4. Deve possuir no mínimo 10 metros de comprimento;

CLÁUSULA DÉCIMA PRIMEIRA – DO CABO DAC AOC 25G 10M**11.1. CARACTERÍSTICAS GERAIS:**

- 11.1.1. Deve ser do mesmo fabricante dos switches ofertados;
- 11.1.2. Cabo *Direct Attach* ativo SFP28 para SFP28;
- 11.1.3. Dever ser compatível com interfaces 25G SFP28;
- 11.1.4. Deve possuir no mínimo 10 metros de comprimento;

CLÁUSULA DÉCIMA SEGUNDA – DO TRANSCEIVER SFP+ 10GBASE-SR**12.1. CARACTERÍSTICAS GERAIS:**

- 12.1.1. Deve ser do mesmo fabricante dos switches ofertados;
- 12.1.2. Deve atender o padrão SFP+;
- 12.1.3. Deve atender ao padrão 10 Gigabit Ethernet IEEE 802.3ae, com comprimento de onda de 850nm em cabo óptico Multimodo;
- 12.1.4. Deve possuir o conector do tipo LC;
- 12.1.5. Deve atender ao padrão 10GBASE-SR;

32/73

CLÁUSULA DÉCIMA TERCEIRA – DO SOFTWARE DE GERENCIAMENTO DOS ATIVOS DE REDE**13.1. CONTROLADOR DE REDE:**

13.1.1. O controlador deverá ser do tipo virtual e compatível com os ambientes VMWare 6.5 e superiores, Hyper-V Windows 2012 R2 e superiores, KVM CentOS 7.3 e superiores, AWS, MS Azure ou GCE. O ambiente virtualizado deverá ser disponibilizado em servidor ou servidores da **CONTRATANTE** com as especificações recomendadas pelo fabricante da solução.

13.1.2. Não serão aceitas soluções baseadas nas premissas de computação em nuvem, pontos de acesso autônomos ou controladores agregados a outros equipamentos, tais como Firewalls ou Roteadores.

13.1.3. Deverá ser do mesmo fabricante dos pontos de acesso fornecidos pela **CONTRATADA**, para fins de compatibilidade e gerenciamento.

13.1.4. Deverá suportar a operação como um cluster (N+1) para prover resiliência e desempenho, podendo o mesmo ser composto por, no mínimo, 2 (dois) controladores e expansível até 4 (quatro) controladores.

13.1.5. Deve ser acompanhado de todos os acessórios necessários para operacionalização da solução, tais como softwares, documentações técnicas e manuais que contenham informações suficientes, que possibilitem a instalação, configuração e operacionalização da solução.

13.1.6. Deve possuir uma arquitetura modular do tipo multi-tenant, permitindo gestão centralizada, mas com acesso independente e isolado para cada domínio.

13.1.7. Deverá suportar pontos de acesso internos e externos nos padrões 802.11a/b/g/n/ac/ax.

13.2. GERENCIAMENTO DE WLAN:

13.2.1. Deve suportar a capacidade para gerenciar, no mínimo, 2.000 (dois mil) Pontos de Acesso por controlador.

13.2.2. Suportar, no mínimo, 35.000 (trinta e cinco mil) dispositivos simultâneos por controlador.

13.2.3. Deve ser fornecido com a capacidade para gerenciamento de todos os Pontos de Acesso desse certame. Caso sejam necessários licenças para realizar o gerenciamento, estas devem ser fornecidas.

13.2.4. Prover o gerenciamento centralizado dos Pontos de Acesso, suportando versões de firmware diferentes.

33/73

13.2.5. Deverá permitir gerenciamento através de Endereço IP, Range de IPs e Sub-Redes pré-configuradas

13.2.6. Permitir a configuração total dos pontos de acesso, assim como os aspectos de segurança da rede wireless (WLAN) e Rádio Frequência (RF)

13.2.7. O controlador poderá estar diretamente e/ou remotamente conectado aos Pontos de Acesso por ele gerenciados, inclusive via roteamento em camada 3 do modelo OSI

13.2.8. Possibilitar a configuração de envio dos eventos do Controlador para um servidor de Syslog remoto

13.2.9. Implementar, pelo menos, os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps SNMP

13.2.10. Permitir a visualização de alertas da rede em tempo real

13.2.11. Implementar, no mínimo, 3 (três) níveis de acesso administrativo ao equipamento (apenas leitura, leitura/escrita e administrador da senha de visitante) protegidos por senhas independentes

13.2.12. Permitir a customização do acesso administrativo através de atribuição de grupo de função do usuário administrador

13.2.13. Permitir a configuração e gerenciamento através de navegador padrão por meio de HTTPS.

13.2.14. Gerenciar de forma centralizada a autenticação de usuários

13.2.15. Permitir o envio de alertas ou alarmes através do protocolo SMTP, sendo que a comunicação com o servidor deverá ser autenticada e cifrada (SMTP/TLS)

13.2.16. Permitir que o processo de atualização de versão seja realizado através de navegador padrão (HTTPS) ou SSH.

13.2.17. Deverá possuir a capacidade de importação de certificados digitais emitidos por uma autoridade certificadora externa.

13.2.18. A disponibilidade da rede sem fio deve ser passível de agendamento para, no mínimo, as opções a seguir:

13.2.19. 24 horas por dia, 07 dias na semana.

13.2.20. Agendamento customizado permitindo escolher os dias da semana e horários.

34/73

13.2.21. Os horários definidos não precisam ser sequenciais, ou seja, a solução deve suportar que o administrador defina o horário de funcionamento das 08:00 às 12:00 e 14:00 às 18:00.

13.2.22. Possuir ferramentas de diagnóstico e log de eventos para depuração e gerenciamento em primeiro nível.

13.2.23. Possuir ferramenta que permite o monitoramento em tempo real de informações de utilização de CPU, memória e estatísticas de rede.

13.2.24. Possibilitar cópia “backup” da configuração, bem como a funcionalidade de restauração da configuração através de navegador padrão (HTTPS) ou FTP ou TFTP.

13.2.25. Possuir a capacidade de armazenar múltiplos arquivos de configuração do controlador pertencente à rede sem fio

13.2.26. Monitorar o desempenho da rede sem fio, permitindo a visualização de informações de cada ponto de acesso.

13.2.27. Suportar a implementação de cluster de controladores no modo ativo/ativo, com sincronismo automático das configurações entre controladores para suporte a redundância em alta disponibilidade (HA - high availability).

13.2.28. Deverá efetuar compartilhamento de recursos e licenças de pontos de acesso entre os controladores participantes do cluster

13.2.29. Deverá em caso de falha realizar a redundância de forma automática e sem nenhuma necessidade de intervenção do administrador de rede

13.2.30. Deverá possuir a capacidade de geração de informações ou relatórios de, no mínimo, os seguintes tipos: Listagem de clientes Wireless, Listagem de Pontos de Acesso, utilização da rede.

13.2.31. Deverá suportar, somente por meio do controlador e do ponto de acesso, a identificação de aplicações dos clientes conectados com base na camada 7 do modelo OSI, permitindo o controle de acesso, de banda (uplink e/ou downlink) e definição de regra de QoS para estas aplicações.

13.2.32. Permitir visualizar a localização dos pontos de acesso e através desta obter o status de funcionamento dos mesmos.

13.2.33. Deverá possibilitar a importação de plantas baixas nos formatos dwg ou jpg ou png, devendo permitir a visualização dos Pontos de Acesso instalados com seu estado de funcionamento, bem como disponibilizar uma visualização da cobertura do sinal em 2.4GHz ou 5GHz.

35/73

13.2.35. Implementar funcionalidade de análise espectral, permitindo a detecção de interferências no ambiente de rede sem fio.

13.2.36. Implementar análise de tráfego por WLAN, Ponto de acesso e dispositivos cliente, apresentando os 10 itens mais usados.

13.2.37. Deve ser possível definir o nível de segurança administrativo da solução suportando, no mínimo:

13.2.38. Habilitar Captcha para Acesso

13.2.39. Período em dias para alteração obrigatória da senha

13.2.40. Política para reutilização de senha

13.2.41. Comprimento mínimo da senha e complexidade

13.2.42. Segundo Fator de Autenticação via SMS

13.2.43. A solução deve suportar a adição de um serviço de SMS externo, tal como Twilio.

13.2.44. Deve suportar integração com tags da Ekahau e AeroScout/Stanley para Real-Time Location Service (RTLS).

13.3. REDE:

13.3.1. Deverá implementar suporte aos protocolos IPv4 e IPv6

13.3.2. Deverá suportar tagging de VLANs

13.3.3. Implementar associação dinâmica de usuário a VLAN com base nos parâmetros da etapa de autenticação via IEEE 802.1X.

13.3.4. Suportar associação dinâmica de ACL e de QoS por usuário, com base nos parâmetros da etapa de autenticação.

13.3.5. Deverá suportar, no mínimo, 1030 (mil e trinta) SSIDs simultâneos

13.3.6. Deverá possuir funcionalidade de balanceamento de carga entre VLANs e permitir que clientes sejam designados para diferentes VLANs dentro de um mesmo SSID, com suporte a até 50 VLANs por pool.

13.3.7. Em caso de falha de comunicação entre os pontos de acesso e a controladora, os usuários associados à rede sem fio devem continuar conectados com acesso à rede. Também deve permitir que novos usuários se associem à rede sem fio utilizando autenticação do tipo 802.1X mesmo que os pontos de acesso estejam sem comunicação com a controladora

36/73

13.3.8. Deve ser possível evitar que dispositivos 802.11b se conectem à rede, visando melhorar o desempenho da rede sem fio.

13.3.9. Deve suportar 802.11d e 802.11k.

13.3.10. Deve suportar captura de pacotes por ponto de acesso para resolução de problemas, sendo possível definir a captura nos rádios de 2.4 GHz e 5 GHz, bem como na interface LAN. Ainda, a operação deve ser realizada via interface Web e deve ser possível exportar o arquivo de captura para análise local em software de análise de pacote, tal como Wireshark.

13.3.11. Deve ser possível rastrear a conexão de um cliente wireless em tempo real para analisar problemas de conectividade e identificar em qual estágio o problema aconteceu.

13.3.12. Deve ser possível estabelecer um limite para o nível de sinal visando permitir que o cliente se junte à rede sem fio, o qual deve ser estabelecido em dBm e variar entre -60dBm e -90dBm.

13.3.13. Deverá suportar de forma centralizada a configuração de agregação de portas (LACP) ethernet dos pontos de acesso que possuírem suporte a essa funcionalidade.

13.3.14. Deve suportar autoconfiguração e autocorreção para rede Mesh.

13.4. SEGURANÇA:

13.4.1. Os itens a seguir devem estar integrados a solução ofertada, não serão aceitos equipamentos externos a solução. Caso sejam necessárias licenças ou softwares de controle os mesmos devem ser fornecidos de forma que a solução esteja operacional e sem nenhuma restrição no ato de sua implementação (hardware e softwares necessários para implementação).

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

13.4.2.1. (WPA) Wi-Fi Protected Access;

13.4.2.2. (WPA2) Wi-Fi Protected Access 2;

13.4.2.3. (WPA3) Wi-Fi Protected Access 3;

13.4.2.4. (TKIP) Temporal Key Integrity Protocol;

13.4.2.5. (AES) Advanced Encryption Standard;

13.4.2.6. PSK (pre-shared key) exclusivo para cada dispositivo no mesmo SSID;

13.4.2.7. IEEE 802.1X;

13.4.2.8. IEEE 802.11i;

37/73

13.4.2.9. IEEE 802.11w;

13.4.2.10. Implementar, pelo menos, os seguintes controles/filtros:

13.4.2.10.1. Baseado em endereço MAC e isolamento de cliente na camada 2 do modelo OSI;

13.4.2.10.2. Baseado em endereço IP;

13.4.2.10.3. Baseado em protocolo, tais como TCP, UDP, ICMP e IGMP;

13.4.2.10.4. Baseado em porta de origem e/ou destino;

13.4.2.10.5. Baseado em tipo ou sistema operacional do dispositivo.

13.4.3. Permitir a autenticação para acesso dos usuários conectados nas redes WLAN (Wireless) através:

13.4.3.1. Endereço MAC;

13.4.3.2. Autenticação Local;

13.4.3.3. Captive Portal;

13.4.3.4. Active Directory;

13.4.3.5. RADIUS;

13.4.3.6. IEEE 802.1X;

13.4.3.7. LDAP.

13.4.4. Deverá permitir a seleção/uso de servidor RADIUS específico com base no SSID.

13.4.5. Deverá suportar servidor de autenticação RADIUS redundante. Isto é na falha de comunicação com o servidor RADIUS principal, o sistema deverá buscar um servidor RADIUS secundário.

13.4.6. A solução deverá suportar a criação de uma zona de visitantes, que terá seu acesso controlado através de senha cadastrada internamente, sendo que esta deverá possuir a configuração de tempo pré-determinado de acesso à rede sem fio.

13.4.7. O controlador deverá permitir a criação de múltiplos usuários visitantes (*guests*) de uma única vez (em lote)

13.4.8. Deve ser possível definir o período de validade da senha de visitantes em quantidade de horas, dias e semanas.

38/73

13.4.9. Deve permitir que após o processo de autenticação de usuários visitantes (*guests*) os mesmos sejam redirecionados para uma página de navegação específica e configurável.

13.4.10. Deve permitir que múltiplos usuários visitantes (*guests*) compartilhem a mesma senha de acesso à rede

13.4.11. Deverá dispor de opção para enviar a senha de usuários visitantes (*guests*) por e-mail ou por SMS.

13.4.12. Deverá permitir o encaminhamento do tráfego de saída de usuários visitantes (*guests*) diretamente para a Internet, de forma totalmente separada do tráfego da rede corporativa

13.4.13. Deverá permitir o isolamento do tráfego unicast, multicast ou ambos entre usuários visitantes (*guests*) em uma mesma VLAN/Subrede, sendo possível adicionar exceções com base em endereços MAC e IP.

13.4.14. Deverá ser possível permitir que o ponto de acesso filtre todo o tráfego IPv4 e IPv6 dos tipos multicast e broadcast dos clientes sem fio associados, com exceção de alguns tráfegos pertencentes a uma lista de exclusões, tais como ARP, DHCPv4 e DHCPv6, MLD, IGMP, IPv6 NS, IPv6 NA, IPv6 RS e todos os pacotes do tipo *unicast*.

13.4.15. Deverá ser possível especificar o tipo de serviço Bonjour que será permitido entre VLANs.

13.4.16. Deve suportar mecanismo de acesso de acordo com o padrão Hotspot 2.0

13.4.17. Deve implementar mecanismos de segurança e proteção da rede sem fio contemplando, no mínimo, os recursos abaixo:

13.4.18. SSID Spoofing – Detectar APs não pertencentes ao controlador propagando o mesmo SSID.

13.4.19. MAC Spoofing – Detectar APs não pertencentes ao controlador propagando o mesmo MAC de um AP válido.

13.4.20. Rogue APs – Detectar APs não pertencentes ao controlador.

13.4.21. Same Network – Detectar APs não pertencentes ao controlador exibindo qualquer SSID pertencentes ao mesmo segmento de rede LAN.

13.4.22. Ad Hoc – Possibilidade de detectar rede Ad Hoc como *Rogue*.

13.4.23. Flood de Deauthentication – Detectar quando há um número excessivo de frames de desautenticação oriundos de um mesmo transmissor.

13.4.24. Flood de Disassociation – Detectar quando há um número excessivo de frames de desassociação oriundos de um mesmo transmissor.

13.4.25. Excesso de Clear to Send (CTS) – Detectar quando há um número excessivo de frames de CTS para um endereço MAC específico.

13.4.26. Excesso de Request to Send (RTS) – Detectar quando há um número excessivo de frames de RTS para um endereço MAC específico.

13.4.27. Excesso de Energia – Possibilidade de detectar tráfego com nível de potência de transmissão excessivo.

13.4.28. Deve implementar varredura de rádio frequência para identificação de ataques e Pontos de Acesso intrusos não autorizados (*rogues*).

13.4.29. Deve fazer a varredura no canal de operação do Ponto de Acesso sem impacto na performance da rede WLAN.

13.4.30. Deve utilizar os Pontos de Acesso para fazer a monitoração do ambiente Wireless procurando por pontos de acesso do tipo rogue de forma automática.

13.4.31. Deve ser possível especificar um ponto de acesso ou grupo de pontos de acesso para atuarem somente com a função de monitoramento visando detectar ataques e analisar o ambiente de rádio frequência.

13.4.32. Deverá ser capaz de localizar Pontos de Acesso do tipo rogue na planta baixa adicionada ao sistema com informações de, no mínimo:

13.4.32.1. Pontos de Acesso que detectam;

13.4.32.2. Tipo de Rogue;

13.4.32.3. Nome da Rede;

13.4.32.4. Nível de sinal de detecção.

13.5. RECURSOS DE GERENCIAMENTO AUTOMÁTICO DE RÁDIO FREQUÊNCIA (RF)

13.5.1. Na ocorrência de inoperância de um Ponto de Acesso, o controlador sem fio deverá ajustar automaticamente a potência dos Pontos de Acesso adjacentes, de modo a prover a cobertura da área não assistida.

13.5.2. Ajustar automaticamente a utilização de canais de modo a otimizar a cobertura de rede e mudar as condições de rádio frequência baseado em desempenho.

40/73

13.5.3. Detectar interferência e ajustar parâmetros de rádio frequência, evitando problemas de cobertura de RF de forma automática.

13.5.4. Implementar sistema automático de balanceamento de carga para associação de clientes entre Pontos de Acesso próximos para otimizar o desempenho.

13.5.5. Implementar funcionalidade de balanceamento de carga entre os rádios de um mesmo Ponto de Acesso.

13.5.6. Permitir que o serviço wireless seja desabilitado de determinado ponto de acesso. Também deve ser possível selecionar o serviço de qual rádio (banda) de determinado ponto de acesso deve ser desabilitado.

13.6. RECURSOS DE CONVERGÊNCIA E MULTIMÍDIA

13.6.1. Suportar 802.11e.

13.6.2. Deverá possuir funcionalidade de configuração do limite de banda disponível por usuário ou através de SSID/BSSID.

13.6.3. Deverá permitir a configuração de prioridade de um determinado SSID sobre outros SSIDs existentes na controladora.

13.6.4. Deve suportar WiFi Calling.

13.7. GERENCIAMENTO DOS SWITCHES

13.7.1. Deverá ser do mesmo fabricante dos Switches fornecidos neste certame, para fins de compatibilidade.

13.7.2. Deve suportar o gerenciamento de pelo menos 400 (quatrocentos) switches por meio de um único controlador e até 1.200 (um mil e duzentos) switches por meio de cluster.

13.7.3. Deve ser fornecido com a capacidade para gerenciamento de todos os switches do certame. Caso seja necessário licenças para realizar o gerenciamento, estas devem ser fornecidas.

13.7.4. Deve ser possível gerenciar Switches com imagens ou perfis de Camada 2 e Camada 3.

13.7.5. Deve ser capaz de gerenciar todos os switches fornecidos neste certame.

13.7.6. Se houver necessidade de licenças para gerenciar os switches, estas devem ser fornecidas juntamente com a respectiva quantidade de switches.

13.7.7. Deve ser possível criar grupos lógicos de switches para facilitar a gestão.

41/73

13.7.8. Deve ser possível associar um switch automaticamente com um respectivo grupo de switches por meio de regras de registro, as quais devem ser definidas por, pelo menos, um dos meios a seguir: faixa de endereço IP, sub-rede ou modelo do switch.

13.7.9. Deve realizar backup da configuração dos switches diariamente, mantendo, no mínimo, um histórico das últimas 7 (sete) versões de arquivos de configurações.

13.7.10. A configuração só deve ser armazenada se houver alguma alteração entre o último backup e o backup atual.

13.7.11. Deve ser possível executar um backup manual.

13.7.12. Deve suportar a restauração de um determinado backup.

13.7.13. Deve dispor de uma opção para visualizar um determinado arquivo de configuração, bem como permitir analisar as diferenças entre arquivos de configurações distintos realçando-as para fácil identificação.

13.7.14. Deve permitir a atualização de firmware dos switches de modo individual e em grupos, bem como manter o histórico das atualizações de cada switch.

13.7.15. Deve permitir o agendamento de atualização de firmware dos switches de modo individual e em grupos.

13.7.16. Deve ser possível definir configurações comuns a um grupo de switches, tais como configurações de DNS e AAA (*Authentication, Authorization e Accounting*).

13.7.17. As configurações de AAA devem permitir habilitar ou desabilitar a autenticação, autorização e *accounting* para SSH ou Telnet, incluindo a seleção da ordem de preferência dos servidores AAA.

13.7.18. Para autenticação, deve ser possível definir servidor Radius, TACACS+ e usuário local.

13.7.19. Para autorização e *accounting*, deve ser possível definir servidor Radius e TACACS+.

13.7.20. Deverá possibilitar a criação de Listas de Controle de Acesso (ACL) do tipo padrão ou estendida e permitir a definição de quando a configuração deve ser aplicada no switch, se imediatamente ou por meio de agendamento.

13.7.21. Deverá permitir a criação de VLANs, permitindo atribuir um nome a esta VLAN, bem como definir quais portas devem ser *untagged* ou *tagged*.

13.7.22. Deve ser possível configurar *DHCP Snooping*, *ARP Inspection* e *IP Source Guard*.

13.7.23. Deve ser possível configurar *IGMP Snooping* Ativo ou Passivo.

42/73

13.7.24. Deve suportar configurações de *Spanning Tree*, tais como permitir definir entre STP (802.1d) ou RSTP (802.1w) e sua respectiva prioridade.

13.7.25. Deverá ser possível criar rotas estáticas e permitir a definição de quando a configuração deve ser aplicada no switch, se imediatamente ou por meio de agendamento.

13.7.26. Deve disponibilizar um histórico das configurações criadas, demonstrando o tipo de configuração, a data e o período em que foram criadas, bem como se a mesma foi implementada com sucesso ou se houve alguma falha.

13.7.27. Deve ser possível definir um *hostname* para cada switch.

13.7.28. Deve ser possível habilitar Jumbo Frame.

13.7.29. Deve suportar DHCP Server e DHCP Relay.

13.7.30. Deve dispor de funcionalidade para copiar configurações de um determinado switch para um ou mais switches.

13.7.31. Deve ser possível criar LAGs (*Link Aggregation Group*) do tipo estático ou dinâmico.

13.7.32. Deve ser possível criar empilhamento de switches.

13.7.33. Deve ser possível habilitar ou desabilitar uma porta, bem como definir um nome para cada porta.

13.7.34. Deve ser possível habilitar ou desabilitar PoE, bem como definir a classe ou prioridade PoE.

13.7.35. Deve ser possível definir configurações de camada 3 para uma porta como, por exemplo, área OSPF e endereço IP.

13.7.36. Deve permitir a visualização de alarmes relacionados ao switch, incluindo, mas não se limitando a: falha de uma fonte de alimentação, falha de um membro do empilhamento ou falha na alocação de PoE.

13.7.37. Deve permitir a detecção e visualização de eventos relacionados ao switch com base em certas condições, bem como permitir o envio de notificações por E-mail e *Traps SNMP*.

13.7.38. Deve ser possível criar eventos customizados, podendo definir o texto que um evento deve conter, condição em quantidade de vezes, janela de tempo em horas e severidade.

13.7.39. Deve dispor de painel gráfico com o estado das portas dos switches.

43/73

13.7.40. Deve disponibilizar um detalhamento das portas de um switch demonstrando, no mínimo, o nome da porta, o estado da porta (*UP/DOWN*), o estado administrativo da porta (*UP/DOWN*), a velocidade, a utilização de PoE para portas PoE, a utilização de banda (*in/out*), total de pacotes *multicast* (*in/out*), total de pacotes broadcast (*in/out*), número de pacotes com erro (*in/out*), erros de CRC e número de pacotes *inbound* descartados.

13.7.41. Deve disponibilizar graficamente a visão do painel frontal de um determinado switch permitindo visualizar, no mínimo, as seguintes informações de uma determinada porta: nome da porta, estado da porta (*UP/DOWN*), *VLANs Untagged e Tagged*, e, para portas PoE, a utilização de PoE.

13.7.42. Deve disponibilizar uma visão da topologia dos dispositivos gerenciados.

13.7.43. Deve possuir painéis demonstrando o volume de tráfego total para todos os switches ou para os switches de um grupo, bem como listar os principais switches do sistema por volume de tráfego, por erro de porta e por utilização de PoE.

13.7.44. Deve monitorar a utilização da CPU, da memória e estado da fonte de alimentação dos switches.

13.7.45. Deve permitir o monitoramento da temperatura de operação dos switches.

13.7.46. Deve ser possível visualizar os equipamentos vizinhos conectados ao switch, incluindo nome do dispositivo, endereço MAC, tipo do dispositivo e a partir de qual porta física do switch esse dispositivo vizinho pode ser encontrado.

13.7.47. Deve dispor de operações remotas para auxílio na resolução de problemas suportando, pelo menos, *Ping e Traceroute*.

13.7.48. Deve dispor de uma ferramenta para análise da conectividade do cliente por meio da inserção do endereço MAC do dispositivo final.

13.7.49. Deve possuir garantia de hardware por, pelo menos, 5 (cinco) anos pelo fabricante.

CLÁUSULA DÉCIMA QUARTA – DA LICENÇA PARA GERENCIAMENTO DOS DISPOSITIVOS SWITCHES TIPO 1, 2 E 3

14.1. CARACTERÍSTICAS GERAIS:

14.1.1. Deve adicionar licença de uso de switch gerenciado na Clausula Décima Terceira– Solução de gerenciamento de ativos de rede.

14.1.2. Deve ser licenciado de forma unitária, permitindo a este órgão adquirir o quantitativo que desejar, respeitando o limite suportado pelo equipamento Controlador de Rede Virtual.

14.1.3. Deve ser obrigatoriamente do mesmo fabricante dos pontos de acesso, controladores e switches.

14.1.4. Deve atender na íntegra os requisitos especificados na Clausula Décima Terceira– Solução de gerenciamento de ativos de rede

14.1.5. Caso aplicável, deve acompanhar suporte do fabricante por um período de 05 (cinco) anos.

CLÁUSULA DÉCIMA QUINTA – DA LICENÇA PARA GERENCIAMENTO DE DISPOSITIVOS PONTO DE ACESSO TIPO 1 E 2

15.1. CARACTERÍSTICAS GERAIS:

15.1.1. Deve adicionar licença de uso de ponto de acesso gerenciado na Clausula Décima Terceira– Solução de gerenciamento de ativos de rede.

15.1.2. Deve ser licenciado de forma unitária, permitindo a este órgão adquirir o quantitativo que desejar, respeitando o limite suportado pelo equipamento Controlador de Rede Virtual.

15.1.3. Deve ser obrigatoriamente do mesmo fabricante dos pontos de acesso, controladores e switches.

15.1.4. Deve atender na íntegra os requisitos especificados no na Clausula Décima Terceira– Solução de gerenciamento de ativos de rede

15.1.5. Caso aplicável, deve acompanhar suporte do fabricante por um período de 05 (cinco) anos.

CLÁUSULA DÉCIMA SEXTA – DO PONTO DE ACESSO INDOOR TIPO 1

16.1. CARACTERÍSTICAS GERAIS:

16.1.1. Ponto de acesso indoor 2x2:2 WI-FI 6.

16.1.2. Deverá ser do mesmo fabricante do CONTROLADOR DE REDE SEM FIO para fins de compatibilidade.

45/73

16.1.3. Deverá possuir estrutura metálica que permita a utilização do equipamento em locais internos, com fixação em teto.

16.1.4. Não serão aceitos equipamentos com padrão de instalação física em parede, conhecidos como “wall plate”, uma vez que a instalação física deverá ocorrer no teto.

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

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

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

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

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

16.1.10. Possuir suporte a pelo menos 16 (dezesesseis) SSIDs por ponto de acesso.

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

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

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

16.1.14. Deverá possuir 02 (duas) interfaces ethernet 10/100/1000 Mbps, utilizando conector RJ-45, para conexão à rede local.

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

46/73

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

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

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

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

16.2. CARACTERÍSTICAS DOS RÁDIOS

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

16.2.2. Implementar as seguintes taxas de transmissão com fallback automático: IEEE 802.11b: 1 Mbps a 11 Mbps, IEEE 802.11a e IEEE 802.11g: 6 Mbps a 54 Mbps, IEEE 802.11n: 6.5 Mbps a 300 Mbps, IEEE 802.11ac: 6.5 Mbps a 867 Mbps e IEEE 802.11ax: 4 Mbps a 1200 Mbps.

16.2.3. Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax, com ganhos de, no mínimo, 1.5 dBi para 2.4GHz e 2.5 dBi para 5GHz.

16.2.4. Deverá suportar potência agregada de saída, considerando todas as cadeias MIMO, de, no mínimo, 25 dBm na frequência de 5 GHz e 26 dBm na frequência de 2.4 GHz.

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

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

16.2.7. Deve possuir sensibilidade mínima de recepção de -97dBm considerando MCS0 HE20 (802.11ax) em 5GHz e 2.4GHz.

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

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

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

16.3. SERVIÇOS, SEGURANÇA E GERENCIAMENTO

47/73

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

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

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

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

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

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

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

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

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

16.3.10. Deve suportar atribuição dinâmica de VLAN por usuário.

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

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

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

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

16.3.15. Implementar, pelo menos, os seguintes padrões de segurança wireless: (WPA) Wi-Fi Protected Access, (WPA2) Wi-Fi Protected Access 2, (WPA3) Wi-Fi Protected Access 3,

48/73

(AES) Advanced Encryption Standard, (TKIP) Temporal Key Integrity Protocol, DPSK, IEEE 802.1X e IEEE 802.11i.

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

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

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

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

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

16.3.21. Deverá suportar funções para análise de espectro.

16.3.22. Deve suportar conversão de tráfego multicast para unicast.

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

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

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

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

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

16.3.28. Deve possuir garantia de hardware por, pelo menos, 5 (cinco) anos pelo fabricante.

CLÁUSULA DÉCIMA SÉTIMA – DO PONTO DE ACESSO INDOOR TIPO 2

17.1. CARACTERÍSTICAS GERAIS

49/73

- 17.1.1.** Ponto de acesso 802.11ax dual-band indoor.
- 17.1.2.** Deverá ser do mesmo fabricante do controlador WLAN para fins de compatibilidade.
- 17.1.3.** Deverá possuir estrutura que permita a utilização do equipamento em locais internos, com fixação em teto e parede.
- 17.1.4.** Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto, com data anterior à publicação do edital, conforme a resolução 242. Não serão aceitos protocolos de entrada ou outros documentos diferentes do certificado, uma vez que os mesmos não garantem o fornecimento de equipamentos homologados e em conformidade com as leis brasileiras.
- 17.1.5.** Visando a plena compatibilidade do ponto de acesso com o padrão WiFi 6 e suas respectivas funcionalidades, a citar, de forma não-exaustiva, DL OFDMA, UL OFDMA, DL MU-MIMO e se faz necessário que o equipamento ofertado esteja listado como Wi-Fi CERTIFIED 6 no programa da WiFi Alliance na data do pregão.
- 17.1.6.** Deve possuir a certificação IEC 61373 para uso em ambientes sujeitos à vibração e impactos.
- 17.1.7.** Deve ser compatível com o padrão UL 2043, o qual regula os componentes dos materiais com o intuito de proteger contra danos causados por fogo, bem como pela fumaça.
- 17.1.8.** Suportar, no mínimo, 500 (quinhentos) usuários wireless simultâneos, sem nenhum tipo de licença adicional.
- 17.1.9.** Possuir suporte a pelo menos 16 (dezesesseis) SSIDs por ponto de acesso.
- 17.1.10.** Possibilitar alimentação elétrica local via fonte de alimentação com seleção automática de tensão (100-240V) e via padrão PoE (IEEE 802.3at ou 802.3bt). Ademais, para PoE, a alimentação elétrica deve ocorrer através de uma única interface de rede, sem perda de funcionalidade e de desempenho.
- 17.1.11.** Deve suportar temperatura de operação entre 0°C a 40°C.
- 17.1.12.** O equipamento ofertado não deverá possuir antenas aparentes externas ao ponto de acesso, evitando desta forma que as mesmas sejam removidas, o que ocasionaria na degradação do desempenho da rede sem fio.
- 17.1.13.** Deverá possuir 2 (duas) interfaces ethernet, sendo 1 (uma) 10/100/1000 Mbps e 1 (uma) 1/2.5 Gbps, utilizando conector RJ-45, para conexão à rede local.

50/73

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

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

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

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

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

17.2. CARACTERÍSTICAS DOS RÁDIOS

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

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

17.2.3. Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax, com ganhos de, no mínimo, 2 dBi para 2.4GHz e 2 dBi para 5GHz.

17.2.4. Deverá suportar potência agregada de saída, considerando todas as cadeias MIMO, de, no mínimo, 28 dBm na frequência de 5 GHz e 26 dBm na frequência de 2.4 GHz.

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

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

17.2.7. Deve possuir sensibilidade mínima de recepção de -98dBm considerando MCS0 HE20 (802.11ax) em 5GHz e -93dBm considerando MCS0 HE20 (802.11ax) em 2.4GHz.

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

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

51/73

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

17.3. SERVIÇOS, SEGURANÇA E GERENCIAMENTO

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

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

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

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

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

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

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

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

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

17.3.10. Deve suportar atribuição dinâmica de VLAN por usuário.

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

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

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

17.3.14. Deve suportar *HotSpot* 2.0, Captive Portal e WISPr.

52/73

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

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

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

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

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

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

17.3.21. Deve implementar autenticação de usuários usando WISPr e *Hotspot 2.0*.

17.3.22. Deverá suportar funções para análise de espectro.

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

17.3.24. Deve suportar conversão de tráfego *multicast* para *unicast*.

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

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

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

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

17.3.29. Deve possuir garantia de hardware por, pelo menos, 5 (cinco) anos pelo fabricante.

53/73

CLÁUSULA DÉCIMA OITAVA – DA FONTE DE ALIMENTAÇÃO POE**18.1. CARACTERÍSTICAS GERAIS**

18.1.1. Deve ser fornecido para operando em 110/220 VAC (50 a 60Hz) com chaveamento automático permitindo ser usado de tomada padrão brasileiro;

18.1.2. Deve ser projetado para funcionar para entrega de energia até 60Watts, padrão PoE 802.3bt;

18.1.3. Deve possuir 02 (duas) portas Ethernet 100/1000Mbps;

18.1.4. Deve possuir garantia de hardware por, pelo menos, 5 (cinco) anos do fabricante.

CLÁUSULA DÉCIMA NONA – DA INSTALAÇÃO FÍSICA E CONFIGURAÇÃO BÁSICA**19.1. CARACTERÍSTICAS GERAIS**

19.1.1. A **CONTRATADA** deverá elaborar um Plano de Implantação detalhando as ações necessárias, os responsáveis envolvidos, o cronograma, o impacto previsto, o plano testes, as informações de configuração, tais como linhas de comando, mapas topológicos, detalhes de endereçamento IP e o risco associado às atividades, observando as boas práticas de mercado. O Plano de Implantação deverá ser elaborado pela **CONTRATADA** em até 15 (quinze) dias úteis após a abertura da Ordem de Serviço, validado e aprovado.

19.1.2. A solução deverá ser implantada de modo a não causar indisponibilidade dos sistemas e serviços informatizados aos usuários, salvo previamente acordado com a equipe de Fiscalização do contrato.

19.1.3. A **CONTRATADA** deverá comprovar que os profissionais responsáveis pela execução do contrato possuem aptidão técnica para realização da instalação e configuração dos equipamentos, por meio de apresentação de certificações e comprovação de experiência técnica mínima.

19.1.4. A **CONTRATADA** ao final do processo de instalação, deverá fornecer documentação em meio eletrônico, contendo descritivo completo do processo de instalação da solução, contendo também detalhes sobre a comunicação dos equipamentos, onde deverá ser demonstrada as velocidades e qualidade da transmissão de dados, conforme plano de testes, para fins de comprovação da conclusão da implantação.

54/73

CLÁUSULA VIGÉSIMA – DA OPERAÇÃO ASSISTIDA**20.1. CARACTERÍSTICAS GERAIS**

20.1.1. Os serviços fornecidos no formato de operação assistida têm como premissa atender as demandas técnicas da **CONTRATANTE**, compreendendo, entre outros:

20.1.1.1. O prazo da operação assistida será de no mínimo 90 (noventa) dias contados a partir da finalização do item de serviço de instalação e configuração básica da solução e no máximo de 180 (cento e oitenta) dias.

20.1.1.2. A **CONTRATADA** deverá manter a disposição da **CONTRATANTE**, durante o período de operação assistida, no mínimo 02 (dois) profissionais técnicos especializados nas soluções ofertadas, sendo ao menos 01 (um) deles com certificados CWNA, ITIL V4 e ambos profissionais, deverão ser certificados pelo fabricante da solução na linha de rede LAN e WLAN.

20.1.1.3. E ainda, a **CONTRATADA** deverá alocar um recurso do próprio fabricante nas dependências da **CONTRATANTE**, para o acompanhamento e verificação do desempenho operacional e eliminação imediata de eventuais falhas detectadas na solução contratada, além de definição do design da arquitetura de rede, com as devidas validações das melhores práticas sugeridas pelo fabricante da solução.

20.1.1.4. Todas as definições de implantação deverão ser previamente apresentadas e aprovadas pela equipe da **CONTRATANTE**.

20.1.1.5. Deverá fazer parte do escopo da operação assistida, configuração avançada da solução, de acordo com as metodologias indicadas pelo especialista do fabricante, mediante apresentação de relatório SOW (Statement of Work), onde deverá constar:

I - Roteiro completo de instalação e da configuração avançada;

II - Detalhamento de todas as configurações dos produtos e programas integrantes da solução;

III - Endereçamentos utilizados;

IV - Topologia física e lógica;

V - Lista com o número de série de cada equipamento, descrição e local de instalação;

VI - Planejamento de atividades periódicas para manutenção e melhoria contínua da solução no ambiente da **CONTRATADA**. Esse planejamento deve conter as seguintes características:

55/73

a) Orientações para emissão periódica de relatórios gerenciais sobre utilização dos recursos da solução e respectivos ganhos obtidos;

b) Lista de atividades técnicas que devem ser realizadas pela equipe da **CONTRATANTE**. Deve conter: descrição, orientações técnicas, periodicidade, estimativa de tempo necessário para execução e resultados esperados. No mínimo deve incluir atividades com periodicidade mensal;

c) Lista de atividades conjuntas entre as equipes técnicas da **CONTRATANTE** e da **CONTRATADA** durante o prazo de vigência do Suporte Técnico e Garantia. Deve conter: descrição, orientações técnicas, periodicidade, estimativa de tempo necessário para execução e resultados esperados. No mínimo deve incluir atividades com periodicidade trimestral;

VII - Sugestão de composição de equipe mínima para operacionalizar a solução no ambiente da CONTRATADA, contendo:

a) Perfis dos profissionais;

b) Conhecimentos necessários para cada perfil (cursos, certificações, tempo de experiência profissional);

c) Quantidade mínima de profissionais por perfil indicando a carga horária mensal de dedicação para as atividades;

20.1.1.6. A CONTRATADA deverá emitir relatório técnico identificando e diagnosticando as falhas que porventura forem identificadas.

20.1.1.7. A CONTRATADA deverá propor e tomar todas as ações necessárias para a prevenção da repetição das falhas que ocorrerem durante o período de execução dos serviços de operação assistida.

20.1.1.8. Prestação de manutenções preventivas e preditivas sob demanda da CONTRATANTE.

20.1.1.9. Auxiliar na implementação do monitoramento do desempenho, disponibilidade e capacidade dos produtos fornecidos.

20.1.1.10. Executar diagnósticos, avaliações e ajustes finos do ambiente conforme melhores práticas sugeridas pelo fabricante da solução.

20.1.1.11. Planejar e executar mudanças ou melhorias na solução.

20.1.1.12. Encaminhar, a pedido da CONTRATANTE, incidentes e problemas ao fabricante da solução.

56/73

20.1.1.13. Realizar ou intermediar, a pedido da **CONTRATANTE**, a execução de atividades corretivas ou preventivas propostas pelo fabricante da solução.

20.1.1.14. Auxiliar a **CONTRATANTE** na formulação da customização e parametrização do ambiente de produção, de acordo com as diretrizes e necessidades da **CONTRATANTE**.

20.1.1.15. Propor novas configurações e ajustes para refinar e melhorar o processo de administração e gerenciamento da solução contratada.

20.1.1.16. Os serviços de operação assistida deverão ser solicitados pela **CONTRATANTE** após o aceite da instalação dos equipamentos de rede, mediante a abertura de ordem de serviço e o prazo de 90 (noventa) dias passará a contar no dia seguinte a apresentação formal nas dependências da **CONTRATANTE** da equipe técnica da **CONTRATADA**. Limitado ao prazo máximo de 180 (cento e oitenta) dias.

20.1.1.17. O prazo de entrega das ordens de serviço poderá ser prorrogado, a critério exclusivo do **CONTRATANTE**, caso sejam apresentadas, tempestivamente, razões de justificativa que comprovem a ocorrência de fatos que restringam as atividades ou que fujam do controle da **CONTRATADA** e impeçam a execução dos trabalhos no prazo estabelecido.

20.1.1.18. As ordens de serviço poderão ser canceladas, a critério exclusivo do **CONTRATANTE**, mediante prévia justificativa. As horas trabalhadas poderão ser computadas para fins de faturamento, desde que o motivo de cancelamento não envolva incapacidade da **CONTRATADA** na solução do chamado nos tempos estabelecidos.

20.1.1.19. A **CONTRATADA** deverá fornecer ainda, os seguintes itens:

20.1.1.20. Experiência para dimensionar a rede ao longo do tempo e manter o alto desempenho.

20.1.1.21. Fornecer um grupo de Engenheiros de Suporte Técnico para fornecer o conhecimento, compreensão e experiência.

20.1.1.22. Revisão mensal de implantação para ajudar a planejar para o próximo período, incluindo atualizações de rede, novas implantações, mudanças de processo, etc. Compartilhar as melhores práticas que podem melhorar o desempenho.

20.1.1.23. Experiência em operações de missão crítica.

20.1.1.24. Restaurar serviços. Correção/fornecer correção de bug de emergência, se necessário. Correções incluídas na próxima atualização ou atualização. Funcionalidade de restauração. Fornece uma solução alternativa.

20.1.1.25. Relatórios mensais sobre os seguintes itens:

57/73

- 20.1.1.26. Tempo necessário para a identificação, solução de problemas e reparo do problema.
- 20.1.1.27. Mudanças, adicionar alterações.
- 20.1.1.28. Implementação de recursos.
- 20.1.1.29. Implementações de segmento.
- 20.1.1.30. Análise de causa raiz e planos de ação corretiva.
- 20.1.1.31. Atualizações de software, alertas de novo lançamento quando disponíveis.
- 20.1.1.32. Verificação de saúde do ambiente.
- 20.1.1.33. Processo de atividade de manutenção (M.A.P.) - consulta para atualizações, implementação de recursos.
- 20.1.1.34. Relatório de operações do cliente (cor) - mensalmente ou conforme solicitado.
- 20.1.1.35. Monitoramento de caso, gestão de ativos, chamadas de operações, relatórios.
- 20.1.1.36. Diagnóstico remoto de verificação mensal de rede e alerta.
- 20.1.1.37. Atualizações e upgrades de software.
- 20.1.1.38. Casos e ativos, revisão de chamadas, relatórios operacionais, revisões regulares de negócios.
- 20.1.1.39. Avaliação de LAN, auditorias de rede.

CLÁUSULA VIGÉSIMA PRIMEIRA – DO TREINAMENTO**21.1. CARACTERÍSTICAS GERAIS:**

- 21.1.1. A empresa **CONTRATADA** deverá realizar repasse de conhecimento necessário para que a equipe da possa operar e, se necessário, reconfigurar os equipamentos.
- 21.1.2. O repasse de conhecimento deverá ser iniciado em até 5 (cinco) dias úteis, após a conclusão da implantação das soluções.
- 21.1.3. O repasse de conhecimento deverá contemplar todos os aspectos essenciais de funcionamento e operação; sendo executado nos horários da manhã e/ou da tarde, em turnos diários de no máximo 8h/dia, com carga de 32 horas mínima para 1 (uma) turma de até 10 alunos e 5 ouvintes.

58/73

21.1.4. O repasse de conhecimento deverá ser realizado de forma remota e presencial, onde a **CONTRATADA** arcará com todas as despesas relativas e necessárias, contemplando pelo menos 4(quatro) horas presenciais, no modelo hands-on.

21.1.5. O idioma a ser adotado deverá ser o português.

21.1.6. Todo o material didático a ser utilizado deverá ser fornecido pela **CONTRATADA**.

21.1.7. O instrutor deve ser profissional certificado pelo fabricante dos produtos e com experiência comprovada nos produtos fornecidos.

CLÁUSULA VIGÉSIMA SEGUNDA – DA GARANTIA E SUPORTE TÉCNICO

22.1. CONDIÇÕES GERAIS:

22.1.1. Todos os produtos ofertados que compõem as soluções devem possuir garantia de hardware, suporte e atendimento por 60 (sessenta) meses, a partir do recebimento definitivo dos equipamentos.

22.1.2. Deverá ter acesso direto ao centro de assistência técnica da fabricante dos equipamentos para abertura dos chamados, bem como para acompanhar e gerenciar os casos quando necessário. Esse acesso deverá ser provido 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana através de login/senha individual.

22.1.3. Deverá ter a opção de abrir os chamados junto à fabricante com o intermédio da **CONTRATADA**.

22.1.4. Durante o prazo de suporte o fabricante deverá fornecer, sem ônus adicionais, correções e novas versões disponíveis para todos os softwares, firmwares, atualizações de bug, patches de segurança e afins dos componentes das soluções.

22.1.5. Deverá ter acesso direto à base de dados de conhecimento do fabricante dos equipamentos que contenham especificações técnicas, informações, assistência e orientação para instalação, desinstalação, configuração e atualização de firmware e software, aplicação de correções(patches), diagnósticos, avaliações e resolução de problemas e demais atividades relacionadas à correta operação e funcionamento dos equipamentos.

22.1.6. Durante o período de suporte, a **CONTRATADA** deverá prestar os serviços de suporte técnico sem custo adicional.

22.1.7. O suporte técnico deverá ser prestado de forma remota ou presencial, na modalidade on-site, nas dependências, na modalidade 24/7, a partir da comunicação do problema, via serviço gratuito telefônico ou sistema web indicado pela **CONTRATADA**. Na

59/73

indisponibilidade do canal de atendimento estabelecido, encaminhará e-mail à **CONTRATADA** solicitando a abertura do chamado, de forma que a contagem de prazo de atendimento se iniciará a partir da data de encaminhamento do e-mail.

22.1.8. A **CONTRATADA** deverá disponibilizar meios para que a equipe técnica possa acompanhar os atendimentos do suporte técnico, on-line, em portal web com acesso controlado por senha.

22.1.9. Os chamados junto à **CONTRATADA** deverão ser atendidos por profissionais da **CONTRATADA**, em português e serão usados para abrir solicitações de informações, reportar incidentes ou esclarecer dúvidas quanto à utilização dos produtos e soluções fornecidos.

22.1.10. A **CONTRATADA** deverá realizar atendimento técnico telefônico/eletrônico, em escala 24x7x365 [24 (vinte e quatro) horas por dia, 7(sete) dias por semana, 365 (trezentos e sessenta e cinco dias) por ano], ininterruptamente, os prazos máximos abaixo para solução de contorno:

SEVERIDADE	QUANDO	PRAZO PARA REGISTRO DO CHAMADO	PRAZO PARA SOLUÇÃO DE CONTORNO
BAIXA	Ambiente de produção operando, contudo, recursos ou funcionalidades apresentam instabilidades	Imediatamente após notificação pelo contratante	até 24 (vinte e quatro) horas úteis
MÉDIA	Ambiente de produção operando parcialmente	Imediatamente após notificação pelo contratante	até 8 (oito) horas corridas
ALTA	Ambiente de produção completamente parado	Imediatamente após notificação pelo contratante	até 4 (quatro) horas corridas

22.1.11. Para solução de contorno, se necessário, a **CONTRATADA** deverá providenciar em caráter temporário componente/equipamento equivalente para substituição do item danificado, estando a **CONTRATADA** responsável por toda logística, instalação e configuração dos equipamentos, assim como pela retirada dos antigos, sem qualquer ônus adicional à **CONTRATANTE**.

22.1.12. Em caso de necessidade de reposição de componentes ou equipamentos durante a vigência da Garantia, este deverá acontecer em até 30 (trinta) dias úteis, ficando a **CONTRATADA** responsável por toda logística, instalação e configuração dos novos equipamentos, assim como pela retirada dos antigos, sem qualquer ônus adicional à

60/73

CONTRATANTE. As peças de reposição deverão ser originais do fabricante, de primeiro uso e fornecidas sem custo adicional para **CONTRATANTE**.

22.1.13. A **CONTRATADA** deverá realizar a substituição definitiva do equipamento, dentro do período de garantia, por outro igual ou superior, novo e sem uso, em perfeito estado de funcionamento, quando houver em prazo inferior a 30 (trinta) dias corridos, registro de mais de 04 (quatro) ocorrências de problemas para o mesmo equipamento ou quando o equipamento apresentar defeito irreparável.

22.1.14. O equipamento ou componente substituto passará à propriedade da **CONTRATANTE**, devendo o mesmo ser incluído no contrato de garantia vigente em substituição ao equipamento danificado.

22.1.15. Os reparos físicos decorrentes do exercício da garantia devem ser executados onde se encontram os equipamentos (modalidade on-site).

22.1.16. Dentro do período de garantia a **CONTRATADA** deverá realizar a substituição definitiva do equipamento, em até 07 (sete) dias corridos, por outro igual ou superior, novo e sem uso, em perfeito estado de funcionamento, quando houver em prazo inferior a 30 (trinta) dias corridos, registro de mais de 04 (quatro) ocorrências de problemas para o mesmo equipamento ou quando o equipamento apresentar defeito irreparável.

22.1.17. Em caso de necessidade de reposição de componentes ou equipamentos durante a vigência da Garantia, este deverá acontecer em até 30 (trinta) dias úteis, ficando a **CONTRATADA** responsável por toda logística, instalação e configuração dos novos equipamentos, assim como pela retirada dos antigos, sem qualquer ônus.

22.1.18. As peças de reposição deverão ser originais do fabricante, de primeiro uso e fornecidas sem custo adicional.

22.1.19. O equipamento ou componente substituto passará à propriedade da **CONTRATADA**, devendo o mesmo ser imediatamente incluído no contrato de manutenção vigente em substituição ao equipamento danificado.

22.1.20. Os reparos básicos decorrentes do exercício da garantia devem ser executados onde se encontram os equipamentos (modalidade on-site).

22.1.21. O serviço de atualização deve incluir correções e execução de medidas necessárias para sanar falhas de funcionamento ou vulnerabilidades.

CLÁUSULA VIGÉSIMA TERCEIRA – DA SUBCONTRATAÇÃO

23.1. É expressamente vedada a subcontratação total ou parcial do objeto.

61/73

23.2. A comercialização de licenças e suporte técnico do fabricante não caracterizam subcontratação.

CLÁUSULA VIGÉSIMA QUARTA – DAS OBRIGAÇÕES DA CONTRATADA

24.1. São obrigações da **CONTRATADA**, além de outras previstas neste Contrato ou decorrentes da natureza do ajuste:

- a) Cumprir fielmente as obrigações contratuais, de acordo com as especificações (cor, formato e tamanho) solicitadas, de forma que os serviços sejam realizados com esmero e perfeição;
- b) Assumir, com exclusividade, todos os impostos e taxas que forem devidos em decorrência do objeto contratado, bem como, as contribuições devidas à Previdência Social, encargos trabalhistas e quaisquer outras despesas que se fizerem necessárias à perfeita execução do objeto deste Contrato, do Termo de Referência e seus Apêndices.
- c) Abster-se de transferir direitos ou obrigações decorrentes do contrato sem a expressa concordância da **CONTRATANTE**.
- d) Não subcontratar o objeto do presente Contrato, sem o consentimento prévio da **CONTRATANTE**, o qual, caso haja, será dado por escrito:
- e) Credenciar junto à **CONTRATANTE** funcionário(s) que atenderá(ão) às solicitações dos serviços objeto deste Contrato;
- f) Substituir, no prazo máximo de 10 (dez) dias a contar do recebimento da notificação formal, os objetos que durante o prazo de garantia, venham apresentar defeitos de fabricação ou quaisquer outros que venham a dificultar ou impossibilitar a sua utilização, desde que, para a sua ocorrência, não tenha contribuído, por ação ou omissão, a **CONTRATANTE**.
- g) Responder, perante a **CONTRATANTE** e terceiros, por eventuais prejuízos e danos decorrentes de sua demora ou de sua omissão, na condução do objeto deste Instrumento sob a sua responsabilidade ou por erros relativos à execução do objeto deste Contrato;
- h) Responsabilizar-se pelo bom comportamento de seus prepostos, podendo a **CONTRATANTE** solicitar a substituição de qualquer indivíduo, cuja permanência seja, a critério da **CONTRATANTE**, considerada inadequada na área de trabalho;
- i) Zelar para que seus prepostos envolvidos na entrega dos materiais contratados se apresentem convenientemente trajados e devidamente identificados;

62/73

- j) Responsabilizar-se pela estrita observância das normas de segurança interna e aquelas determinadas pelo Ministério do Trabalho;
- k) Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados no desempenho dos serviços ou em conexão com eles, ainda que acontecido nas dependências da **CONTRATANTE**;
- l) Entregar os objetos em perfeito estado de uso e funcionamento, de acordo com as especificações exigidas neste Contrato, no Termo de Referência e seus Apêndices;
- m) Promover por sua conta, através de seguros, a cobertura dos riscos a que se julgar exposta em vista das responsabilidades que lhe cabem na execução do objeto deste instrumento.

CLÁUSULA VIGÉSIMA QUINTA - DAS OBRIGAÇÕES DA CONTRATANTE

25.1. São obrigações da Assembleia Legislativa do Estado de Mato Grosso:

- a) Gerenciar, fiscalizar, prestar, por meio de seu representante, as informações necessárias, bem como atestar as Notas Fiscais oriundas das obrigações contraídas;
- b) Emitir pareceres sobre atos relativos à execução do objeto deste, em especial, quanto ao acompanhamento e fiscalização das entregas, à exigência de condições estabelecidas neste Contrato, no Termo de Referência e à proposta de aplicação de sanções;
- c) Assegurar-se do fiel cumprimento das condições estabelecidas neste Contrato, no Termo de Referência, no instrumento convocatório e seus anexos;
- d) Assegurar-se de que os preços contratados são os mais vantajosos para a Administração, por meio de estudo comparativo dos preços praticados pelo mercado;
- e) Proporcionar todas as facilidades para que a contratada possa desempenhar seus serviços dentro das normas deste Contrato;
- f) Comunicar a contratada as irregularidades observadas na execução dos serviços.

CLÁUSULA VIGÉSIMA SEXTA – DAS CONDIÇÕES DE SUSTENTABILIDADE

26.1. Todo documento deverá ser entregue pela **CONTRATADA**, quer seja pelo processo de cópia ou impresso, deverão ser feitos, preferencialmente, através de papel A4 ou papel ofício oriundos de processo de reciclagem, inclusive, os envelopes que forem entregues ao Pregoeiro, preferencialmente deverão ser todos em material reciclado.

63/73

CLÁUSULA VIGÉSIMA SÉTIMA - DO PAGAMENTO

27.1. O pagamento será em até 10 (dez) dias da entrada da Nota Fiscal/Fatura na Secretaria de Planejamento, Orçamento e Finanças, de acordo com a Nota de Empenho e a Nota de Autorização de Despesa - NAD, após o atesto pela fiscalização do recebimento pela **CONTRATANTE**.

27.2. A **CONTRATADA** deverá indicar no corpo da Nota Fiscal/Fatura, descrição do produto (com detalhes), o número e o nome do Banco, Agência e número da conta corrente onde deverá ser feito o pagamento, via ordem bancária e apresentação dos comprovantes atualizados de regularidade abaixo, sob pena de aplicação das penalidades específicas previstas na Cláusula Trigésima:

a) Prova de regularidade fiscal para com a Fazenda Federal, Estadual e Municipal do domicílio ou sede da Contratada, consistindo em certidões ou documento equivalente, emitidos pelos órgãos competentes e dentro dos prazos de validade expresso nas próprias certidões ou documentos;

b) Prova de regularidade fiscal para com a Procuradoria da Fazenda Nacional e para com a Procuradoria Geral do Estado, nos casos em que não sejam emitidas em conjunto às regularidades fiscais;

c) Prova de regularidade perante o Fundo de Garantia por Tempo de Serviço – FGTS (art. 27 da Lei 8.036/90), em plena validade, relativa à **CONTRATADA**;

d) Prova de regularidade perante o Instituto Nacional de Seguridade Social - INSS (art. 195, § 3º da Constituição Federal), em plena validade, relativa à **CONTRATADA**;

e) Certidão Negativa de Débitos Trabalhista – TRT.

27.3. A **CONTRATADA** deverá apresentar **NOTA FISCAL ELETRÔNICA** correspondente produtos efetivamente entregues, nos termos previstos em contrato.

27.4. As Notas Fiscais deverão ser emitidas em nome da Assembleia Legislativa do Estado de Mato Grosso – com o seguinte endereço: Edifício Gov. Dante Martins De Oliveira, Avenida André Antônio Maggi, S/N - CPA - Cuiabá/MT, CNPJ nº 03.929.049/0001-11, e deverão ser entregues no local indicado pela **CONTRATANTE**.

27.5. O pagamento efetuado à adjudicatária não a isentará de suas responsabilidades vinculadas ao fornecimento, especialmente aquelas relacionadas com a qualidade e validade, nem implicará aceitação definitiva do fornecimento;

64/73

27.6. Deverá apresentar a Nota Fiscal de fornecimento/entrada dos produtos/serviços no ato da liquidação, procedimento de conferência.

27.7. Não haverá, sob hipótese alguma, pagamento antecipado;

27.8. Havendo vício a reparar em relação à nota fiscal/fatura apresentada ou em caso de descumprimento pela **CONTRATADA** de obrigação contratual, o prazo constante no item 27.1, poderá ser suspenso até que haja reparação do vício ou adimplemento da obrigação;

27.9. Caso constatado alguma irregularidade nas Notas Fiscais/Faturas, estas serão devolvidas pela Secretaria de Planejamento, Orçamento e Finanças ao fornecedor, para as necessárias correções, com as informações que motivaram sua rejeição, contando-se o prazo para pagamento da data da sua reapresentação;

27.10. Nenhum pagamento será efetuado à empresa adjudicatária enquanto pendente de liquidação qualquer obrigação. Esse fato não será gerador de direito a reajustamento de preços ou a atualização monetária;

27.11. A **CONTRATANTE** não efetuará pagamento de título descontado, ou por meio de cobrança em banco, bem como, os que forem negociados com terceiros por intermédio de operação de *factoring*;

27.12. O pagamento somente será efetuado mediante apresentação da regularidade documental.

27.13. As eventuais despesas bancárias decorrentes de transferência de valores para outras praças ou agências são de responsabilidade da **CONTRATADA**;

27.14. Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pela Administração, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes fórmulas:

$$I = \frac{TX}{100}$$
$$365$$
$$EM = I \times N \times VP, \text{ onde:}$$

I = Índice de atualização financeira;

TX = Percentual da taxa de juros de mora anual;

EM = Encargos moratórios;

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

VP = Valor da parcela em atraso.

27.14.1. Na hipótese de pagamento de juros de mora e demais encargos por atraso, os autos devem ser instruídos com as justificativas e motivos e submetidos à apreciação da autoridade

65/73

competente, que adotará as providências para eventual apuração de responsabilidade, identificação dos envolvidos e imputação de ônus a quem deu causa à mora.

27.15. Caso haja aplicação de multa, o valor será descontado de qualquer fatura ou crédito existente na Assembleia Legislativa em favor da Contratada, se esse valor for superior ao crédito eventualmente existente, a diferença será cobrada administrativamente ou judicialmente, se necessário.

27.15.1. Caso a **CONTRATADA** não tenha nenhum valor a receber da **CONTRATANTE**, ser-lhe-á concedido o prazo de 15 (quinze) dias úteis, contados de sua intimação, para efetuar o pagamento.

27.15.2. Após esse prazo, não sendo efetuado o pagamento, seus dados serão encaminhados ao Órgão competente para que seja inscrita na dívida ativa do Estado, podendo, ainda a Administração proceder a cobrança judicial do valor devido.

27.16. O pagamento da fatura não será considerado como aceitação definitiva do objeto contratado e não isentará a **CONTRATADA** das responsabilidades contratuais quaisquer que sejam.

CLÁUSULA VIGÉSIMA OITAVA – DO REAJUSTE

28.1. Os preços são fixos e irremovíveis no prazo de 12 (doze) meses contados da assinatura do contrato.

28.2. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de 12 (doze) meses contados da data de assinatura do contrato, aplicando-se o IPCA – Índice Nacional de Preços ao Consumidor Amplo, ou outro índice oficial que vier a substituí-lo, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência do prazo acima mencionado.

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

28.4. No caso de atraso ou não divulgação do índice de reajustamento, o **CONTRATANTE**, pagará à **CONTRATADA** a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

28.5. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

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

66/73

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

28.8. O reajuste será realizado por apostilamento.

28.9. O reajuste somente será concedido após análise pelo setor competente e mediante motivação e comprovação, por parte da **CONTRATADA**.

28.10. De forma a explanar acerca do índice escolhido, se faz necessário ressaltar que ante a ausência de normativa própria desta Assembleia Legislativa, que disponha sobre as contratações na área de tecnologia da informação, utilizamos para subsidiar as contratações de serviços e produtos a Instrução Normativa n.º 01/2019 do Governo Federal, que trata das contratações relacionadas a Tecnologia da Informação e que vincula os órgãos da administração pública federal.

28.11. A referida normativa dispõe sobre a necessidade de a utilização do ICTI – Índice de Custos da Tecnologia da Informação, para serviços relacionados a TI, ocorre que em pesquisas realizadas em órgãos públicos da administração federal, tais como TCU e STF (Contrato SEI/STF 0746706, SEI/STF 0489055 Contrato n.º 063/2017, Pregão Eletrônico TCU n.º 080/2019, Pregão Eletrônico n.º 23/2020), observamos que os referidos órgãos utilizam o IPCA – Índice Nacional de Preços ao Consumidor, pois é o que mais se aproxima do efetivo índice inflacionário.

CLÁUSULA VIGÉSIMA NONA – DA RESCISÃO

29.1. O presente Contrato poderá ser rescindido pelos motivos previstos nos artigos 77 e 78 e nas formas estabelecidas no art. 79, acarretando as consequências do art. 80, todos da Lei n.º 8.666/93, nas seguintes hipóteses:

29.1.1. A inexecução total ou parcial do contrato enseja a sua rescisão, com as consequências contratuais e as previstas em lei ou regulamento;

29.1.2. O não cumprimento de cláusulas contratuais, especificações, projetos ou prazos;

29.1.3. O cumprimento irregular de cláusulas contratuais, especificações, projetos e prazos;

29.1.4. A lentidão do seu cumprimento, levando a Administração a comprovar a impossibilidade da conclusão da obra, do serviço ou do fornecimento, nos prazos estipulados;

29.1.5. O atraso injustificado no início da obra, serviço ou fornecimento;

29.1.6. A paralisação da obra, do serviço ou do fornecimento, sem justa causa e prévia comunicação à Administração;

67/73



29.1.7. A subcontratação total do seu objeto, a associação da **CONTRATADA** com outrem, a cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação, não admitidas no edital e no contrato;

29.1.8. Desatendimento das determinações regulares da autoridade designada para acompanhar e fiscalizar a sua execução, assim como as de seus superiores;

29.1.9. O cometimento reiterado de faltas na sua execução, anotadas na forma do § 1º do art. 67 desta Lei;

29.1.10. A decretação de falência ou a instauração de insolvência civil;

29.1.11. A dissolução da sociedade ou o falecimento da **CONTRATADA**;

29.1.12. A alteração social ou a modificação da finalidade ou da estrutura da empresa, que prejudique a execução do contrato;

29.1.13. Razões de interesse público, de alta relevância e amplo conhecimento, justificadas e determinadas pela máxima autoridade da esfera administrativa a que está subordinado a **CONTRATANTE** e exaradas no processo administrativo a que se refere o contrato;

29.1.14. A supressão, por parte da Administração, de obras, serviços ou compras, acarretando modificação do valor inicial do contrato além do limite permitido no § 1º do art. 65 da Lei 8666/93;

29.1.15. A suspensão de sua execução, por ordem escrita da Administração, por prazo superior a 120 (cento e vinte) dias, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra, ou ainda por repetidas suspensões que totalizem o mesmo prazo, independentemente do pagamento obrigatório de indenizações pelas sucessivas e contratualmente imprevistas desmobilizações e mobilizações e outras previstas, assegurado a **CONTRATADA**, nesses casos, o direito de optar pela suspensão do cumprimento das obrigações assumidas até que seja normalizada a situação;

29.1.16. O atraso superior a 90 (noventa) dias dos pagamentos devidos pela Administração decorrentes de obras, serviços ou fornecimento, ou parcelas destes, já recebidos ou executados, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra, assegurado ao contratado o direito de optar pela suspensão do cumprimento de suas obrigações até que seja normalizada a situação;

29.1.17. A não liberação, por parte da Administração, de área, local ou objeto para execução de obra, serviço ou fornecimento, nos prazos contratuais, bem como das fontes de materiais naturais especificadas no projeto;

68/73

29.1.18. A ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da execução do contrato;

29.1.19. Descumprimento do disposto no inciso V, do art. 27 da Lei nº 8.666/93, sem prejuízo das sanções penais cabíveis.

29.2. A rescisão, por algum dos motivos previstos na Lei nº 8.666/93 e suas alterações, não dará à **CONTRATADA** direito a indenização a qualquer título, independentemente de interpelação judicial ou extrajudicial;

29.3. A rescisão acarretará, independentemente de qualquer procedimento judicial ou extrajudicial por parte da **CONTRATANTE**, a retenção dos créditos decorrentes deste Contrato, limitada ao valor dos prejuízos causados, além das sanções previstas neste ajuste até a completa indenização dos danos;

29.4. Fica expressamente acordado que, em caso de rescisão, nenhuma remuneração será cabível, a não ser o ressarcimento de despesas autorizadas pela **CONTRATANTE** e, previstas no presente Contrato e comprovadamente realizadas pela **CONTRATADA**.

29.5. Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa.

CLÁUSULA TRIGÉSIMA – DAS SANÇÕES ADMINISTRATIVAS

30.1. Se a **CONTRATADA** descumprir quaisquer das condições deste instrumento ficará sujeita às penalidades previstas na Lei n. 10.520/2002, bem como nos art. 86 e 87 da Lei 8.666/93, quais sejam:

30.1.1. Por atraso injustificado na entrega do produto;

30.1.2. Atraso de até 10 (dez) dias, multa diária de 0,25% (vinte e cinco centésimos por cento), do valor adjudicado;

30.1.3. Atraso superior a 10 (dez) dias, multa diária de 0,50% (cinquenta centésimos por cento), do valor adjudicado, sobre o total dos dias em atraso, sem prejuízo das demais cominações legais;

30.2. No caso de atraso no recolhimento da multa aplicada, incidirá nova multa sobre o valor devido, equivalente a 0,20% (vinte centésimos por cento) até 10 (dez) dias de atraso e 0,40% (quarenta centésimos por cento) do valor adjudicado, acima desse prazo, calculado sobre o total dos dias em atraso.

69/73

30.3. Pela inexecução parcial ou total das condições estabelecidas neste ato convocatório, a Assembleia Legislativa do Estado de Mato Grosso poderá, garantida a prévia defesa, aplicar, também, as seguintes sanções:

30.3.1. Advertência,

30.3.2. Multa de até 20% (vinte por cento) sobre o valor homologado, atualizado, recolhida no prazo de 15 (quinze) dias corridos, contados da comunicação oficial, sem embargo de indenização dos prejuízos porventura causados a Assembleia Legislativa do Estado de Mato Grosso;

30.3.3. Suspensão temporária de participação em licitação e impedimento de licitar e contratar com a Administração Pública, bem como o cancelamento de seu certificado de registro cadastral no cadastro de fornecedores do Estado de Mato Grosso por prazo não superior a 02 (dois) anos.

30.4. As multas serão descontadas dos créditos da empresa detentora da ata ou cobradas administrativa ou judicialmente.

30.5. As penalidades previstas neste item têm caráter de sanção administrativa, consequentemente, a sua aplicação não exige a empresa detentora da ata, da reparação das eventuais perdas e danos que seu ato venha acarretar a **CONTRATANTE**.

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

30.7. Nas hipóteses de apresentação de documentação inverossímil, cometimento de fraude ou comportamento de modo inidôneo, a licitante poderá sofrer, além dos procedimentos cabíveis de atribuição desta instituição e do previsto no art. 7.º da Lei 10.520/02, quaisquer das sanções adiante previstas, que poderão ser aplicadas cumulativamente:

30.7.1. Desclassificação ou inabilitação, caso o procedimento se encontre em fase de julgamento;

30.7.2. Cancelamento do contrato, se esta já estiver assinada, procedendo-se a paralisação do fornecimento;

30.8. As penalidades serão obrigatoriamente registradas no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Cadastro de Fornecedores do Estado de Mato Grosso, e no caso de ficar impedida de licitar e contratar, a licitante deverá ser descredenciada por igual período, sem prejuízo das multas previstas neste Termo de Referência, Edital e das demais cominações legais.

70/73

CLÁUSULA TRIGÉSIMA PRIMEIRA – DO ACOMPANHAMENTO E FISCALIZAÇÃO

31.1. Para o acompanhamento e a fiscalização da execução do contrato será designada a Comissão de Recebimento de Bens e Serviços, formada por servidores nomeados pela Secretaria de Tecnologia da Informação da Assembleia Legislativa do Estado de Mato Grosso, nos termos do art. 67, Lei nº 8.666, de 1993, que se responsabilizará pelo registro de todas as ocorrências relacionadas com a execução e determinará o que for necessário à regularização de falhas ou defeitos observados;

31.2. A fiscalização de que trata o item anterior não exclui nem reduz a responsabilidade da **CONTRATADA**, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade da Assembleia Legislativa do Estado de Mato Grosso ou de seus agentes, em conformidade com o art. 70 da Lei nº 8.666, de 1993;

31.2.1. A CONTRATADA

31.2.1.1. Deverá possuir o seguinte ator agindo para a execução contratual:

a) Preposto – Funcionário representante da **CONTRATADA**, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto a **CONTRATANTE**, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual.

31.2.1.2. A **CONTRATADA** deverá aceitar, antecipadamente, todos os métodos de inspeção, verificação e controle a serem adotados pela fiscalização, obrigando-se a fornecer-lhe todos os dados, elementos, explicações, esclarecimentos, soluções e comunicações de que esta necessitar e que forem julgados necessários ao cumprimento do objeto deste Contrato.

31.2.1.3. A existência e a atuação da fiscalização em nada restringem a responsabilidade única, integral e exclusiva da contratada, no que concerne ao objeto da respectiva contratação, às implicações próximas e remotas perante a **CONTRATANTE** o ou perante terceiros, do mesmo modo que a ocorrência de irregularidade decorrentes da execução contratual não implica em corresponsabilidade da **CONTRATANTE** ou de seus prepostos, devendo, ainda, a contratada, sem prejuízo das penalidades previstas, proceder ao ressarcimento imediato dos prejuízos apurados e imputados às falhas em suas atividades.

71/73

CLÁUSULA TRIGÉSIMA SEGUNDA– DA GARANTIA

32.1. A **CONTRATADA** deverá apresentar a garantia de execução contratual de 5% (cinco por cento), sobre o valor global da contratação, em uma das modalidades previstas no §1º do art. 56 da Lei nº 8.666/93, no momento da assinatura do contrato.

CLÁUSULA TRIGÉSIMA TERCEIRA– DA CLÁUSULA ANTICORRUPÇÃO

33.1. Para execução deste contrato, nenhuma das partes poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação vantagens financeiras ou benefícios de qualquer espécie, seja de forma direta ou indireta quanto ao objeto deste contrato, ou de outra forma a ele relacionada, o que deve ser observado, ainda, pelos prepostos e colaboradores.

CLÁUSULA TRIGÉSIMA QUARTA– DA SUJEIÇÃO ÀS NORMAS LEGAIS E CONTRATUAIS

34.1. A legislação aplicável a este Contrato será a Lei Estadual nº. 10.534 de 13 de abril de 2017, e, subsidiariamente pela Lei Federal nº 8.666, de 21 de junho de 1993 e suas alterações posteriores, Lei nº. 8.078/1990 (Código de Defesa do Consumidor), demais legislações pertinentes e as condições e especificações estabelecidas no Processo Licitatório Pregão Eletrônico nº. 003/2022 (SGED 2021/1447.1397-5) e no Termo de Referência nº. 019/2021-STI, bem como as cláusulas deste Instrumento.

CLÁUSULA TRIGÉSIMA QUINTA – DAS DISPOSIÇÕES GERAIS

35.1. Integram este Contrato, o Termo de Referência nº. 019/2021-STI e seus anexos, e a proposta comercial apresentada pela **CONTRATADA**.

35.2. Os casos omissos serão resolvidos conforme dispõem as Leis Federais nº 8.078/1990 (Código de Defesa do Consumidor), nº 10.534/2017 e nº 8.666/1993, Código Civil e demais legislações vigentes e pertinentes à matéria;

35.3. A abstenção, por parte da **CONTRATANTE**, de quaisquer direitos e/ou faculdades que lhe assistem em razão deste contrato e/ou lei não importará renúncia a estes, não gerando, pois, precedente invocável.

72/73

CLÁUSULA TRIGÉSIMA SEXTA – DO FORO

36.1 - Fica eleito o foro da cidade de Cuiabá, Estado de Mato Grosso, como competente para dirimir quaisquer dúvidas ou questões decorrentes da execução deste Contrato.

E, por se acharem justas e contratadas, as partes assinam o presente instrumento na presença das testemunhas abaixo, em 3 (três) vias de igual teor e forma, para que produza todos os efeitos legais.

Cuiabá – MT 30 de março de 2022.

<u>CONTRATANTE</u> ASSEMBLEIA LEGISLATIVA DO ESTADO DE MATO GROSSO CNPJ nº 03.929.049/0001-11	<u>DEPUTADOS – MESA DIRETORA</u> Eduardo Botelho: _____ Presidente Max Russi: _____ 1º Secretário
<u>CONTRATADA</u> AVANT TECNOLOGIA E INFORMÁTICA LTDA CNPJ nº. 30.649.749/0001-25	<u>REPRESENTANTE LEGAL</u> Lucas Ribeiro Ganem CNH nº. 00177279769 - DETRAN/DF CPF nº. 866.374.951-15
<u>TESTEMUNHA</u> NOME: _____ RG Nº: _____ CPF Nº: _____ ASSINATURA: _____	<u>TESTEMUNHA</u> NOME: Midiã Maira C. G. de Sá CPF nº 021.211.711-42 RG Nº: _____ CPF : _____ ASSINATURA: _____

**LUCAS
RIBEIRO
GANEM:86
637495115**

Assinado de
forma digital por
LUCAS RIBEIRO
GANEM:86637495
115
Dados: 2022.03.23
16:54:45 -03'00'

