LOGO MARCA DA EMPRESA

NOME COMERCIAL DA EMPRESA

CNPJ Nº

Ao
Governo do Estado de Roraima
Secretaria de Estado da Saúde – SESAU
Gerencia Especial de Cotação – GEC

CARIMBO CNPJ Nº

MODELO DA PROPOSTA DE PREÇOS

PROCESSO Nº. 20101.053816/2026.52

Eventual contratação de empresa especializada para o fornecimento de solução tecnológica integrada de infraestrutura de rede lógica e óptica, conectividade, cibersegurança e governança de Tecnologia da Informação, compreendendo o fornecimento de equipamentos, softwares, licenças, materiais, instalação, configuração, remanejamento, treinamento, garantia, suporte técnico especializado e demais serviços necessários à implantação da solução, destinada à modernização, padronização e fortalecimento da infraestrutura tecnológica das unidades da Secretaria de Estado da Saúde de Roraima – SESAU/RR, na capital e no interior do Estado, visando assegurar a continuidade dos serviços públicos de saúde, a disponibilidade dos sistemas institucionais, a proteção de dados pessoais sensíveis e o atendimento às diretrizes da Lei Geral de Proteção de Dados – LGPD.

LOTE 01						
ITEM	**CATMAT/ CATSER**	**ESPECIFICAÇÃO**	**UND.**	**QTD**	**VALOR UNIT.**	**VALOR TOTAL**
1	27570	Instalação de Novo Ponto de Rede Categoria 6a	UN	3000		
2	27570	Manutenção de Ponto de Rede Categoria 6a	UN	2450		
3	27570	Instalação e Fornecimento de Patch Panel de 24 portas categoria 6a	UN	125		
4	437666	Patch Cord Categoria 6a de 1,5m	UN	3000		
5	437666	Patch Cord Categoria 6a de 2,44m	UN	3000		
6	422721	Rack de Parede 19” de 12U x 550mm	UN	40		
7	617522	Rack de Piso 19" de 44U x 670mm	UN	10		
8	27570	Instalação e/ou Organização de Rack de 19" x 12 RU incluindo as identificações necessárias	UN	50		
9	27570	Instalação e/ou Organização de Rack de 19" x 44 RU incluindo as identificações necessárias	UN	125		
10	27570	Instalação de Cabo Óptico Monomodo Interno/Externo	MT	20000		

11	27570	Instalação de Cabo Óptico Multimodo Interno/Externo	MT	5000		
12	27570	Instalação de DIO e/ou adaptador óptico e seus acessórios	UN	50		
13	27570	Execução de Fusão Direta de Fibra Óptica	UN	250		
VALOR TOTAL LOTE 01						
LOTE 02						
ITEM	**CATMAT/ CATSER**	**ESPECIFICAÇÃO**	**UND.**	**QTD**	**VALOR UNIT.**	**VALOR TOTAL**
14	609689	Switch Tipo I, Layer 2+, 24 portas x 1 Gbps RJ45, 4 x 1 Gbps SFP	UN	70		
15	609689	Switch Tipo II, Layer 2+ POE, 24 portas x 1 Gbps RJ45, 4 x 1 Gbps SFP	UN	15		
16	609689	Switch Tipo III, Layer 2+ POE, 24 portas x 2.5 Gbps RJ45, 4 x 10 Gbps SFP+	UN	30		
17	609689	Switch Tipo IV, Layer 2+, 24 portas x 1 Gbps SFP, 4 x 10 Gbps SFP+	UN	15		
18	609689	Switch Tipo V, Layer 3, 26 portas x 10 Gbps SFP+, 6 x 25 Gbps SFP28	UN	10		
19	393277	Access Point Tipo I - Indoor	UN	180		
20	393277	Access Point Tipo II - Indoor	UN	220		
21	393277	Access Point Tipo III - Outdoor	UN	20		
22	390879	Transceiver Tipo I – 1 Gbps SFP SR	UN	200		
23	390879	Transceiver Tipo II – 10 Gbps SFP+ SR	UN	110		
24	390879	Transceiver Tipo III – 10 Gbps SFP+ LR	UN	35		
25	390879	Transceiver Tipo IV – 25 Gbps SFP28 LR	UN	25		
26	390879	Cabo DAC Tipo I – 25 Gbps SFP28 1 Metro	UN	20		
27	27464	Software de Gerência Centralizada	UN	560		
28	27570	Serviços de Instalação, Migração e Configuração do Lote	SRV	560		
29	27570	Repasse de Conhecimento	SRV	10		
VALOR TOTAL 02						
LOTE 03						
ITEM	**CATMAT/ CATSER**	**ESPECIFICAÇÃO**	**UND**	**QTD.**	**VALOR UNIT.**	**VALOR TOTAL**
30	609340	NEXT GENERATION FIREWALL (NGFW) – Com garantia e suporte de 60 (sessenta) meses	UN	2		
31	609340	SOLUÇÃO DE NDR (NETWORK DETECTION AND RESPONSE) – Com garantia e suporte de 60 (sessenta) meses	UN	1		
32	609340	SOLUÇÃO DE EXTENDED DETECTION AND RESPONSE (XDR) – Com garantia e suporte de 60 (sessenta) meses	UN	1		
33	27570	SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DO NDR, XDR e NGFW	SRV	1		

34	27472	SERVIÇO DE SOC (SECURITY OPERATIONS CENTER)	SRV	1		
VALOR TOTAL 03						

VALIDADE DE 180 DIAS.

Favor mencionar os dados abaixo na proposta:

a) **Dados cadastrais;**
b) **Prazo de entrega;**
c) **Demais impostos e custos, deverão ser inclusos;**
d) **Assinatura, data e endereço;**
e) **E-mail e número de telefone (válidos)**

_____

E-mail:

_____

Telefone:

_____

Local e Data

_____

(Assinatura e Carimbo do Representante Legal)

OBS: RESPONDER PARA O E-MAIL – cotacao.cgplan@saude.rr.gov.br

Telefone: (95) 98404-1642 (também é WhatsApp)

INSTRUÇÃO NORMATIVA Nº 65, DE 7 DE JULHO DE 2021

Art. 5º A pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição e contratação de serviços em geral será realizada mediante a utilização dos seguintes parâmetros, empregados de forma combinada ou não:
[...]
IV - Pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital;

DECRETO Nº 39.050-E, DE 18 DE AGOSTO DE 2025

Art. 17º A pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição de bens e contratação de serviços em geral será realizada mediante a utilização dos seguintes parâmetros, empregados de forma combinada ou não:

[...]

IV - Pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital;

INFRMAÇÕES ADICIONAIS:

19.2. Prazo de Entrega e Execução dos Lotes 02 e 03

19.2.1. Os equipamentos, softwares, licenças e demais componentes referentes aos **Lotes 02 e 03** deverão ser disponibilizados no prazo máximo de **120 (cento e vinte) dias úteis**, contado do recebimento da respectiva Ordem de Fornecimento e/ou Ordem de Serviço pela Contratada, observados os quantitativos e as condições nela estabelecidos.

19.2.2. Quando os componentes demandados dependerem de instalação, configuração, integração, ativação, migração, testes ou outras atividades necessárias ao seu funcionamento, essas etapas deverão integrar o atendimento da respectiva demanda, conforme os prazos e condições estabelecidos no Termo de Referência e na Ordem correspondente.

19.2.3. A simples entrega física dos equipamentos ou disponibilização das licenças não caracterizará a conclusão integral da demanda quando houver serviços associados necessários à implantação e ao funcionamento da solução.

19.2.4. O marco inicial das garantias, licenças, subscrições, suporte e demais períodos associados à solução deverá ser expressamente definido no Termo de Referência, evitando o início antecipado de períodos contratados antes da efetiva disponibilização ou ativação do respectivo componente, quando tecnicamente aplicável.

19.3. Prazo de Entrega e Execução do Lote 01

19.3.1. Os materiais e serviços referentes ao **Lote 01** serão demandados conforme a necessidade da SESAU/RR, mediante emissão de Ordem de Fornecimento e/ou Ordem de Serviço.

19.3.2. Cada demanda deverá ser atendida no prazo máximo de **30 (trinta) dias úteis**, contado do recebimento da respectiva ordem pela Contratada, observados os itens, quantitativos, locais e condições de execução nela estabelecidos.

19.3.3. O prazo previsto no item 19.3.2 poderá, excepcionalmente, ser prorrogado mediante solicitação formal e devidamente fundamentada da Contratada, apresentada antes do término do prazo inicialmente estabelecido e condicionada à análise e à aprovação da Contratante.

19.3.4. A eventual prorrogação deverá considerar a natureza, a complexidade e as circunstâncias da respectiva demanda, sem afastar a responsabilidade da Contratada por atrasos que lhe sejam imputáveis.

19.4. Locais de Entrega e Execução

19.4.1. Os bens permanentes, quando não houver determinação de entrega ou instalação diretamente em unidade específica da SESAU/RR, deverão ser entregues no endereço **Rua Madrid, nº 180, Bairro Aeroporto, Boa Vista/RR, CEP 69310-043**, em dias úteis, de segunda a sexta-feira, exceto feriados, em horário previamente acordado com a fiscalização ou com o setor responsável pelo recebimento.

19.4.2. Quando a Ordem de Fornecimento e/ou Ordem de Serviço determinar entrega, instalação ou execução diretamente em uma das unidades ou estruturas contempladas pela contratação, a Contratada deverá observar o endereço, as condições de acesso e as demais orientações indicadas pela Contratante.

19.4.3. A execução diretamente nas unidades deverá ser previamente coordenada com os responsáveis indicados pela Administração, especialmente quando as atividades puderem interferir no funcionamento da infraestrutura tecnológica ou nas atividades administrativas e assistenciais.

19.5. Transporte e Acondicionamento

19.5.1. Todos os custos relacionados ao transporte, frete, seguro, carga, descarga, movimentação, acondicionamento e demais despesas necessárias à entrega dos equipamentos e materiais e à execução dos serviços nos locais determinados pela Administração serão de responsabilidade da Contratada, não cabendo cobrança adicional à Contratante.

19.5.2. Os equipamentos e materiais deverão ser entregues em embalagens adequadas às suas características, capazes de preservar sua integridade durante o transporte e armazenamento e contendo as identificações necessárias à conferência e rastreabilidade dos itens.

19.5.3. No momento do recebimento serão verificadas as condições aparentes dos equipamentos e materiais, podendo ser recusados itens que apresentem avarias, sinais de uso indevido, oxidação, danos físicos, violação incompatível com as condições normais de fornecimento ou outras situações capazes de comprometer sua integridade, funcionamento, segurança ou garantia.

ANEXO I

DO ESTUDO TÉCNICO PRELIMINAR CARACTERÍSTICAS E ESPECIFICAÇÕES TÉCNICAS

LOTE 01				
ITEM	**CATMAT/ CATSERV**	**ESPECIFICAÇÃO**	**UNID**	**QUANTIDADE**
1	27570	**Instalação de Novo Ponto de Rede Categoria 6a**, fornecimento de cabo tipo U/UTP com extensão de até 90 metros, acompanhado de 1 (uma) Tomada Fêmea RJ45 para ativação de um ponto no rack, tudo de categoria 6A. O cabo deverá estar devidamente conectorizado em ambas as extremidades (Patch Panel e Tomada Fêmea RJ45). Instalação da infraestrutura externa/interna necessária para conectar o ponto, partindo do rack indicado até a estação de trabalho ou equipamento. Isso inclui canaletas e/ou eletrocalhas, terminando em espelho ou caixa de sobrepor, conforme necessário. As canaletas devem ter tamanho de 55 x 20 x 2000mm de 2 vias e/ou 120 x 35 x 2000mm de 4 vias. Também é necessário fornecer todos os acessórios necessários, como fixa cabos, curvas internas/externas, conexões, terminais de extremidade, caixas de derivação, buchas, parafusos, etc. As eletrocalhas devem ser do tipo perfurada, com dimensões de 100x50mm e/ou 50x50mm, para acomodar adequadamente todos os cabos e atender às normas para taxa de ocupação, considerando a quantidade de pontos solicitada e prevendo margem para futuras expansões, além de pêndulos, tirantes e/ou mão francesa para fixação em paredes e lajes. Todos os acessórios necessários para a instalação e acabamento do ponto devem ser considerados. Os elementos do ponto, como espelho, caixa, cabo e painel, devem ser identificados adequadamente utilizando rotuladora eletrônica e fita adequada à superfície. Por fim, solicita-se a apresentação de um Relatório de Certificação de Rede em formato eletrônico (PDF e arquivo nativo do certificador) com resultado "PASSA", atestando que o ponto atende os requisitos da categoria 6A, deverá possuir conformidade com as especificações técnicas contidas neste documento conforme os itens 1.1, 1.2 e 1.14 do ANEXO I.	UN	3000
2	27570	**Manutenção de Ponto de Rede Categoria 6a**, deverá ser feito diagnóstico através de ferramentas específicas para identificação do problema. A manutenção deverá contemplar todos as peças partes necessárias para sanar o problema, seja ela novo lançamento de cabo, conectores fêmeas, caixa de sobrepor com tampa, conectorização do conector fêmea e do patch panel e quando o patch panel for estruturado substituição do conector do patch panel, quando identificado a necessidade de nova fixação de canaletas também deverá ser fornecido buchas e parafusos/fitas dupla face, não sendo necessário a substituição de tubulação existente para substituição do cabo de par trançado. Os materiais fornecidos devem estar em conformidade com a categoria do cabo 6a e todos os materiais utilizados deverão ser novos e de um único fabricante ou comprovado através de documento a compatibilidade dos componentes que	UN	2450

		eventualmente sejam de marcas diferentes. Deverá possuir rotulação de identificação no espelho, no cabo a ser utilizado e no patch panel, a fim de permitir organização da rede. Apresentação de um Relatório de Certificação de Rede em formato eletrônico (PDF e arquivo nativo do certificador) com resultado "PASSA", garantindo que o ponto atende ou supera os requisitos da categoria 6a, deverá possuir conformidade com as especificações técnicas contidas neste documento conforme o item 1.1, 1.2 e 1.14 do ANEXO I.		
3	27570	**Instalação e Fornecimento de Patch Panel de 24 portas Categoria 6a,** o mesmo deve possuir conformidade com as especificações técnicas especificadas neste documento conforme o item 1.4 do ANEXO I e crimpagem de todos os cabos necessários.	UN	125
4	437666	**Patch Cord Categoria 6a de 1,5m**, deverá possuir conformidade com as especificações técnicas contidas neste documento conforme o item 1.3 do ANEXO I, tamanho de no mínimo 1,5 metros.	UN	3000
5	437666	**Patch Cord Categoria 6a de 2,44m**, deverá possuir conformidade com as especificações técnicas contidas neste documento conforme o item 1.3 do ANEXO I, tamanho de no mínimo 2,44 metros.	UN	3000
6	422721	**Rack de Parede 19” de 12U x 550mm,** com finalidade de proporcionar praticidade e organização dos equipamentos de rede, fixação na parede, deve ser totalmente fechado, prover plano de fixação padrão 19", deverá ser na cor preta e possuir porta de vidro e deve atender todas as especificações técnicas contidas neste documento conforme o item 1.12 do ANEXO I.	UN	40
7	617522	**Rack de Piso 19'' de 44U x 670mm,** com finalidade de proporcionar praticidade e organização dos equipamentos de rede, deve ser totalmente fechado, prover plano de fixação padrão 19", deverá ser na cor preta e possuir porta de vidro e deve atender todas as especificações técnicas contidas neste documento conforme o item 1.13 do ANEXO I.	UN	10
8	27570	**Instalação e/ou Organização de Rack de 19'' x 12 RU incluindo as identificações necessárias**, instalação e/ou organização de rack de 12 RU, com respectiva alimentação elétrica, deverá ser organizado todos os cabos na parte traseira e frontal dos racks, quando necessário a rotulação de todos os cabos, patch panel de acordo com a informação repassada pela contratante, como também a acomodação dos equipamentos de TI, deverá ser contemplado também todos os outros insumos para organização de rack, como parafuso lentilha, porta gaiola, parafusos de fixação e buchas, velcros, organizadores de cabos frontais e traseiros, deverá ser feita seguindo os padrões da ABNT para arrumação de cabos dentro do rack para melhor distribuição de espaço. Observação: Não serão fornecidos para esse serviço rack, patch cords, patch panel e conectores fêmea de patch panel, visto que, estes estão contemplados em outros itens deste termo.	UN	50
9	27570	**Instalação e Organização de Rack de 19'' x 44 RU incluindo as identificações necessárias**, instalação e organização de rack de 44 RU, com respectiva alimentação elétrica, deverá ser organizado todos os cabos na parte traseira e frontal dos racks, quando necessário a rotulação de todos os cabos, patch panel de acordo com a informação repassada pela contratante, como também a acomodação dos equipamentos de TI, deverá ser contemplado também todos os outros insumos para organização de rack, como parafuso lentilha, porta gaiola, parafusos de fixação e buchas, velcros, organizadores de cabos frontais e traseiros, deverá ser feita seguindo os padrões da ABNT para arrumação de cabos dentro do rack para melhor distribuição de espaço. Observação: Não serão fornecidos para esse serviço rack, patch cords, patch panel e conectores fêmea de patch panel, visto que, estes estão contemplados em outros itens deste termo.	UN	125
10	27570	**Instalação de Cabo Óptico Monomodo Interno/Externo**, consiste na prestação de serviços de fornecimento e lançamento de cabo óptico conforme o item 1.8 do ANEXO I, todos os materiais e acessórios necessários para o lançamento dos cabos ópticos devem ser fornecidos e instalados, como abraçadeiras bap ajustáveis, olhal completo para ancoragem, alças preformadas, caixas de emenda óptica, etc. O cabo óptico deve possuir as características discriminadas conforme o item 1.8 e deve ser identificado por etiqueta e certificado mediante os seguintes testes, deve realizar teste de perda óptica OLTS utilizando método de referência de 1 jumper, apresentando relatório em formato eletrônico (PDF e arquivo nativo do OLTS – Optical Loss Test System) com resultado “PASSA” e listagem dos padrões de rede aferidos e em conformidade, os testes OLTS devem contemplar cálculo prévio de estimativa de atenuação de sinal óptico em dB, deve realizar teste OTDR, apresentando relatório em formato	MT	20000

		eletrônico (PDF e arquivo nativo do OTDR) com gráfico e lista de eventos de atenuações e reflexões ópticas identificados.		
11	27570	**Instalação de Cabo Óptico Multimodo Interno/Externo**, consiste na prestação de serviços de fornecimento e lançamento de cabo óptico conforme o item 1.6 do ANEXO I, todos os materiais e acessórios necessários para o lançamento dos cabos ópticos devem ser fornecidos e instalados, sejam eles conduites, velcros, abraçadeiras, etc. O cabo óptico deve possuir as características discriminadas conforme o item 1.6 e deve ser identificado por etiqueta e certificado mediante os seguintes testes, deve realizar teste de perda óptica OLTS utilizando método de referência de 1 jumper, apresentando relatório em formato eletrônico (PDF e arquivo nativo do OLTS – Optical Loss Test System) com resultado "PASSA" e listagem dos padrões de rede aferidos e em conformidade, os testes OLTS devem contemplar cálculo prévio de estimativa de atenuação de sinal óptico em dB, deve realizar teste OTDR, apresentando relatório em formato eletrônico (PDF e arquivo nativo do OTDR) com gráfico e lista de eventos de atenuações e reflexões ópticas identificados.	MT	5000
12	27570	**Instalação de DIO e/ou adaptador óptico e seus acessórios**, consiste na instalação de DIO e/ou adaptador óptico e seus respectivos acessórios (pigtails, bandejas de emenda, tampas de proteção, etc) destinados a proteger e abrigar emendas diretas ou derivadas de cabos ópticos. O DIO e/ou adaptador óptico deve possuir as características discriminadas conforme os itens 1.9, 1.10, 1.11 do ANEXO I, deve ser identificado adequadamente via etiquetagem.	UN	50
13	27570	**Execução de Fusão Direta de Fibra Óptica,** deverá ser realizado serviço de emendas em fibras ópticas, utilizando o método de fusão, em uma caixa de emenda aérea, terminador óptico ou DIO (Distribuidor Interno Óptico) seja ele de qualquer tipo ou capacidade para terminação de cabo óptico. Será realizada confecção de emendas em fibras ópticas por fusão, garantindo perdas não superiores a 0,3 dB. Após a fusão da emenda, será fornecido um relatório contendo as seguintes informações: Número da emenda; Local da emenda; Número de fibras; Informações dos cabos (origem – destino); Tipo de caixa de emenda utilizada; Data da emenda; Valor da perda na fusão (registrado pelo OTDR); Executor da emenda.	UN	250
LOTE 02				
ITEM	**CATMAT/ CATSERV**	**ESPECIFICAÇÃO**	**UNID**	**QUANTIDADE**
1	609689	**Switch Tipo I, Layer 2+, 24 portas x 1 Gbps RJ45, 4 x 1 Gbps SFP**, deverá possuir conformidade com as especificações técnicas contidas neste documento conforme o item 2.1 do ANEXO I.	UN	70
2	609689	**Switch Tipo II, Layer 2+ POE, 24 portas x 1 Gbps RJ45, 4 x 1 Gbps SFP**, deverá possuir conformidade com as especificações técnicas contidas neste documento conforme o item 2.2 do ANEXO I.	UN	15
3	609689	**Switch Tipo III, Layer 2+ POE, 24 portas x 2.5 Gbps RJ45, 4 x 10 Gbps SFP+**, deverá possuir conformidade com as especificações técnicas contidas neste documento conforme o item 2.3 do ANEXO I.	UN	30
4	609689	**Switch Tipo IV, Layer 2+, 24 portas x 1 Gbps SFP, 4 x 10 Gbps SFP+**, deverá possuir conformidade com as especificações técnicas contidas neste documento conforme o item 2.4 do ANEXO I.	UN	15
5	609689	**Switch Tipo V, Layer 3, 26 portas x 10 Gbps SFP+, 6 x 25 Gbps SFP28**, deverá possuir conformidade com as especificações técnicas contidas neste documento conforme o item 2.5 do ANEXO I.	UN	10
6	393277	**Access Point Tipo I – Indoor**, deverá possuir conformidade com as especificações técnicas contidas neste documento conforme o item 2.6 do ANEXO I.	UN	180
7	393277	**Access Point Tipo II – Indoor**, deverá possuir conformidade com as especificações técnicas contidas neste documento conforme o item 2.7 do ANEXO I.	UN	220
8	393277	**Access Point Tipo III - Outdoor**, deverá possuir conformidade com as especificações técnicas contidas neste documento conforme o item 2.8 do ANEXO I.	UN	20

9	390879	**Transceiver Tipo I – 1 Gbps SFP SR**, deverá possuir conformidade com as especificações técnicas contidas neste documento conforme o item 2.9 do ANEXO I.	UN	200
10	390879	**Transceiver Tipo II – 10 Gbps SFP+ SR**, deverá possuir conformidade com as especificações técnicas contidas neste documento conforme o item 2.10 do ANEXO I.	UN	110
11	390879	**Transceiver Tipo III – 10 Gbps SFP+ LR**, deverá possuir conformidade com as especificações técnicas contidas neste documento conforme o item 2.11 do ANEXO I.	UN	35
12	390879	**Transceiver Tipo IV – 25 Gbps SFP28 LR**, deverá possuir conformidade com as especificações técnicas contidas neste documento conforme o item 2.12 do ANEXO I.	UN	25
13	390879	**Cabo DAC Tipo I – 25 Gbps SFP28 1 Metro**, deverá possuir conformidade com as especificações técnicas contidas neste documento conforme o item 2.13 do ANEXO I.	UN	20
14	27464	**Software de Gerência Centralizado**, Licença para Switchs e Access Points, deverá possuir conformidade com as especificações técnicas contidas neste documento conforme o item 2.14 do ANEXO I.	UN	560
15	27570	**Serviços de Instalação, Migração e Configuração do Lote,** conforme todas as demandas especificações técnicas contidas neste documento conforme o item 2.15 do ANEXO I.	SRV	560
16	27570	**Repasse de Conhecimento,** conforme todas as demandas especificações técnicas contidas neste documento conforme o item 2.16 do ANEXO I.	SRV	10
LOTE 03				
ITEM	**CATMAT/ CATSERV**	**ESPECIFICAÇÃO**	**UNID**	**QUANTIDADE**
1	609340	**NEXT GENERATION FIREWALL (NGFW) – Com garantia e suporte de 60 (sessenta) meses**, conforme todas as demandas especificações técnicas contidas neste documento conforme o item 3.1 do ANEXO I.	UN	2
2	609340	**SOLUÇÃO DE NDR (NETWORK DETECTION AND RESPONSE) – Com garantia e suporte de 60 (sessenta) meses**, conforme todas as demandas especificações técnicas contidas neste documento conforme o item 3.2 do ANEXO I.	UN	1
3	609340	**SOLUÇÃO DE EXTENDED DETECTION AND RESPONSE (XDR) – Com garantia e suporte de 60 (sessenta) meses**, conforme todas as demandas especificações técnicas contidas neste documento conforme o item 3.3 do ANEXO I.	UN	1
4	27570	**SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DO NDR, XDR e NGFW**, conforme todas as demandas especificações técnicas contidas neste documento conforme o item 3.4 do ANEXO I.	SRV	1
5	27472	**SERVIÇO DE SOC (SECURITY OPERATIONS CENTER),** conforme todas as demandas especificações técnicas contidas neste documento conforme o item 3.6 do ANEXO I.	SRV	1

ESPECIFICAÇÕES TÉCNICAS DOS MATERIAIS DE CABEAMENTO METÁLICO E ÓPTICO (LOTE 01)

Todos os componentes de conectividade relacionados à solução de Cabeamento Metálico U/UTP e Cabeamento Óptico (LOTE 01) devem ser de um único fabricante, visando assegurar a perfeita interoperabilidade dos produtos entre si, bem como assegurar o desempenho dos mesmos. Os cabos de transmissão de dados devem possuir homologação ANATEL vigente. A seguir as especificações técnicas mínimas exigidas para os componentes da rede estruturada metálica e rede de fibra óptica:

1.1 Cabo LSZH U/UTP Categoria 6A

Os Cabos U/UTP deverão possuir as seguintes características técnicas obrigatórias:

- 1.1.1 Cumprir ou superar as especificações da norma ANSI/TIA-568.2-D - Transmission Performance Specifications for 4-Par 100 Ω Category 6A Cabling.
- 1.1.2 O cabo deve ser do tipo U/UTP.
- 1.1.3 Existir compatibilidade mecânica e elétrica dos produtos de Categoria 6A com as categorias anteriores.
- 1.1.4 Ter o código de cores de pares conforme abaixo:
- 1.1.5 Par 1: Azul-Branco.
- 1.1.6 Par 2: Laranja-Branco.
- 1.1.7 Par 3: Verde-Branco.
- 1.1.8 Par 4: Marrom-Branco.
- 1.1.9 Tensão Máxima: 11.5 kg / Bitola: 24 AWG.
- 1.1.10 Temperatura de Operação: -20°C à 60°C.
- 1.1.11 Deve suportar transmissões de 100Mbps, 1Gbps e 10Gbps em canais de até 100 metros.
- 1.1.12 Possuir certificação de desempenho elétrico do cabo por laboratório Independente, segundo as especificações da norma ANSI/TIA 568- D.
- 1.1.13 Deve estar em conformidade com as recomendações da IEEE 802.3bt Type 4 para trasmissões PoE.
- 1.1.14 Diâmetro nominal de até 7 mm.
- 1.1.15 O cabo deve ser do tipo LSZH.
- 1.1.16 Método de teste de fumaça: IEC 61034-2.
- 1.1.17 Método de teste de gases ácidos: IEC 60754-2.
- 1.1.18 Método de teste de chamas: IEC 60332-3-22.
- 1.1.19 O cabo deve atender a classificação IEC 60332-3-22 – teste mais rigoroso de queima realizado em feixes de cabos, garantindo mais segurança para os ambientes onde os cabos são instalados. Não serão aceitas certificações onde o teste de queima é realizado com apenas um (01) cabo na queima.
- 1.1.20 Na capa do cabo deverá ter impressa a seguinte informação: nome do fabricante, tipo de cabo, número de pares, tipo de material de capa, as marcas de medição sequenciais de comprimento e o número da Anatel.
- 1.1.21 Possuir certificado ANATEL referente à Categoria 6A em nome do fabricante ofertado.
- 1.1.22 Devem estar de acordo com a diretiva RoHS 2002/95/EC.
- 1.1.23 Todos os componentes da solução que compõe a solução de cabeamento estruturado em cobre, tais como os Patch Panels, Conectores, Cabos devem ser de um único fabricante, garantindo assim total compatibilidade na instalação dos mesmos.

1.2 Conector RJ-45 U/UTP Fêmea Categoria 6A

Os conectores RJ-45 deverão possuir as seguintes características técnicas obrigatórias:

- 1.2.1 Conector deve ser entregue no padrão U/UTP.

- 1.2.2 Devem ser entregues na cor branca.
- 1.2.3 Devem ser utilizados conectores RJ45 de 8 pinos categoria 6A cumprindo ou superando as especificações da norma ANSI/TIA-568.2-D.
- 1.2.4 Devem garantir que os pares fiquem minimamente destorcidos até o ponto de conexão com as lâminas dentro do conector, devendo ainda suportar re-conexões sem deterioração física, além de conexões frontais com "patch cord", atendendo os parâmetros estipulados pelas normas de teste e desempenho (ISO/IEC 11801).
- 1.2.5 Os conectores devem aceitar ferramentas de conexão rápida (tipo alicate) ou ferramentas de impacto – "punch down" – tipo 110 para crimpagem dos cabos dos mesmos.
- 1.2.6 Deve atender a requisitos de flamabilidade de acordo com padrão UL 94 V-0.
- 1.2.7 Deve estar em conformidade com as recomendações da IEEE 802.3bt Type 4 para trasmissões PoE.
- 1.2.8 Deve apresentar teste em canal para 04 conexões para a Categoria 6A emitida por laboratório oficial.
- 1.2.9 Devem ser do tipo IDC – Insulation Displacement Contact (contato por deslocamento do isolador dielétrico) angulado – que aceitem condutor sólido unifilar medindo entre 22 AWG a 26 AWG. O "jack" deve ainda poder ser instalado em pontos de consolidação ou caixas de superfície, permitindo compatibilidade na montagem nestes produtos.
- 1.2.10 Os contatos do conector RJ-45 Macho deverão ser banhados a ouro sobre níquel.
- 1.2.11 Temperatura de operação entre -10 °C a +60 °C.
- 1.2.12 Devem aceitar padrão de conexão T568A ou T568B na parte traseira do mesmo.
- 1.2.13 Devem estar de acordo com a diretiva RoHS 2002/95/EC.
- 1.2.14 Todos os componentes da solução que compõe a solução metálica de cabeamento estruturado, tais como os Patch Panels, Conectores, Cabos metálicos devem ser de um único fabricante, garantindo assim total compatibilidade na instalação dos mesmos.

1.3 Patch Cord Categoria 6A U/UTP LSZH

Os Patch Cords deverão possuir as seguintes características técnicas obrigatórias:

- 1.3.1 Devem atender as recomendações da ANSI/TIA-568.2-D para categoria 6A.
- 1.3.2 A performance do Alien Crosstalk deve ser garantida para as instalações com 4 conexões em canais de até 100 metros de comprimento.
- 1.3.3 Devem ser entregues no modelo U/UTP.
- 1.3.4 O cabo deve ser do tipo LSZH.
- 1.3.5 Devem ser entregues na cor preta ou azul.
- 1.3.6 Deve suportar transmissões de até 10Gbps (10 gigabit por segundo).
- 1.3.7 Deve estar em conformidade com as recomendações da IEEE 802.3bt Type 4 para trasmissões PoE.
- 1.3.8 Devem ser nos comprimentos de no mínimo 1,50 e 2,44 metros de acordo com o solicitado em cada item.

- 1.3.9 Os patch cords para a conexão dos equipamentos do usuário final devem ser construídos com conectores macho (plug) tipo RJ45 em ambas as extremidades.
- 1.3.10 O cabo utilizado para estes patch cords deverá ser cabo Flexível (multifilar) categoria 6A de 24 AWG de cobre em par trançado e ter as mesmas características de desempenho nominais do cabeamento horizontal especificado.
- 1.3.11 Deve ser montado usando mapa de pinagem T568B.
- 1.3.12 Suportar ciclos de inserção de 750 vezes no mínimo.
- 1.3.13 O cabo deve ser do tipo LSZH de acordo com a norma IEC 60332-3-22.
- 1.3.14 Método de teste de gases ácidos: IEC 60754-2.
- 1.3.15 Método de teste de fumaça: IEC 61034-2.
- 1.3.16 Deve possuir certificação ANATEL referente à Categoria 6A em nome do fabricante ofertado.
- 1.3.17 Todos os componentes da solução que compõe a solução metálica de cabeamento estruturado, tais como os Patch Panels, Conectores, Cabos metálicos devem ser de um único fabricante, garantindo assim total compatibilidade na instalação dos mesmos.

1.4 Patch Panel Categoria 6A - 24 portas

Os Patch Panels deverão possuir as seguintes características técnicas obrigatórias:

- 1.4.1 Deve ser descarregado e possuir 24 portas de conexão para instalação de RJ-45.
- 1.4.2 Deve possuir painel frontal em plástico, não-propagante a chama na cor preta.
- 1.4.3 Devem ser entregues no modelo U/UTP, não sendo aceitos modelos blindados para este projeto.
- 1.4.4 Estrutura em aço e termoplástico de alto impacto.
- 1.4.5 Apresentar largura de 19”, conforme requisitos da norma ANSI/TIA-310D e altura de 1U.
- 1.4.6 Deve possuir identificação do fabricante no corpo do produto.
- 1.4.7 Deve possuir identificação dos conectores na parte frontal do Patch Panel.
- 1.4.8 Deve atender a requisitos de flamabilidade de acordo com padrão UL 94 V-0.
- 1.4.9 Os patch panels deverão acompanhar os 24 conectores RJ-45 fêmea categoria 6a para preenchimento do mesmo conforme as especificações do item 1.2 deste anexo na cor preta.
- 1.4.10 O painel deve possuir porta etiquetas para identificação das portas e esta devem ser instaladas e protegidas por proteção plástica.
- 1.4.11 Os patch panels deverão atender a diretiva RoHS 2002/95/EC.
- 1.4.12 O painel deve possuir certificação UL ou ETL Listed.
- 1.4.13 O patch panel deve estar preparado para receber sistema de gerenciamento de rede inteligente.
- 1.4.14 Todos os componentes da solução que compõe a solução metálica de cabeamento estruturado, tais como os Patch Panels, Conectores, Cabos metálicos devem ser de um único fabricante, garantindo assim total compatibilidade na instalação dos mesmos.

1.5 Cordão Óptico Duplex Multimodo LC/LC

Os cordões ópticos deverão possuir as seguintes características técnicas obrigatórias:

- 1.5.1 Apresentar perda de retorno mínima de 27 dB.
- 1.5.2 Apresentar perda por inserção máxima de 0.3 dB.
- 1.5.3 O produto deve ser testado em fábrica.
- 1.5.4 Deve ser fornecido no padrão duplex com terminações de conectores LC/UPC.
- 1.5.5 Utilizar padrão “zip-cord” de reunião das fibras para diâmetro de 1.8mm.
- 1.5.6 Deverá ser constituído de fibras ópticas multimodo do tipo OM4.
- 1.5.7 Deve possuir classificação LSZH (IEC 60332-3).
- 1.5.8 A fibra deve ser multimodo, de índice gradual com especificações de 50/125µm e devendo suportar velocidades de transmissão de até 10 Gbps, para comprimentos de até 550 metros com comprimentos de onda de 850 nm para a IEEE802.3ae.
- 1.5.9 Largura de banda mínima para:
- 1.5.10 850 nm: 4700 MHz-km (laser), 3500 MHz-km (OFL).
- 1.5.11 1300 nm: 500 MHz-km (laser), 500 MHz-km (OFL).
- 1.5.12 Durabilidade de acoplamento: acréscimo máximo de < 0.20 dB depois de 500 acoplamentos;
- 1.5.13 Deve possuir comprimento mínimo de 3 metros.
- 1.5.14 Devem estar de acordo com a diretiva RoHS 2002/95/EC.
- 1.5.15 Todos os componentes da solução que compõe a solução do cabeamento estruturado, tais como, Patch Panels Metálicos, Bastidores Ópticos, Cabos ópticos e metálicos devem ser de um único fabricante, garantindo assim total compatibilidade na instalação dos mesmos.

1.6 Cabos Ópticos Indoor / Outdoor – Multimodo OM4

Os cabos ópticos deverão possuir as seguintes características técnicas obrigatórias:

- 1.6.1 Deverá ser formado por 12 fibras ópticas multimodo do tipo OM4.
- 1.6.2 Deverá suportar instalações em ambientes internos e externos.
- 1.6.3 Deverá ser tight buffer obrigatoriamente.
- 1.6.4 Deverá possuir capa na cor preta.
- 1.6.5 Deve cumprir ou superar as especificações da norma ANSI/TIA-492AAAF.
- 1.6.6 O diâmetro do núcleo das fibras deve ser de 50µm e o diâmetro da via deve ser de 125µm.
- 1.6.7 O cabo de fibra óptica deve ser do tipo LSZH para distribuição interna e construção Tight Buffered de 900 µm para uso interno/externo (não-geleada).
- 1.6.8 Deve possuir peso máximo de 50.0 kg/km.
- 1.6.9 Deve possuir diâmetro máximo de 7.3 mm.
- 1.6.10 Os parâmetros mínimos de temperatura que a fibra óptica deve suportar sem que sua operação e rendimento sejam afetados deve ser entre -40 ºC e +70 ºC.
- 1.6.11 O comprimento de Onda que a fibra deverá transmitir será nas janelas de 850nm e 1300 nm.
- 1.6.12 A atenuação máxima permitida será de 3 dB/km @ 850 nm e 1 dB/km @ 1300 nm.

- 1.6.13 A largura de Banda da fibra deverá ser no mínimo de 3500 MHz/km @ 850 nm e 500 MHz/KM @ 1300 nm.
- 1.6.14 Os cabos devem atender, para teste de flamabilidade as normas IEC 60332-3, IEC 60754-2, IEC 61034-2, UL 1666 e UL 1685.
- 1.6.15 O cabo de atender as normas ANSI/ICEA S-104-696, EN 187105, Telcordia GR-20 CORE Issue 3 (penetração de água) e Telcordia GR-409 CORE Issue 2.
- 1.6.16 Deverá ser entregue, junto com a entrega dos cabos, relatórios de testes do lote do cabo entregue para a obra, contendo os seguintes dados e resultados dos seguintes parâmetros: Código do Produto, Data dos Testes, Atenuação em dB/km de cada fibra do cabo para os comprimentos de onda de 850nm e 1300nm, ou ainda ser entregue código para consulta destes parâmetros pela internet através de codificação única que mostre os resultados de testes do lote do cabo utilizado.
- 1.6.17 A fibra óptica deverá suportar velocidades de transmissão de 10 Gbps para distâncias de 550 m a 850 nm.
- 1.6.18 Deve suportar uma carga máxima de instalação de até 1335 N.
- 1.6.19 Devem estar de acordo com a diretiva RoHS 2002/95/EC.
- 1.6.20 Todos os componentes da solução que compõe a solução do cabeamento estruturado, tais como, Patch Panels Metálicos, Bastidores Ópticos, Cabos ópticos e metálicos devem ser de um único fabricante, garantindo assim total compatibilidade na instalação dos mesmos.

1.7 Cordão Óptico Duplex Monomodo LC/LC

Os cordões ópticos deverão possuir as seguintes características técnicas obrigatórias:

- 1.7.1 Este cordão deverá ser constituído por um par de fibras ópticas monomodo (Single Mode) padrão G.657.A2
- 1.7.2 Apresentar perda de retorno mínima de 50 dB.
- 1.7.3 Apresentar perda por inserção máxima de 0.25 dB.
- 1.7.4 Devem ser fornecidos no padrão duplex com terminações de conectores LC/UPC.
- 1.7.5 Utilizar padrão “zip-cord” de reunião das fibras para diâmetro de 1.8mm.
- 1.7.6 Deve possuir classificação LSZH (IEC 60332-3).
- 1.7.7 O cordão óptico duplo deverá vir devidamente conectorizado em suas extremidades e testado de fábrica.
- 1.7.8 Dispersão:
- 1.7.9 1310 nm: 3.5 ps/(nm-km) de 1285 a 1330 nm (máximo).
- 1.7.10 1550 nm: 18 ps/(nm-km) (máximo).
- 1.7.11 Devem estar de acordo com a diretiva RoHS 2002/95/EC.
- 1.7.12 Deve possuir comprimento mínimo de 3 metros.
- 1.7.13 Todos os componentes da solução que compõe a solução do cabeamento óptico, tais como os cabos ópticos, painéis ópticos, bastidores ópticos devem ser de um único fabricante, garantindo total compatibilidade na instalação dos mesmos.

1.8 Cabos Ópticos Indoor / Outdoor – Monomodo OS2

Os cabos ópticos deverão possuir as seguintes características técnicas obrigatórias:

- 1.8.1 Deverá ser formado por 12 fibras ópticas Monomodo (Single Mode) OS2 padrão G.652.D e G.657.A1.
- 1.8.2 Deverá suportar instalações em ambientes internos e externos.
- 1.8.3 Deverá possuir capa na cor preta.
- 1.8.4 Capa com resistência a raios UV.
- 1.8.5 Deve cumprir ou superar as especificações da norma ANSI/TIA-492CAAB.
- 1.8.6 O diâmetro do núcleo das fibras deve ser de 8,3µm e o diâmetro da via deve ser de 125µm.
- 1.8.7 O cabo de fibra óptica deve ser do tipo LSZH para distribuição interna e construção Tight Buffered de 900µm para uso interno/externo (não-geleada).
- 1.8.8 Deve possuir peso máximo de 50.0 kg/km.
- 1.8.9 Deve possuir diâmetro máximo de 7.30 mm.
- 1.8.10 Os parâmetros mínimos de temperatura que a fibra óptica deve suportar sem que sua operação e rendimento sejam afetados deve ser entre 0 ºC e +70 ºC.
- 1.8.11 O comprimento de Onda que a fibra deverá transmitir será nas janelas de 1310nm e 1550nm.
- 1.8.12 Os cabos devem atender, para teste de flamabilidade as normas IEC 603323, IEC 60754 2, IEC 61034 2, UL 1666 e UL 1685.
- 1.8.13 O cabo de atender as normas ANSI/ICEA S-104-696-2001, EN 187105, Telcordia GR-20 CORE Issue 3 (penetração de água) e Telcordia GR-409 CORE Issue 2.
- 1.8.14 Teste de penetração de água segundo FOTP-82, IEC 60794-1-2, Seção 24 – para ciclo de 24 h.
- 1.8.15 Deverá ser entregue, junto com a entrega dos cabos, relatório de testes dos lotes entregue para a obra, contendo os seguintes dados e resultados dos seguintes parâmetros: Código do Produto, Data dos Testes, Atenuação em dB/km de cada fibra do cabo para os comprimentos de onda de 1310nm e 1550nm, ou ainda ser entregue código para consulta destes parâmetros pela internet através de codificação única que mostre os resultados de testes do lote do cabo utilizado.
- 1.8.16 A fibra óptica deverá possuir atenuação máxima de 0,50 dB/km @ 1310 nm | 0,50 dB/km @ 1550 nm.
- 1.8.17 Deve suportar uma carga máxima de instalação de 1335 N.
- 1.8.18 Devem estar de acordo com a diretiva RoHS 2002/95/EC.
- 1.8.19 Todos os componentes da solução que compõe a solução do cabeamento óptico, tais como os cabos ópticos, painéis ópticos, bastidores ópticos devem ser de um único fabricante, garantindo total compatibilidade na instalação dos mesmos.

1.9 Distribuidor Interno Óptico para fusão – 1U

O DIO deverá possuir as seguintes características técnicas obrigatórias:

- 1.9.1 Deve possuir altura de 1U.
- 1.9.2 Dimensão compatível com o padrão 19”.

- 1.9.3 Devem permitir a instalação de até 96 fusões (fusão e conectores) com o uso de adaptadores ópticos na face frontal do DIO para conectores LC duplex.
- 1.9.4 Deve suportar montagem com o uso de conectores ópticos de montagem em campo.
- 1.9.5 Devem ser capaz de permitir a aplicação com cabos ópticos pré-terminados com conectores ópticos LC atingindo também 96 fibras ópticas SM ou MM através de conectores LC duplex.
- 1.9.6 Deve possuir gaveta deslizante, facilitando a manutenção sem que haja necessidade de retirá-las do rack.
- 1.9.7 Deve ser produzido em aço, não será aceito Distribuidores de plástico.
- 1.9.8 Deve possuir organizador de patch cords que se estende para frente com relação ao primeiro plano do de fixação do rack.
- 1.9.9 Deve ser oferecida pelo fabricante a possibilidade de aquisição de tampas cegas para fechar os espaços não ocupados do DIO, protegendo assim as fibras ópticas dentro do mesmo.
- 1.9.10 As bandejas devem contar com recortes para a inserção dos cabos de fibra óptica fim de melhorar o manejo dos feixes de cabos.
- 1.9.11 Deverá ser colocada uma proteção plástica que impeça o contato do metal do corpo da bandeja com o cabo que ingressa na mesma.
- 1.9.12 Deverão ser fornecidos todos os elementos adequados para a fixação do cabo na bandeja.
- 1.9.13 Devem estar de acordo com a diretiva RoHS 2002/95/EC.
- 1.9.14 Todos os componentes da solução que compõe a solução do cabeamento estruturado, tais como, Patch Panels Metálicos, Bastidores Ópticos, Cabos ópticos e metálicos devem ser de um único fabricante, garantindo assim total compatibilidade na instalação dos mesmos.

1.10 Painel Adaptador de Acopladores Ópticos

- O conjunto adaptador deverá possuir as seguintes características técnicas obrigatórias:
- 1.10.1 Os Módulos de Fibra Óptica devem possuir capacidade de até 24 fibras LC simplex ou 12 fibras LC duplex.
- 1.10.2 Devem ser compatíveis com os Distribuidores Ópticos ofertados neste processo.
- 1.10.3 Deve ser entregue com os pigtails (extensões ópticas) apropriados (Multimodo ou Monomodo) para uso com o conjunto adaptadores para adaptadores LC.
- 1.10.4 Deve ter organizador de excesso de fibras dos pigtails ópticos acoplado ao próprio conjunto adaptador.
- 1.10.5 Deve ser oferecida pelo fabricante a possibilidade de aquisição de tampas cegas para fechar os espaços não ocupados do DIO, no mesmo formato dos conjuntos adaptadores de conectores ópticos.
- 1.10.6 Os adaptadores ópticos devem contar com tampa protetora escamoteável para garantir proteção dos mesmos mesmo quando um conector óptico não estiver inserido nele.
- 1.10.7 Devem estar de acordo com a diretiva RoHS 2002/95/EC.
- 1.10.8 Todos os componentes da solução que compõe a solução do cabeamento óptico, tais como os cabos ópticos, painéis ópticos, bastidores ópticos devem ser de um único fabricante, garantindo total compatibilidade na instalação dos mesmos.

1.11 Bandeja de Emenda Óptica

Deve ser fornecida junto ao Distribuidor óptico devendo possuir as seguintes características técnicas obrigatórias:

- 1.11.1 Suportar até 48 emendas ópticas em uma única bandeja de emenda.
- 1.11.2 Ser fornecido com os SMOVs para a proteção das fusões ópticas.
- 1.11.3 Devem ser compatíveis com os Distribuidores Ópticos ofertados neste processo.
- 1.11.4 Devem estar de acordo com a diretiva RoHS 2002/95/EC.
- 1.11.5 Todos os componentes da solução que compõe a solução do cabeamento óptico, tais como os cabos ópticos, painéis ópticos, bastidores ópticos devem ser de um único fabricante, garantindo total compatibilidade na instalação dos mesmos.

1.12 Rack de Parede 19'' x 12 RU

- 1.12.1 Rack de Parede de 12 RU e padrão 19".
- 1.12.2 Rack deve possuir dimensões de no mínimo 0,58m A x 0,53m L x 0,55m P.
- 1.12.3 Porta frontal em vidro temperado de no mínimo 4mm.
- 1.12.4 Serigrafado com fecho cilindro e chave.
- 1.12.5 Estrutura monobloco em chapa de aço.
- 1.12.6 Planos de montagem com marcação em meio ‘’U’’ e regulagem em profundidade.
- 1.12.7 Teto com predisposição para dois ventiladores.
- 1.12.8 Laterais removíveis e com aletas para ventilação e fecho rápido.
- 1.12.9 Abertura para entrada e saída de cabos no teto e base.
- 1.12.10 Acabamento em pintura eletrostática a pó na cor preta.

1.13 Rack de Piso 19'' x 44 RU

- 1.13.1 Rack de Piso de 44 RU e padrão 19".
- 1.13.2 Rack deve possuir dimensões de no mínimo 2,10m A x 0,56m L x 0,67m P.
- 1.13.3 Porta frontal em vidro de 5mm temperado e serigrafado com fecho cilindro com chave.
- 1.13.4 Deverá possuir estrutura em chapa de aço de no mínimo 1,5mm.
- 1.13.5 Possuir planos de montagem com marcação em meio “U” e regulagem na profundidade em chapa de aço de no mínimo 1,5mm.
- 1.13.6 Deverá possuir teto removível em chapa de aço 0,75mm com aletas para ventilação e predisposição para instalação de 4 micro ventiladores.
- 1.13.7 Deverá possuir fundo removível e bipartido na horizontalmente chapa de aço de no mínimo 0,75mm.
- 1.13.8 Base soleira em chapa de aço de no mínimo 1,5mm para acomodação de reserva técnica de cabos.
- 1.13.9 Laterais removíveis e bipartidas na horizontal em chapa de aço 0,75mm com fecho cilindro com chave.

- 1.13.10 Deverá possuir pés niveladores.
- 1.13.11 Acabamento em aço e revestido com pintura eletrostática a pó na cor preta.

1.14 Eletrocalhas e Canaletas

- 1.14.1 As eletrocalhas devem ser do tipo perfurada nas dimensões 100x50mm e/ou 50x50mm, devendo acomodar devidamente todos os cabos e atender as normas para taxa de ocupação e a quantidade de pontos solicitada, prevendo inclusive margem para expansões futuras.
- 1.14.2 As eletrocalhas devem ser metálicas fabricadas em chapas de aço SAE 1008/1010, conforme a NBR 11888-2 e NBR 7013.
- 1.14.3 As eletrocalhas devem ser totalmente perfuradas, permitindo assim a ventilação nos cabos.
- 1.14.4 Devem permitir a distribuição de energia elétrica, telefonia e dados, em qualquer tipo de instalação elétrica, tais como galpões industriais, comerciais e prédios.
- 1.14.5 Deve possuir os acabamentos do tipo pré zincada a fogo (NBR 7008-ZC) ou galvanizado a fogo (NBR 6323).
- 1.14.6 Sistema de canaletas e acessórios aparentes deverá ser de formato curvo, fabricados em material plástico na cor branca, com alta resistência ao impacto, destinado para condução de fios e cabos, tomadas embutidas ou sobrepostas nas bases, de tamanhos 55x20mm e/ou 120x35mm e 2 metros de comprimento.
- 1.14.7 Os perfis das tampas deverão ser fornecidos com filme autocolante para proteção contra riscos e sujeira no transporte e durante a instalação.
- 1.14.8 O sistema de canaletas deve atender as normas ABNT NBR-IEC 61084:2006 (Sistemas de canaletas e condutos perfilados para instalações elétricas); ABNT NBR 14565:2013 (Norma Brasileira de Cabeamento Estruturado para edifícios Comerciais e Data Centers), ABNT NBR 16415:2015 (Caminhos e espaços para cabeamento estruturado), assim como contemplar as normas ANSI/TIA-569-C (Padrão para Encaminhamentos e Espaços para Cabeamento de Telecomunicação em Edifícios Comerciais), ANSI/TIA-568-C nos quesitos que interferem com as canaletas.
- 1.14.9 Com relação à sustentabilidade ambiental, preferencialmente deve ser acondicionado em embalagens adequadas de materiais recicláveis, com o menor volume possível e de forma a garantir a máxima proteção durante o transporte e o armazenamento. Por fim, que as canaletas não contenham substâncias perigosas em concentração acima da recomendada.
- 1.14.10 O sistema de canaletas deverá possibilitar o uso de tomadas de energia padrão Brasileiro ABNT NBR 14136:2013, com encaixe rápido no suporte e ou caixa da canaleta, sem necessidade de parafusos de fixação. Os conectores keystones RJ45 fêmea também devem ser instalados por engate rápido.
- 1.14.11 Os acessórios, curvas internas, externas, horizontais (Ls) e THs do sistema de canaletas deverão respeitar os critérios de raio de curvatura dos cabos de acordo com a indicação da norma ABNT NBR 16415:2015, contemplando também a norma ANSI / TIA 568-C. As tampas deverão possuir encaixe lateral reforçado, que se conecta na base, dificultando a abertura da canaleta.
- 1.14.12 As canaletas deverão conter sistema de fixa cabos, que possibilita a permanência dos cabos no leito das bases, quando da instalação e manutenção evitando que os mesmos caiam durante as manobras com as tampas abertas.

2. ESPECIFICAÇÕES TÉCNICAS DOS ITENS DE CONECTIVIDADE DE REDE (LOTE 02)

Todos os componentes de conectividade do LOTE 02 devem ser de um único fabricante, visando assegurar a perfeita interoperabilidade e compatibilidade dos produtos entre si, bem como assegurar o desempenho da solução como um todo. Os switches e access points devem suporte para abertura de chamados em regime 8x5.

2.1 Switch Tipo I, Layer 2+, 24 portas x 1 Gbps RJ45, 4 x 1 Gbps SFP

- 2.1.1 Características:
- 2.1.2 Deve possuir 24 (vinte e quatro) portas Gigabit Ethernet 10/100/1000Base-T Conforme Padrões IEEE 802.3, IEEE 802.3u, IEEE 802.3ab;
- 2.1.3 As interfaces deverão ser Full-Duplex, auto sensing com conectores RJ45 fêmea e implementar mecanismos de autoconfiguração em todas as portas, do tipo MDI/MDI-X;
- 2.1.4 Deve possuir adicionalmente no mínimo 4 (quatro) portas 1Gbps (SFP);
- 2.1.5 As interfaces dos 2.1.2 e 2.1.4 devem operar de modo simultâneo;
- 2.1.6 Deve possuir no mínimo 1 (uma) porta console exclusiva para fins de gerenciamento e configuração. Esta porta deverá ser do tipo USB ou micro USB;
- 2.1.7 Deve possuir fonte de alimentação interna ao equipamento, que opere com tensões de entrada entre 100 e 240 VAC e frequência de 50/60Hz;
- 2.1.8 Desempenho e Capacidades:
- 2.1.9 Deve possuir capacidade de processamento de no mínimo 56 Gbps;
- 2.1.10 Deve possuir taxa de encaminhamento de pacotes igual ou superior a 41.66 Mbps;
- 2.1.11 Sua tabela de MAC Address deve suportar no mínimo 16.000 MAC address;
- 2.1.12 Deve possuir Buffer de pacotes de no mínimo 12Mbit;
- 2.1.13 Deve suportar jumbo frame de no mínimo 9 KB;
- 2.1.14 Deve ser do tipo Fanless, ou seja, não possuir ventoinha para dissipação de calor evitando ruídos de operação;
- 2.1.15 Deve suportar temperatura de operação entre 0° e 45°;
- 2.1.16 Deve suportar operação sob umidade entre 10% e 90% RH sem condensamento;
- 2.1.17 Deve possuir Memória Flash de no mínimo 32MB;
- 2.1.18 Deve possuir Memória DRAM de no mínimo 256MB;
- 2.1.19 Funcionalidades de Camada 2:
- 2.1.20 Deve implementar agregação de links de modo estático, bem como LACP (Link Aggregation Control Protocol) conforme IEEE 802.3ad;
- 2.1.21 Deve suportar a criação de no mínimo 8 grupos de portas agregadas com no mínimo 8 portas por grupo;
- 2.1.22 Deve implementar o protocolo Spanning tree e suas variações:
- 2.1.23 IEEE 802.1d STP (Spanning tree protocol);
- 2.1.24 IEEE 802.1w RSTP (Rapid Spanning Tree Protocol);
- 2.1.25 IEEE 802.1s MSTP (Multiple Spanning Tree Protocol);

- 2.1.26 Deve possuir mecanismo de detecção e proteção contra loops;
- 2.1.27 Deve implementar Filtro de BPDU (Bridge Protocol Data Unit);
- 2.1.28 Deve possuir recurso de proteção da porta root como root guard, root protect ou similar;
- 2.1.29 Deve implementar controle de fluxo conforme IEEE 802.3X;
- 2.1.30 Deve implementar espelhamento de porta possibilitando o monitoramento de uma porta ou de um grupo de portas. Também deve possibilitar a escolha da direção do tráfego a ser espelhado, sendo TX, RX ou ambos;
- 2.1.31 Deve implementar no mínimo 4000 Vlans;
- 2.1.32 Deve possibilitar a configuração do ID da Vlan entre 2 e 4094;
- 2.1.33 Deve implementar Tagged Vlan conforme IEEE 802.1Q;
- 2.1.34 Deve implementar MAC Vlan;
- 2.1.35 Deve Implementar GVRP (Generic Vlan Registration Protocol);
- 2.1.36 Deve implementar Vlan de voz. O Switch deverá ser capaz de reconhecer um telefone IP automaticamente e atribuí-lo à uma VLAN de voz;
- 2.1.37 Multicast:
- 2.1.38 Deve implementar IGMP Snooping v1, v2 e v3;
- 2.1.39 Deve suportar IGMP Fast Leave, IGMP Snooping Querier e IGMP Authentication;
- 2.1.40 Deve suportar no mínimo 500 grupos IGMP;
- 2.1.41 Deve suportar MLD Snooping v1 e v2;
- 2.1.42 Deve suportar MLD Snooping Querier e MLD Fast Leave;
- 2.1.43 Deve suportar a configuração de Grupos estáticos MLD Snooping;
- 2.1.44 Deve implementar MVR (Multicast VLAN Registration);
- 2.1.45 Funcionalidades L3:
- 2.1.46 Deve suportar no mínimo 48 rotas estáticas;
- 2.1.47 Deve implementar no mínimo 16 interfaces Vlan para fins de roteamento entre vlans;
- 2.1.48 Deve suportar no 512 entradas ARP;
- 2.1.49 Deve implementar DHCP Server;
- 2.1.50 Deve implementar DHCP Relay;
- 2.1.51 Deve implementar Proxy Arp;
- 2.1.52 Qualidade de Serviço:
- 2.1.53 Deve implementar classificação e marcação de pacotes em CoS e DSCP conforme IEEE 802.1p;
- 2.1.54 Deve implementar os seguintes algoritmos de gerenciamento de filas:
- 2.1.55 WRR (Weighted Round Robin);
- 2.1.56 SP (Strict Priority);

- 2.1.57 SP+WRR (Strict Priority + Weighted Round Robin);
- 2.1.58 Deve Implementar controle de banda por porta;
- 2.1.59 Deve possibilitar a implementação de no mínimo 8 filas de prioridade;
- 2.1.60 Deve possibilitar a remarcação de QoS;
- 2.1.61 Segurança:
- 2.1.62 Deve implementar Access Control List (ACL);
- 2.1.63 Deve suportar ACL baseada em tempo;
- 2.1.64 Deve suportar ACL Baseada em MAC Address:
- 2.1.65 MAC de Origem
- 2.1.66 MAC de Destino
- 2.1.67 VLAN ID
- 2.1.68 User Priority
- 2.1.69 Ether Type
- 2.1.70 Deve implementar ACL baseada em IP;
- 2.1.71 IP de Origem
- 2.1.72 IP de Destino
- 2.1.73 Protocolo IP
- 2.1.74 TCP/UDP Port
- 2.1.75 DSCP/IP TOS
- 2.1.76 Deve implementar ACL sobre IPv6;
- 2.1.77 Deve implementar IP-MAC-PORT Binding sob IPv4 com no mínimo 500 entradas;
- 2.1.78 Deve implementar IP Source Guard com no mínimo 100 entradas;
- 2.1.79 Deve implementar proteção contra ataques DoS;
- 2.1.80 Deve implementar port security;
- 2.1.81 Deve possuir filtro DHCP a fim de inibir servidores DHCP não autorizados;
- 2.1.82 Deve implementar Broadcast, Multicast e Unicast Storm Control;
- 2.1.83 Deve implementar IEEE 802.1X com autenticação baseada em porta e MAC;
- 2.1.84 Deve suportar IEEE 802.1X com associação automática de Vlan;
- 2.1.85 Deve suportar MAB (MAC Authentication Bypass);
- 2.1.86 Deve ter suporte à servidor RADIUS para autenticação;
- 2.1.87 Deve implementar Guest Vlan;
- 2.1.88 Deve implementar DHCP Snooping;
- 2.1.89 Deve suportar gerenciamento através de HTTPS com SSLv3/TLS 1.2;

- 2.1.90 Deve suportar gerenciamento através de interface de comandos segura com SSH V1 e v2;
- 2.1.91 Deve suportar os algoritmos de encriptação AES128-CBC, AES192-CBC, AES256-CBC, Blowfish-CBC, CAST128-CBC e 3DES-CBC;
- 2.1.92 Gerenciamento:
- 2.1.93 Deve implementar gerenciamento via WEB com HTTP e HTTPS;
- 2.1.94 Deve permitir o gerenciamento através de linha de comandos (CLI) para interface console bem como para comunicação TCP com Telnet e SSH;
- 2.1.95 Deve ter suporte para AAA incluindo TACACS+;
- 2.1.96 Deve ter suporte para EEE (Energy Efficient Ethernet);
- 2.1.97 Deve suportar SNMP V1, V2c e V3;
- 2.1.98 Deve implementar MIB II conforme RFC1213;
- 2.1.99 Deve implementar RMON com no mínimo 4 grupos;
- 2.1.100 Deve implementar NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol);
- 2.1.101 Deve implementar FTP (File Transfer Protocol) ou TFTP (Trivial File Transfer Protocol);
- 2.1.102 Deve Implementar LLDP e LLDP MED conforme IEEE 802.1ab;
- 2.1.103 Deve implementar Syslog;
- 2.1.104 Deve implementar DHCP/BOOT Cliente;
- 2.1.105 Deve possibilitar o monitoramento da CPU do Switch;
- 2.1.106 Deve possibilitar o armazenamento de dois arquivos de configuração simultaneamente (Dual Image);
- 2.1.107 Deve implementar Diagnóstico de cabos;
- 2.1.108 Deve implementar Ethernet Link OAM conforme IEEE 802.3ah;
- 2.1.109 Deve implementar DLDP (Device Link Detect Protocol);
- 2.1.110 Deve suportar DDM (Digital Diagnostic Monitoring);
- 2.1.111 Deve ser possível o gerenciamento do Switch através de solução de gerenciamento centralizado do próprio fabricante podendo ser este software ou apliance;
- 2.1.112 IPv6:
- 2.1.113 Deve implementar Pilha dupla (Dual IPv4/IPv6);
- 2.1.114 Deve implementar MLD (Multicast Listener Discovery);
- 2.1.115 Deve implementar ACL sobre IPv6;
- 2.1.116 Deve implementar rotas estáticas em IPv6 e interfaces VLAN sobre IPv6;
- 2.1.117 Deve implementar IPv6 Neighbor Discover (ND);
- 2.1.118 Deve implementar ICMP v6;
- 2.1.119 Deve implementar Path maximum transmission unit (MTU) Discovery;

- 2.1.120 Deve suportar as seguintes aplicações sobre IPv6:
- 2.1.121 DHCPv6 Cliente;
- 2.1.122 Ping6;
- 2.1.123 Tracert6;
- 2.1.124 Telnet v6;
- 2.1.125 SNMP;
- 2.1.126 SSH;
- 2.1.127 SSL;
- 2.1.128 HTTP/HTTPS sobre IPv6;
- 2.1.129 FTP ou TFTP sobre IPv6;
- 2.1.130 Certificações, padronização e documentações:
- 2.1.131 Possuir homologação da ANATEL, de acordo com a resolução número 242 de 30/11/2000;
- 2.1.132 O fabricante do produto indicado deve estar listado no relatório do Gartner – Magic Quadrant for Wired and Wireless LAN Access Infrastructure, publicado em Novembro de 2022 -. O relatório Gartner – Magic Quadrant é uma representação gráfica das atividades do mercado tecnológico em um determinado período e fornece uma relação dos agentes mais relevantes do mercado;
- 2.1.133 Possuir Certificação FCC, CE;
- 2.1.134 Deve ser RoHS (Restriction of Certain Hazardous Substances) Compliance;
- 2.1.135 O equipamento deve possuir garantia de 60 meses ON-SITE pela Contratada;
- 2.1.136 O tempo de troca em caso de falhas deve ser de no máximo 30 (trinta) dias corridos, na modalidade de RMA Troca balcão;
- 2.1.137 Em caso de troca, o produto reposto deve ser novo e em perfeito estado, igual ou superior ao produto enviado;
- 2.1.138 O produto entregue pela contratada deve ser novo e acomodado em caixa de papelão;
- 2.1.139 O Proponente deve ser revenda autorizada pelo fabricante;
- 2.1.140 O proponente deve emitir declaração do fabricante atestando ser revenda autorizada a comercializar os produtos em território nacional;
- 2.1.141 Deve ser montável em rack padrão EIA 19’’(dezenove polegadas) e possuir kits completos para instalação bem como ocupar o espaço de 1 (um) U em Rack;
- 2.1.142 Deve acompanhar manuais, licenças de software, cabo de energia, cabo de acesso via console e aletas de montagem em rack;
- 2.1.143 Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste lote 02.

2.2 Switch Tipo II, Layer 2+ POE, 24 portas x 1 Gbps RJ45, 4 x 1 Gbps SFP

- 2.2.1 Características:

- 2.2.2 Deve possuir 24 (vinte e quatro) portas Gigabit Ethernet 10/100/1000Base-T Conforme Padrões IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab;
- 2.2.3 As interfaces deverão ser Full-Duplex, auto sensing com conectores RJ45 fêmea e implementar mecanismos de autoconfiguração em todas as portas, do tipo MDI/MDI-X;
- 2.2.4 Deve possuir adicionalmente pelo menos 4 (quatro) slots 1G (SFP) conforme padrões IEEE 802.3z 1000BASE-X;
- 2.2.5 As interfaces dos itens 2.2.2 e 2.2.4 devem operar de modo simultâneo;
- 2.2.6 Deve possuir no mínimo 2 (duas) portas console uma do tipo RJ45 e outra Micro-USB;
- 2.2.7 Deve possuir fonte de alimentação interna, que opere com tensões de entrada entre 100 e 240 VAC e frequência de 50/60Hz;
- 2.2.8 Alimentação e Consumo:
- 2.2.9 Deve possuir consumo de energia em modo standby de até 15.7W;
- 2.2.10 Deve implementar os padrões IEEE 802.3at e IEEE 802.3af;
- 2.2.11 Deve ser capaz de fornecer 30W por porta (não simultâneo);
- 2.2.12 Deve possuir o Budget PoE de no mínimo 380W;
- 2.2.13 Deve possuir recurso de Priorização de energia por porta de no mínimo três níveis: Baixa, média e alta;
- 2.2.14 Deve possuir recurso de limitação por porta, no qual deverá ser possível determinar limite de alimentação por classe com no mínimo 4 níveis: Até 4W, até 7W, até 15.4W e até 30W;
- 2.2.15 Desempenho e Capacidades:
- 2.2.16 Deve possuir capacidade de processamento de no mínimo 56 Gbps;
- 2.2.17 Deve possuir taxa de encaminhamento de pacotes igual ou superior a 41.66 Mpps;
- 2.2.18 Sua tabela de MAC Address deve suportar no mínimo 16.000 MAC address;
- 2.2.19 Deve possuir Buffer de pacotes de no mínimo 12 Mbit;
- 2.2.20 Deve suportar jumbo frame de no mínimo 9 KB;
- 2.2.21 O equipamento deve possuir sistema de resfriamento interno com no mínimo 2 ventiladores;
- 2.2.22 Deve suportar temperatura de operação entre 0° e 45°C;
- 2.2.23 Deve suportar operação sob umidade entre 10% e 90% RH sem condensamento;
- 2.2.24 Funcionalidades de Camada 2:
- 2.2.25 Deve implementar agregação de links de modo estático;
- 2.2.26 Deve implementar o protocolo LACP (Link Aggregation Control Protocol) conforme IEEE 802.3ad;
- 2.2.27 Deve suportar a criação de no mínimo 8 grupos de portas agregadas com no mínimo 8 portas por grupo;
- 2.2.28 Deve implementar o protocolo Spanning tree e suas variações:
- 2.2.29 IEEE 802.1d STP (Spanning tree protocol);

- 2.2.30 IEEE 802.1w RSTP (Rapid Spanning Tree Protocol);
- 2.2.31 IEEE 802.1s MSTP (Multiple Spanning Tree Protocol);
- 2.2.32 Pelo menos 255 instâncias MSTI;
- 2.2.33 Deve implementar os protocolos de segurança STP:
- 2.2.34 TC Protect;
- 2.2.35 BPDU filter;
- 2.2.36 BPDU protect;
- 2.2.37 Root protect;
- 2.2.38 Loop protec;
- 2.2.39 Deve implementar controle de fluxo conforme IEEE 802.3X;
- 2.2.40 Deve implementar loopback detection baseada em porta e Vlan;
- 2.2.41 Deve implementar espelhamento de porta possibilitando o monitoramento de uma porta ou de um grupo de portas. Também deve possibilitar a escolha da direção do tráfego a ser espelhado, sendo TX, RX ou ambos;
- 2.2.42 Deve implementar o espelhamento da CPU para análises investigadas de eventuais falhas;
- 2.2.43 Deve implementar no mínimo 4.000 grupos de Vlans;
- 2.2.44 Deve possibilitar a configuração do ID da Vlan entre 2 e 4094;
- 2.2.45 Deve implementar Tagged Vlan conforme IEEE 802.1Q;
- 2.2.46 Deve implementar MAC Vlan com pelo menos 12 entradas;
- 2.2.47 Deve suportar no mínimo 511 grupos IGMP;
- 2.2.48 Deve suportar pelo menos 8 anéis ERPS;
- 2.2.49 Deve Implementar GVRP (Generic Vlan Registration Protocol);
- 2.2.50 Deve implementar Vlan de voz. O Switch deverá ser capaz de reconhecer um telefone IP automaticamente e atribuí-lo uma VLAN de voz;
- 2.2.51 Multicast:
- 2.2.52 Deve implementar IGMP Snooping v1, v2 e v3;
- 2.2.53 Deve suportar IGMP Fast Leave, IGMP Snooping Querier e IGMP Authentication;
- 2.2.54 Deve suportar configuração de grupo de multicast estático;
- 2.2.55 Deve suportar MLD Snooping v1 e v2;
- 2.2.56 Deve suportar MLD Snooping Querier e MLD Fast Leave;
- 2.2.57 Deve implementar MVR (Multicast VLAN Registration);
- 2.2.58 Deve implementar filtro multicast com pelo menos 256 profiles e 16 entradas por profile;
- 2.2.59 Funcionalidades L3:
- 2.2.60 Deve suportar no mínimo 48 rotas estáticas IPv4/IPv6;

- 2.2.61 Deve implementar no mínimo 16 interfaces Vlan para fins de roteamento entre vlans;
- 2.2.62 Deve implementar interface Vlan para IPv4 e para IPv6;
- 2.2.63 Deve suportar configuração de interface de Loopback;
- 2.2.64 Deve implementar ARP estático com mínimo de 128 entradas;
- 2.2.65 Deve implementar servidor DHCP com pelo menos 8 pools;
- 2.2.66 Deve Implementar DHCP Relay com interface e Vlan relay;
- 2.2.67 Qualidade de Serviço:
- 2.2.68 Deve implementar classificação e marcação de pacotes em CoS e DSCP conforme IEEE 802.1p;
- 2.2.69 Deve implementar os seguintes algoritmos de gerenciamento de filas:
- 2.2.70 WRR (Weighted Round Robin);
- 2.2.71 SP (Strict Priority);
- 2.2.72 SP+WRR (Strict Priority + Weighted Round Robin);
- 2.2.73 Deve Implementar controle de banda por porta;
- 2.2.74 Deve possibilitar a implementação de no mínimo 8 filas;
- 2.2.75 Deve possibilitar a remarcação de QoS;
- 2.2.76 Deve implementar controle de banda port/flow based rating limiting;
- 2.2.77 Segurança
- 2.2.78 Deve implementar os seguintes tipos de Access Control List (ACL):
- 2.2.79 MAC de origem;
- 2.2.80 MAC de destino;
- 2.2.81 VLAN ID;
- 2.2.82 User Priority;
- 2.2.83 Ether Type;
- 2.2.84 IP de origem;
- 2.2.85 IP de destino;
- 2.2.86 Fragmento;
- 2.2.87 Protocolo IP;
- 2.2.88 Flag TCP;
- 2.2.89 Porta TCP/UDP;
- 2.2.90 DCSP/IP TOS;
- 2.2.91 ACL combinada;
- 2.2.92 Deve suportar ACL baseada em tempo;
- 2.2.93 As configurações de ACL devem ser aplicadas na porta e Vlan;

- 2.2.94 Deve implementar IP-MAC-PORT Binding com 512 entradas;
- 2.2.95 Deve implementar IP Source Guard com pelo menos 100 entradas;
- 2.2.96 Deve implementar proteção contra-ataques DoS;
- 2.2.97 Deve implementar port security;
- 2.2.98 Deve implementar Broadcast, Multicast e Unknown-unicast Storm Control;
- 2.2.99 Deve implementar IEEE 802.1X com autenticação baseada em porta e MAC;
- 2.2.100 Deve suportar IEEE 802.1X com associação automática de Vlan;
- 2.2.101 Deve suportar MAB (MAC Authentication Bypass);
- 2.2.102 Deve ter suporte à servidor RADIUS para autenticação;
- 2.2.103 Deve implementar Guest Vlan;
- 2.2.104 Deve implementar DHCP Snooping para IPv4 e para IPv6;
- 2.2.105 Deve suportar gerenciamento através de HTTPS com SSLv3/TLS 1.2;
- 2.2.106 Deve suportar gerenciamento através de interface de comandos segura com SSH V1 e v2;
- 2.2.107 Gerenciamento:
- 2.2.108 Deve implementar gerenciamento via WEB com HTTP e HTTPS;
- 2.2.109 Deve permitir o gerenciamento seguro através de linha de comandos (CLI) com SSHv2;
- 2.2.110 Deve ter suporte para AAA incluindo TACACS+;
- 2.2.111 Deve ter suporte para EEE (Energy Efficient Ethernet);
- 2.2.112 Deve suportar SNMP V1, V2c e V3;
- 2.2.113 Deve suportar SNMP Trap;
- 2.2.114 Deve suportar SNMP Inform;
- 2.2.115 Deve suportar as seguintes RFCs:
- 2.2.116 RFC1213;
- 2.2.117 RFC1493;
- 2.2.118 RFC1643;
- 2.2.119 RFC2021;
- 2.2.120 RFC2233;
- 2.2.121 RFC2618;
- 2.2.122 RFC2620;
- 2.2.123 RFC2674;
- 2.2.124 RFC2819;
- 2.2.125 RFC2925;
- 2.2.126 Deve implementar RMON com no mínimo 4 grupos;

- 2.2.127 Deve implementar Syslog;
- 2.2.128 Deve implementar NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol);
- 2.2.129 Deve implementar FTP/FTPv6 (File Transfer Protocol) ou TFTP/TFTPv6 (Trivial File Transfer Protocol);
- 2.2.130 Deve Implementar LLDP e LLDP MED conforme IEEE 802.1ab;
- 2.2.131 Deve implementar DHCP/BOOTP Cliente;
- 2.2.132 Deve possibilitar o monitoramento da CPU do Switch;
- 2.2.133 Deve possibilitar o armazenamento de dois arquivos de configuração simultaneamente (Dual Image);
- 2.2.134 Deve implementar Diagnóstico de cabos;
- 2.2.135 Deve implementar Ethernet Link OAM conforme IEEE 802.3ah;
- 2.2.136 Deve implementar DLDP (Device Link Detect Protocol);
- 2.2.137 Deve ser possível o gerenciamento do Switch através de solução de gerenciamento centralizado do próprio fabricante podendo ser este software ou appliance;
- 2.2.138 IPv6:
- 2.2.139 Deve implementar Pilha dupla (Dual IPv4/IPv6);
- 2.2.140 Deve implementar MLD (Multicast Listener Discovery);
- 2.2.141 Deve implementar ACL sobre IPv6;
- 2.2.142 Deve implementar rotas estáticas em IPv6 e interfaces VLAN sobre IPv6;
- 2.2.143 Deve implementar IPv6 Neighbor Discover (ND);
- 2.2.144 Deve implementar ICMP v6;
- 2.2.145 Deve implementar DHCPv6 Snooping;
- 2.2.146 Deve suportar as seguintes aplicações sobre IPv6:
- 2.2.147 DHCPv6 Cliente;
- 2.2.148 Ping6;
- 2.2.149 Tracert6;
- 2.2.150 Telnet v6;
- 2.2.151 IPv6 SNMP;
- 2.2.152 IPv6 SSH;
- 2.2.153 IPv6 SSL;
- 2.2.154 HTTP/HTTPS sobre IPv6;
- 2.2.155 FTP ou TFTP sobre IPv6;
- 2.2.156 Certificações, padronização e documentações:

- 2.2.157 Possuir homologação da ANATEL, de acordo com a resolução nº 715, de 23 de outubro de 2019;
- 2.2.158 O fabricante do produto indicado deve estar listado no relatório do Gartner – Magic Quadrant for Wired and Wireless LAN Access Infrastructure, publicado em março de 2024 -. O relatório Gartner – Magic Quadrant é uma representação gráfica das atividades do mercado tecnológico em um determinado período e fornece uma relação dos agentes mais relevantes do mercado;
- 2.2.159 Possuir Certificação FCC e CE;
- 2.2.160 Deve ser RoHS (Restriction of Certain Hazardous Substances) Compliance;
- 2.2.161 Deve possuir garantia de 60 meses ON-SITE pela Contratada;
- 2.2.162 O tempo de troca em caso de falhas deve ser de no máximo 30 (trinta) dias corridos, na modalidade de RMA Troca balcão;
- 2.2.163 Em caso de troca, o produto reposto deve ser novo e em perfeito estado, igual ou superior ao produto enviado;
- 2.2.164 O produto entregue pela contratada deve ser novo e acomodado em caixa de papelão;
- 2.2.165 O Proponente deve ser revenda autorizada pelo fabricante;
- 2.2.166 O proponente deve emitir declaração do fabricante atestando ser revenda autorizada a comercializar os produtos em território nacional;
- 2.2.167 Deve ser montável em rack padrão EIA 19’’(dezenove polegadas) e possuir kits completos para instalação bem como ocupar o espaço de 1 (um) U em Rack;
- 2.2.168 Deve acompanhar manuais, cabo de energia, cabo para a porta console e aletas de montagem em rack.
- 2.2.169 Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste lote 02.

2.3 Switch Tipo III, Layer 2+ POE, 24 portas x 2.5 Gbps RJ45, 4 x 10 Gbps SFP+

- 2.3.1 Características:
- 2.3.2 Deve possuir 24 (vinte e quatro) portas Gigabit Ethernet 10/100/1000/2500Base-T Conforme Padrões IEEE 802.3u, IEEE 802.3ab, IEEE 802.3bz;
- 2.3.3 As interfaces deverão ser Full-Duplex, auto sensing com conectores RJ45 fêmea e implementar mecanismos de autoconfiguração em todas as portas, do tipo MDI/MDI-X;
- 2.3.4 Deve possuir adicionalmente pelo menos 4 (quatro) slots 10G (SFP+) conforme padrões IEEE 802.3ae 10GBASE-SR e 10GBASE-LR;
- 2.3.5 As interfaces dos itens 2.3.2 e 2.3.4 devem operar de modo simultâneo;
- 2.3.6 Deve possuir no mínimo 2 (duas) portas console uma do tipo RJ45 e outra Micro-USB;
- 2.3.7 Deve possuir fonte de alimentação interna, que opere com tensões de entrada entre 100 e 240 VAC e frequência de 50/60Hz;
- 2.3.8 Alimentação e Consumo:

- 2.3.9 Deve possuir consumo de energia em modo standby de até 24.2W;
- 2.3.10 Deve implementar os padrões IEEE 802.3at, IEEE 802.3af e IEEE 802.3bt;
- 2.3.11 Deve ser capaz de fornecer 30W por porta (não simultâneo);
- 2.3.12 Deve possuir o Budget PoE de no mínimo 490W;
- 2.3.13 Deve possuir recurso de Priorização de energia por porta de no mínimo três níveis: Baixa, média e alta;
- 2.3.14 Deve possuir recurso de agendamento de tempo de alimentação por porta;
- 2.3.15 Deve possuir recurso de limitação por porta, no qual deverá ser possível determinar limite de alimentação por classe com no mínimo 4 níveis: Até 4W, até 7W, até 15.4W, até 30W e até 60W;
- 2.3.16 Desempenho e Capacidades:
- 2.3.17 Deve possuir capacidade de processamento de no mínimo 200 Gbps;
- 2.3.18 Deve possuir taxa de encaminhamento de pacotes igual ou superior a 148 Mpps;
- 2.3.19 Sua tabela de MAC Address deve suportar no mínimo 32.000 MAC address;
- 2.3.20 Deve possuir Buffer de pacotes de no mínimo 16 Mbit;
- 2.3.21 Deve suportar jumbo frame de no mínimo 9 KB;
- 2.3.22 O equipamento deve possuir sistema de resfriamento com no mínimo 3 ventiladores;
- 2.3.23 Deve suportar temperatura de operação entre 0° e 40°C;
- 2.3.24 Deve suportar operação sob umidade entre 10% e 90% RH sem condensamento;
- 2.3.25 Funcionalidades de Camada 2:
- 2.3.26 Deve implementar agregação de links de modo estático;
- 2.3.27 Deve implementar o protocolo LACP (Link Aggregation Control Protocol) conforme IEEE 802.3ad;
- 2.3.28 Deve suportar a criação de no mínimo 8 grupos de portas agregadas com no mínimo 8 portas por grupo;
- 2.3.29 Deve implementar o protocolo Spanning tree e suas variações:
- 2.3.30 IEEE 802.1d STP (Spanning tree protocol);
- 2.3.31 IEEE 802.1w RSTP (Rapid Spanning Tree Protocol);
- 2.3.32 IEEE 802.1s MSTP (Multiple Spanning Tree Protocol);
- 2.3.33 Pelo menos 8 instâncias MSTI;
- 2.3.34 Deve implementar os protocolos de segurança STP:
- 2.3.35 TC Protect;
- 2.3.36 BPDU filter;
- 2.3.37 BPDU protect;
- 2.3.38 Root protect;

- 2.3.39 Loop protect;
- 2.3.40 Deve implementar controle de fluxo conforme IEEE 802.3X;
- 2.3.41 Deve implementar loopback detection baseada em porta e Vlan;
- 2.3.42 Deve implementar espelhamento de porta possibilitando o monitoramento de uma porta ou de um grupo de portas. Também deve possibilitar a escolha da direção do tráfego a ser espelhado, sendo TX, RX ou ambos;
- 2.3.43 Deve implementar o espelhamento da CPU para análises investigadas de eventuais falhas;
- 2.3.44 Deve implementar no mínimo 4.000 grupos de Vlans;
- 2.3.45 Deve possibilitar a configuração do ID da Vlan entre 2 e 4094;
- 2.3.46 Deve implementar Tagged Vlan conforme IEEE 802.1Q;
- 2.3.47 Deve implementar MAC Vlan com pelo menos 30 entradas;
- 2.3.48 Deve suportar no mínimo 511 grupos IGMP;
- 2.3.49 Deve suportar pelo menos 8 anéis ERPS;
- 2.3.50 Deve Implementar GVRP (Generic Vlan Registration Protocol);
- 2.3.51 Deve implementar Vlan de voz. O Switch deverá ser capaz de reconhecer um telefone IP automaticamente e atribuí-lo uma VLAN de voz;
- 2.3.52 Multicast:
- 2.3.53 Deve implementar IGMP Snooping v1, v2 e v3;
- 2.3.54 Deve suportar IGMP Fast Leave, IGMP Snooping Querier e IGMP Authentication;
- 2.3.55 Deve suportar configuração de grupo de multicast estático;
- 2.3.56 Deve suportar MLD Snooping v1 e v2;
- 2.3.57 Deve suportar MLD Snooping Querier e MLD Fast Leave;
- 2.3.58 Deve implementar MVR (Multicast VLAN Registration);
- 2.3.59 Deve implementar filtro multicast com pelo menos 256 profiles e 16 entradas por profile;
- 2.3.60 Funcionalidades L3:
- 2.3.61 Deve suportar no mínimo 48 rotas estáticas IPv4/IPv6;
- 2.3.62 Deve implementar no mínimo 32 interfaces Vlan para fins de roteamento entre vlans;
- 2.3.63 Deve implementar interface Vlan para IPv4 e para IPv6;
- 2.3.64 Deve suportar configuração de interface de Loopback;
- 2.3.65 Deve implementar ARP estático com mínimo de 128 entradas;
- 2.3.66 Deve implementar servidor DHCP com pelo menos 8 pools;
- 2.3.67 Deve Implementar DHCP Relay com interface e Vlan relay;
- 2.3.68 Qualidade de Serviço:
- 2.3.69 Deve implementar classificação e marcação de pacotes em CoS e DSCP conforme IEEE 802.1p;

- 2.3.70 Deve implementar os seguintes algoritmos de gerenciamento de filas:
- 2.3.71 WRR (Weighted Round Robin);
- 2.3.72 SP (Strict Priority);
- 2.3.73 SP+WRR (Strict Priority + Weighted Round Robin);
- 2.3.74 Deve Implementar controle de banda por porta;
- 2.3.75 Deve possibilitar a implementação de no mínimo 8 filas;
- 2.3.76 Deve possibilitar a remarcação de QoS;
- 2.3.77 Deve implementar controle de banda port/flow based rating limiting;
- 2.3.78 Segurança:
- 2.3.79 Deve implementar os seguintes tipos de Access Control List (ACL):
- 2.3.80 MAC de origem;
- 2.3.81 MAC de destino;
- 2.3.82 VLAN ID;
- 2.3.83 User Priority;
- 2.3.84 Ether Type;
- 2.3.85 IP de origem;
- 2.3.86 IP de destino;
- 2.3.87 Fragmento;
- 2.3.88 Protocolo IP;
- 2.3.89 Flag TCP;
- 2.3.90 Porta TCP/UDP;
- 2.3.91 DCSP/IP TOS;
- 2.3.92 ACL combinada;
- 2.3.93 Deve suportar ACL baseada em tempo;
- 2.3.94 As configurações de ACL devem ser aplicadas na porta e Vlan;
- 2.3.95 Deve implementar IP-MAC-PORT Binding com 512 entradas;
- 2.3.96 Deve implementar IP Source Guard;
- 2.3.97 Deve implementar proteção contra-ataques DoS;
- 2.3.98 Deve implementar port security;
- 2.3.99 Deve implementar Broadcast, Multicast e Unknown-unicast Storm Control;
- 2.3.100 Deve implementar IEEE 802.1X com autenticação baseada em porta e MAC;
- 2.3.101 Deve suportar IEEE 802.1X com associação automática de Vlan;
- 2.3.102 Deve suportar MAB (MAC Authentication Bypass);

- 2.3.103 Deve ter suporte à servidor RADIUS para autenticação;
- 2.3.104 Deve implementar Guest Vlan;
- 2.3.105 Deve implementar DHCP Snooping para IPv4 e para IPv6;
- 2.3.106 Deve suportar gerenciamento através de HTTPS com SSLv3/TLS 1.2;
- 2.3.107 Deve suportar gerenciamento através de interface de comandos segura com SSH V1 e v2;
- 2.3.108 Gerenciamento:
- 2.3.109 Deve implementar gerenciamento via WEB com HTTP e HTTPS;
- 2.3.110 Deve permitir o gerenciamento seguro através de linha de comandos (CLI) com SSHv2;
- 2.3.111 Deve ter suporte para AAA incluindo TACACS+;
- 2.3.112 Deve ter suporte para EEE (Energy Efficient Ethernet);
- 2.3.113 Deve suportar SNMP V1, V2c e V3;
- 2.3.114 Deve suportar SNMP Trap;
- 2.3.115 Deve suportar SNMP Inform;
- 2.3.116 Deve suportar as seguintes RFCs:
- 2.3.117 RFC1213;
- 2.3.118 RFC1493;
- 2.3.119 RFC1643;
- 2.3.120 RFC2021;
- 2.3.121 RFC2233;
- 2.3.122 RFC2618;
- 2.3.123 RFC2620;
- 2.3.124 RFC2674;
- 2.3.125 RFC2819;
- 2.3.126 RFC2925;
- 2.3.127 Deve implementar RMON com no mínimo 4 grupos;
- 2.3.128 Deve implementar Syslog;
- 2.3.129 Deve implementar NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol);
- 2.3.130 Deve implementar FTP/FTPv6 (File Transfer Protocol) ou TFTP/TFTPv6 (Trivial File Transfer Protocol);
- 2.3.131 Deve Implementar LLDP e LLDP MED conforme IEEE 802.1ab;
- 2.3.132 Deve implementar DHCP/BOOTP Cliente;
- 2.3.133 Deve possibilitar o monitoramento da CPU do Switch;

- 2.3.134 Deve possibilitar o armazenamento de dois arquivos de configuração simultaneamente (Dual Image);
- 2.3.135 Deve implementar Diagnóstico de cabos;
- 2.3.136 Deve implementar Ethernet Link OAM conforme IEEE 802.3ah;
- 2.3.137 Deve implementar DLDP (Device Link Detect Protocol);
- 2.3.138 Deve ser possível o gerenciamento do Switch através de solução de gerenciamento centralizado do próprio fabricante podendo ser este software ou appliance;
- 2.3.139 IPv6:
- 2.3.140 Deve implementar Pilha dupla (Dual IPv4/IPv6);
- 2.3.141 Deve implementar MLD (Multicast Listener Discovery);
- 2.3.142 Deve implementar ACL sobre IPv6;
- 2.3.143 Deve implementar rotas estáticas em IPv6 e interfaces VLAN sobre IPv6;
- 2.3.144 Deve implementar IPv6 Neighbor Discover (ND);
- 2.3.145 Deve implementar ICMP v6;
- 2.3.146 Deve implementar DHCPv6 Snooping;
- 2.3.147 Deve suportar as seguintes aplicações sobre IPv6:
- 2.3.148 DHCPv6 Cliente;
- 2.3.149 Ping6;
- 2.3.150 Tracert6;
- 2.3.151 Telnet v6;
- 2.3.152 IPv6 SNMP;
- 2.3.153 IPv6 SSH;
- 2.3.154 IPv6 SSL;
- 2.3.155 HTTP/HTTPS sobre IPv6;
- 2.3.156 FTP ou TFTP sobre IPv6;
- 2.3.157 Certificações, padronização e documentações:
- 2.3.158 Possuir homologação da ANATEL, de acordo com a resolução nº 715, de 23 de outubro de 2019;
- 2.3.159 O fabricante do produto indicado deve estar listado no relatório do Gartner – Magic Quadrant for Wired and Wireless LAN Access Infrastructure, publicado em março de 2024 -. O relatório Gartner – Magic Quadrant é uma representação gráfica das atividades do mercado tecnológico em um determinado período e fornece uma relação dos agentes mais relevantes do mercado;
- 2.3.160 Possuir Certificação FCC e CE;
- 2.3.161 Deve ser RoHS (Restriction of Certain Hazardous Substances) Compliance;
- 2.3.162 Deve possuir garantia de 60 meses ON-SITE pela Contratada;

- 2.3.163 O tempo de troca em caso de falhas deve ser de no máximo 30 (trinta) dias corridos, na modalidade de RMA Troca balcão;
- 2.3.164 Em caso de troca, o produto reposto deve ser novo e em perfeito estado, igual ou superior ao produto enviado;
- 2.3.165 O produto entregue pela contratada deve ser novo e acomodado em caixa de papelão;
- 2.3.166 O Proponente deve ser revenda autorizada pelo fabricante;
- 2.3.167 O proponente deve emitir declaração do fabricante atestando ser revenda autorizada a comercializar os produtos em território nacional;
- 2.3.168 Deve ser montável em rack padrão EIA 19''(dezenove polegadas) e possuir kits completos para instalação bem como ocupar o espaço de 1 (um) U em Rack;
- 2.3.169 Deve acompanhar manuais, cabo de energia, cabo para a porta console e aletas de montagem em rack.
- 2.3.170 Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste lote 02.

2.4 Switch Tipo IV, Layer 2+, 24 portas x 1 Gbps SFP, 4 x 10 Gbps SFP+

- 2.4.1 Características:
- 2.4.2 Deve possuir 20 (vinte) slots SFP 1000Base-X Conforme Padrões IEEE 802.3ae;
- 2.4.3 Deve possuir 4 (quatro) slots SFP/RJ45 no formato combo;
- 2.4.4 Deve possuir adicionalmente pelo menos 4 (quatro) slots 10G (SFP+) conforme padrões IEEE 802.3ae 10GBASE-SR e 10GBASE-LR;
- 2.4.5 As interfaces dos itens 2.4.2, 2.4.3 e 2.4.4 devem operar de modo simultâneo;
- 2.4.6 Deve possuir no mínimo 2 (duas) portas console uma do tipo RJ45 e outra Micro-USB;
- 2.4.7 Deve possuir fonte de alimentação interna, que opere com tensões de entrada entre 100 e 240 VAC e frequência de 50/60Hz;
- 2.4.8 Alimentação e Consumo:
- 2.4.9 Deve possuir consumo de energia máximo de até 35.7W;
- 2.4.10 Deve possuir consumo de energia em modo standby de até 17.6W;
- 2.4.11 Desempenho e Capacidades:
- 2.4.12 Deve possuir capacidade de processamento de no mínimo 128 Gbps;
- 2.4.13 Deve possuir taxa de encaminhamento de pacotes igual ou superior a 95.23 Mpps;
- 2.4.14 Sua tabela de MAC Address deve suportar no mínimo 16.000 MAC address;
- 2.4.15 Deve possuir Buffer de pacotes de no mínimo 12 Mbit;
- 2.4.16 Deve suportar jumbo frame de no mínimo 9 KB;
- 2.4.17 O equipamento deve possuir sistema de resfriamento com no máximo 1 fan;

- 2.4.18 Deve suportar temperatura de operação entre 0° e 45°C;
- 2.4.19 Deve suportar operação sob umidade entre 10% e 90% RH sem condensamento;
- 2.4.20 Funcionalidades de Camada 2:
- 2.4.21 Deve implementar agregação de links de modo estático;
- 2.4.22 Deve implementar o protocolo LACP (Link Aggregation Control Protocol) conforme IEEE 802.3ad;
- 2.4.23 Deve suportar a criação de no mínimo 8 grupos de portas agregadas com no mínimo 8 portas por grupo;
- 2.4.24 Deve implementar o protocolo Spanning tree e suas variações:
- 2.4.25 IEEE 802.1d STP (Spanning tree protocol);
- 2.4.26 IEEE 802.1w RSTP (Rapid Spanning Tree Protocol);
- 2.4.27 IEEE 802.1s MSTP (Multiple Spanning Tree Protocol);
- 2.4.28 Pelo menos 8 instâncias MSTI;
- 2.4.29 Deve implementar os protocolos de segurança STP:
- 2.4.30 TC Protect;
- 2.4.31 BPDU filter;
- 2.4.32 BPDU protect;
- 2.4.33 Root protect;
- 2.4.34 Loop protect;
- 2.4.35 Deve implementar controle de fluxo conforme IEEE 802.3X;
- 2.4.36 Deve implementar loopback detection baseada em porta e Vlan;
- 2.4.37 Deve implementar espelhamento de porta possibilitando o monitoramento de uma porta ou de um grupo de portas. Também deve possibilitar a escolha da direção do tráfego a ser espelhado, sendo TX, RX ou ambos;
- 2.4.38 Deve implementar o espelhamento da CPU para análises investigadas de eventuais falhas;
- 2.4.39 Deve implementar no mínimo 4.000 grupos de Vlans;
- 2.4.40 Deve possibilitar a configuração do ID da Vlan entre 2 e 4094;
- 2.4.41 Deve implementar Tagged Vlan conforme IEEE 802.1Q;
- 2.4.42 Deve implementar MAC Vlan com pelo menos 30 entradas;
- 2.4.43 Deve suportar no mínimo 1000 grupos IGMP;
- 2.4.44 Deve suportar pelo menos 8 anéis ERPS;
- 2.4.45 Deve Implementar GVRP (Generic Vlan Registration Protocol);
- 2.4.46 Deve implementar Vlan de voz. O Switch deverá ser capaz de reconhecer um telefone IP automaticamente e atribuí-lo uma VLAN de voz;

- 2.4.47 Multicast:
- 2.4.48 Deve implementar IGMP Snooping v1, v2 e v3;
- 2.4.49 Deve suportar IGMP Fast Leave, IGMP Snooping Querier e IGMP Authentication;
- 2.4.50 Deve suportar configuração de grupo de multicast estático;
- 2.4.51 Deve suportar MLD Snooping v1 e v2;
- 2.4.52 Deve suportar MLD Snooping Querier e MLD Fast Leave;
- 2.4.53 Deve implementar MVR (Multicast VLAN Registration);
- 2.4.54 Deve implementar filtro multicast com pelo menos 256 profiles e 16 entradas por profile;
- 2.4.55 Funcionalidades L3:
- 2.4.56 Deve suportar no mínimo 48 rotas estáticas IPv4/IPv6;
- 2.4.57 Deve implementar no mínimo 16 interfaces Vlan para fins de roteamento entre vlans;
- 2.4.58 Deve implementar interface Vlan para IPv4 e para IPv6;
- 2.4.59 Deve suportar configuração de interface de Loopback;
- 2.4.60 Deve implementar ARP estático com mínimo de 128 entradas;
- 2.4.61 Deve implementar servidor DHCP com pelo menos 8 pools;
- 2.4.62 Deve Implementar DHCP Relay com interface e Vlan relay;
- 2.4.63 Qualidade de Serviço:
- 2.4.64 Deve implementar classificação e marcação de pacotes em CoS e DSCP conforme IEEE 802.1p;
- 2.4.65 Deve implementar os seguintes algoritmos de gerenciamento de filas:
- 2.4.66 WRR (Weighted Round Robin);
- 2.4.67 SP (Strict Priority);
- 2.4.68 SP+WRR (Strict Priority + Weighted Round Robin);
- 2.4.69 Deve Implementar controle de banda por porta;
- 2.4.70 Deve possibilitar a implementação de no mínimo 8 filas;
- 2.4.71 Deve possibilitar a remarcação de QoS;
- 2.4.72 Deve implementar controle de banda port/flow based rating limiting;
- 2.4.73 Segurança:
- 2.4.74 Deve implementar os seguintes tipos de Access Control List (ACL):
- 2.4.75 MAC de origem;
- 2.4.76 MAC de destino;
- 2.4.77 VLAN ID;
- 2.4.78 User Priority;
- 2.4.79 Ether Type;

- 2.4.80 IP de origem;
- 2.4.81 IP de destino;
- 2.4.82 Fragmento;
- 2.4.83 Protocolo IP;
- 2.4.84 Flag TCP;
- 2.4.85 Porta TCP/UDP;
- 2.4.86 DCSP/IP TOS;
- 2.4.87 ACL combinada;
- 2.4.88 Deve suportar ACL baseada em tempo;
- 2.4.89 As configurações de ACL devem ser aplicadas na porta e Vlan;
- 2.4.90 Deve implementar IP-MAC-PORT Binding com 512 entradas;
- 2.4.91 Deve implementar IP Source Guard;
- 2.4.92 Deve implementar proteção contra-ataques DoS;
- 2.4.93 Deve implementar port security;
- 2.4.94 Deve implementar Broadcast, Multicast e Unknown-unicast Storm Control;
- 2.4.95 Deve implementar IEEE 802.1X com autenticação baseada em porta e MAC;
- 2.4.96 Deve suportar IEEE 802.1X com associação automática de Vlan;
- 2.4.97 Deve suportar MAB (MAC Authentication Bypass);
- 2.4.98 Deve ter suporte à servidor RADIUS para autenticação;
- 2.4.99 Deve implementar Guest Vlan;
- 2.4.100 Deve implementar DHCP Snooping para IPv4 e para IPv6;
- 2.4.101 Deve suportar gerenciamento através de HTTPS com SSLv3/TLS 1.2;
- 2.4.102 Deve suportar gerenciamento através de interface de comandos segura com SSH V1 e v2;
- 2.4.103 Gerenciamento:
- 2.4.104 Deve implementar gerenciamento via WEB com HTTP e HTTPS;
- 2.4.105 Deve permitir o gerenciamento seguro através de linha de comandos (CLI) com SSHv2;
- 2.4.106 Deve ter suporte para AAA incluindo TACACS+;
- 2.4.107 Deve ter suporte para EEE (Energy Efficient Ethernet);
- 2.4.108 Deve suportar SNMP V1, V2c e V3;
- 2.4.109 Deve suportar SNMP Trap;
- 2.4.110 Deve suportar SNMP Inform;
- 2.4.111 Deve suportar as seguintes RFCs:
- 2.4.112 RFC1213;

- 2.4.113 RFC1493;
- 2.4.114 RFC1643;
- 2.4.115 RFC2021;
- 2.4.116 RFC2233;
- 2.4.117 RFC2618;
- 2.4.118 RFC2620;
- 2.4.119 RFC2674;
- 2.4.120 RFC2819;
- 2.4.121 RFC2925;
- 2.4.122 Deve implementar RMON com no mínimo 4 grupos;
- 2.4.123 Deve implementar Syslog;
- 2.4.124 Deve implementar NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol);
- 2.4.125 Deve implementar FTP/FTPv6 (File Transfer Protocol) ou TFTP/TFTPv6 (Trivial File Transfer Protocol);
- 2.4.126 Deve Implementar LLDP e LLDP MED conforme IEEE 802.1ab;
- 2.4.127 Deve implementar DHCP/BOOTP Cliente;
- 2.4.128 Deve possibilitar o monitoramento da CPU do Switch;
- 2.4.129 Deve possibilitar o armazenamento de dois arquivos de configuração simultaneamente (Dual Image);
- 2.4.130 Deve implementar Diagnóstico de cabos;
- 2.4.131 Deve implementar Ethernet Link OAM conforme IEEE 802.3ah;
- 2.4.132 Deve implementar DLDP (Device Link Detect Protocol);
- 2.4.133 Deve ser possível o gerenciamento do Switch através de solução de gerenciamento centralizado do próprio fabricante podendo ser este software ou appliance;
- 2.4.134 IPv6:
- 2.4.135 Deve implementar Pilha dupla (Dual IPv4/IPv6);
- 2.4.136 Deve implementar MLD (Multicast Listener Discovery);
- 2.4.137 Deve implementar ACL sobre IPv6;
- 2.4.138 Deve implementar rotas estáticas em IPv6 e interfaces VLAN sobre IPv6;
- 2.4.139 Deve implementar IPv6 Neighbor Discover (ND);
- 2.4.140 Deve implementar ICMP v6;
- 2.4.141 Deve implementar DHCPv6 Snooping;
- 2.4.142 Deve suportar as seguintes aplicações sobre IPv6:
- 2.4.143 DHCPv6 Cliente;

- 2.4.144 Ping6;
- 2.4.145 Tracert6;
- 2.4.146 Telnet v6;
- 2.4.147 IPv6 SNMP;
- 2.4.148 IPv6 SSH;
- 2.4.149 IPv6 SSL;
- 2.4.150 HTTP/HTTPS sobre IPv6;
- 2.4.151 FTP ou TFTP sobre IPv6;
- 2.4.152 Certificações, padronização e documentações:
- 2.4.153 Possuir homologação da ANATEL, de acordo com a resolução nº 715, de 23 de outubro de 2019;
- 2.4.154 O fabricante do produto indicado deve estar listado no relatório do Gartner – Magic Quadrant for Wired and Wireless LAN Access Infrastructure, publicado em março de 2024 -. O relatório Gartner – Magic Quadrant é uma representação gráfica das atividades do mercado tecnológico em um determinado período e fornece uma relação dos agentes mais relevantes do mercado;
- 2.4.155 Possuir Certificação FCC e CE;
- 2.4.156 Deve ser RoHS (Restriction of Certain Hazardous Substances) Compliance;
- 2.4.157 Deve possuir garantia de 60 meses ON-SITE pela Contratada;
- 2.4.158 O tempo de troca em caso de falhas deve ser de no máximo 30 (trinta) dias corridos, na modalidade de RMA Troca balcão;
- 2.4.159 Em caso de troca, o produto reposto deve ser novo e em perfeito estado, igual ou superior ao produto enviado;
- 2.4.160 O produto entregue pela contratada deve ser novo e acomodado em caixa de papelão;
- 2.4.161 O Proponente deve ser revenda autorizada pelo fabricante;
- 2.4.162 O proponente deve emitir declaração do fabricante atestando ser revenda autorizada a comercializar os produtos em território nacional;
- 2.4.163 Deve ser montável em rack padrão EIA 19’’(dezenove polegadas) e possuir kits completos para instalação bem como ocupar o espaço de 1 (um) U em Rack;
- 2.4.164 Deve acompanhar manuais, cabo de energia, cabo para a porta console e aletas de montagem em rack.
- 2.4.165 Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste lote 02.

2.5 Switch Tipo V, Layer 3, 26 portas x 10 Gbps SFP+, 6 x 25 Gbps SFP28

- 2.5.1 Características:

- 2.5.2 Deve possuir 26 (vinte e seis) slots 10GE SFP+ conforme padrões IEEE 802.3ae 10GBASE-SR e 10GBASE-LR;
- 2.5.3 Deve possuir adicionalmente pelo menos 6 (seis) slots 25GE SFP28 conforme padrões IEEE802.3by 25GBASE-SR e 25GBASE-LR;
- 2.5.4 As interfaces dos itens 2.5.2 e 2.5.3 devem operar de modo simultâneo;
- 2.5.5 Deve possuir no mínimo 2 (duas) portas console do tipo RJ45 e USB-C;
- 2.5.6 Deve possuir no mínimo 1 (uma) porta de gerenciamento RJ45;
- 2.5.7 Deve possuir no mínimo 2 (duas) portas USB 3.0;
- 2.5.8 Deve possuir fonte de alimentação modular redundante Hot-Swappable, que opere com tensões de entrada entre 100 e 240 VAC e frequência de 50/60Hz;
- 2.5.9 Deve ter sistema de proteção ESD de +-15kV ar e +-8kV contact;
- 2.5.10 Deve ter sistema de proteção Surge de +-6kV service port e +-4kV power port;
- 2.5.11 Desempenho e Capacidades:
- 2.5.12 Deve possuir capacidade de processamento de no mínimo 820 Gbps;
- 2.5.13 Deve possuir taxa de encaminhamento de pacotes igual ou superior a 610 Mpps;
- 2.5.14 Sua tabela de MAC Address deve suportar no mínimo 128.000 MAC address;
- 2.5.15 Deve possuir Buffer de pacotes de no mínimo 8 MB;
- 2.5.16 Deve suportar jumbo frame de no mínimo 9 KB;
- 2.5.17 O equipamento deve possuir no mínimo 4 (quatro) ventoinhas modulares Hot-Swappable para resfriamento;
- 2.5.18 Deve ter sistema de direção de ar front-to-back;
- 2.5.19 Deve suportar temperatura de operação entre -5° e 50° para altitude de até 300m;
- 2.5.20 Deve suportar operação sob umidade entre 10% e 90% RH sem condensamento;
- 2.5.21 Funcionalidades de Camada 2:
- 2.5.22 Deve implementar agregação de links de modo estático;
- 2.5.23 Deve implementar o protocolo LACP (Link Aggregation Control Protocol) conforme IEEE 802.3ad;
- 2.5.24 Deve suportar a criação de no mínimo 120 grupos de portas agregadas com no mínimo 8 portas por grupo;
- 2.5.25 Deve implementar o protocolo Spanning tree e suas variações:
- 2.5.26 IEEE 802.1d STP (Spanning tree protocol);
- 2.5.27 IEEE 802.1w RSTP (Rapid Spanning Tree Protocol);
- 2.5.28 IEEE 802.1s MSTP (Multiple Spanning Tree Protocol);
- 2.5.29 Pelo menos 64 instâncias MSTI;
- 2.5.30 Deve implementar os protocolos de segurança STP:

- 2.5.31 TC Protect;
- 2.5.32 BPDU filter;
- 2.5.33 BPDU protect;
- 2.5.34 Root protect;
- 2.5.35 Loop protec;
- 2.5.36 Deve implementar controle de fluxo conforme IEEE 802.3X;
- 2.5.37 Deve implementar loopback detection baseada em porta e Vlan;
- 2.5.38 Deve implementar espelhamento de porta possibilitando o monitoramento de uma porta ou de um grupo de portas. Também deve possibilitar a escolha da direção do tráfego a ser espelhado, sendo TX, RX ou ambos;
- 2.5.39 Deve implementar o espelhamento da CPU para análises investigadas de eventuais falhas;
- 2.5.40 Deve implementar no mínimo 4000 grupos de Vlans;
- 2.5.41 Deve possibilitar a configuração do ID da Vlan entre 2 e 4094;
- 2.5.42 Deve implementar Tagged Vlan conforme IEEE 802.1Q;
- 2.5.43 Deve implementar MAC Vlan com pelo menos 200 entradas;
- 2.5.44 Deve suportar no mínimo 4093 grupos IGMP;
- 2.5.45 Deve suportar pelo menos 64 anéis ERPS;
- 2.5.46 Deve implementar RSPAN;
- 2.5.47 Deve Implementar GVRP (Generic Vlan Registration Protocol);
- 2.5.48 Deve implementar Vlan de voz. O Switch deverá ser capaz de reconhecer um telefone IP automaticamente e atribuí-lo uma VLAN de voz;
- 2.5.49 Multicast:
- 2.5.50 Deve implementar IGMP Snooping v1, v2 e v3;
- 2.5.51 Deve suportar IGMP Fast Leave, IGMP Snooping Querier, IGMP Authentication e L2 Multicast table com no mínimo de 4.093 entradas;
- 2.5.52 Deve suportar configuração de grupo de multicast estático;
- 2.5.53 Deve suportar MLD Snooping v1 e v2;
- 2.5.54 Deve suportar MLD Snooping Querier e MLD Fast Leave;
- 2.5.55 Deve implementar MVR (Multicast VLAN Registration) com mínimo de 4.093 entradas;
- 2.5.56 Deve implementar filtro multicast com pelo menos 256 profiles e 16 entradas por profile;
- 2.5.57 Deve implementar PIM-DM/SM baseado em IPv4 com mínimo de 1.024 entradas de rotas multicast.
- 2.5.58 Funcionalidades L3:
- 2.5.59 Deve suportar no mínimo 2048 rotas estáticas IPv4;

- 2.5.60 Deve suportar no mínimo 1024 rotas estáticas IPv6;
- 2.5.61 Deve implementar 15.300 entradas de Host Route Table;
- 2.5.62 Deve implementar no mínimo 256 interfaces Vlan para fins de roteamento entre vlans;
- 2.5.63 Deve implementar interface Vlan para IPv4 e para IPv6;
- 2.5.64 Deve suportar configuração de interface de Loopback;
- 2.5.65 Deve implementar Proxy Arp;
- 2.5.66 Deve implementar protocolo de roteamento RIPv1/v2 com mínimo de 102.400 entradas;
- 2.5.67 Deve implementar protocolo de roteamento RIPng com no mínimo 51.200 entradas
- 2.5.68 Deve implementar protocolo de roteamento OSPF;
- 2.5.69 Pelo menos 102.400 na versão 2;
- 2.5.70 Pelo menos 51.200 na versão 3;
- 2.5.71 Deve suportar empilhamento de no mínimo 8 stacks;
- 2.5.72 Deve suportar o protocolo VRRP v2/v3 de pelo menos 64 grupos;
- 2.5.73 Deve implementar mínimo 256 entradas ECMP;
- 2.5.74 Deve implementar o roteamento policy-based (PBR);
- 2.5.75 Deve implementar ARP estático com mínimo de 1.024 entradas;
- 2.5.76 Deve implementar ARP dinâmico com mínimo de 24.576 entradas;
- 2.5.77 Deve implementar servidor DHCP com 64 pools de IPs e 1.000 entradas de vinculação manual;
- 2.5.78 Deve Implementar DHCP Relay com relayed interface e Vlan;
- 2.5.79 Qualidade de Serviço:
- 2.5.80 Deve implementar classificação e marcação de pacotes em CoS e DSCP conforme IEEE 802.1p;
- 2.5.81 Deve implementar os seguintes algoritmos de gerenciamento de filas:
- 2.5.82 WRR (Weighted Round Robin);
- 2.5.83 SP (Strict Priority);
- 2.5.84 SP+WRR (Strict Priority + Weighted Round Robin);
- 2.5.85 Deve Implementar controle de banda por porta;
- 2.5.86 Deve possibilitar a implementação de no mínimo 8 filas;
- 2.5.87 Deve possibilitar a remarcação de QoS;
- 2.5.88 Deve implementar controle de banda rate limit e storm control;
- 2.5.89 Segurança:
- 2.5.90 Deve implementar os seguintes tipos de Access Control List (ACL):
- 2.5.91 MAC de origem;
- 2.5.92 MAC de destino;

- 2.5.93 VLAN ID;
- 2.5.94 User Priority;
- 2.5.95 Ether Type;
- 2.5.96 IP de origem;
- 2.5.97 IP de destino;
- 2.5.98 Fragmento;
- 2.5.99 Protocolo IP;
- 2.5.100 Flag TCP;
- 2.5.101 Porta TCP/UDP;
- 2.5.102 DCSP/IP TOS;
- 2.5.103 ACL combinada;
- 2.5.104 Deve suportar ACL baseada em tempo;
- 2.5.105 Deve implementar ACL sobre IPv6;
- 2.5.106 As configurações de ACL devem ser aplicadas na porta e Vlan;
- 2.5.107 Deve implementar IP-MAC-PORT Binding com 1.024 entradas;
- 2.5.108 Deve implementar IP Source Guard;
- 2.5.109 Deve implementar proteção contra-ataques DoS;
- 2.5.110 Deve implementar port security;
- 2.5.111 Deve implementar Broadcast, Multicast e Unknown-unicast Storm Control;
- 2.5.112 Deve implementar IEEE 802.1X com autenticação baseada em porta e MAC;
- 2.5.113 Deve suportar IEEE 802.1X com associação automática de Vlan;
- 2.5.114 Deve suportar MAB (MAC Authentication Bypass);
- 2.5.115 Deve ter suporte à servidor RADIUS para autenticação;
- 2.5.116 Deve implementar Guest Vlan;
- 2.5.117 Deve implementar DHCP Snooping para IPv4 e para IPv6;
- 2.5.118 Deve suportar gerenciamento através de HTTPS com SSLv3/TLS 1.2;
- 2.5.119 Deve suportar gerenciamento através de interface de comandos segura com SSH V1 e v2;
- 2.5.120 Gerenciamento:
- 2.5.121 Deve implementar gerenciamento via WEB com HTTP e HTTPS;
- 2.5.122 Deve permitir o gerenciamento seguro através de linha de comandos (CLI) com SSHv2;
- 2.5.123 Deve ter suporte para AAA incluindo TACACS+;
- 2.5.124 Deve ter suporte para EEE (Energy Efficient Ethernet);
- 2.5.125 Deve suportar SNMP V1, V2c e V3;

- 2.5.126 Deve suportar SNMP Trap;
- 2.5.127 Deve suportar SNMP Inform;
- 2.5.128 Deve suportar as seguintes RFCs:
- 2.5.129 RFC1213;
- 2.5.130 RFC1493;
- 2.5.131 RFC1643;
- 2.5.132 RFC2021;
- 2.5.133 RFC2233;
- 2.5.134 RFC2618;
- 2.5.135 RFC2620;
- 2.5.136 RFC2674;
- 2.5.137 RFC2819;
- 2.5.138 RFC2925;
- 2.5.139 Deve implementar RMON com no mínimo 4 grupos;
- 2.5.140 Deve implementar NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol);
- 2.5.141 Deve implementar FTP/FTPv6 (File Transfer Protocol) ou TFTP/TFTPv6 (Trivial File Transfer Protocol);
- 2.5.142 Deve Implementar LLDP e LLDP MED conforme IEEE 802.1ab;
- 2.5.143 Deve implementar Syslog;
- 2.5.144 Deve implementar DHCP/BOOTP Cliente;
- 2.5.145 Deve possibilitar o monitoramento da CPU do Switch;
- 2.5.146 Deve possibilitar o armazenamento de dois arquivos de configuração simultaneamente (Dual Image);
- 2.5.147 Deve implementar Diagnóstico de cabos;
- 2.5.148 Deve implementar Diagnóstico de cabos virtual (VCT);
- 2.5.149 Deve implementar Ethernet Link OAM conforme IEEE 802.3ah;
- 2.5.150 Deve implementar DLDP (Device Link Detect Protocol);
- 2.5.151 Deve ser possível o gerenciamento do Switch através de solução de gerenciamento centralizado do próprio fabricante podendo ser este software ou appliance;
- 2.5.152 IPv6:
- 2.5.153 Deve implementar Pilha dupla (Dual IPv4/IPv6);
- 2.5.154 Deve implementar MLD (Multicast Listener Discovery);
- 2.5.155 Deve implementar ACL sobre IPv6;
- 2.5.156 Deve implementar rotas estáticas em IPv6 e interfaces VLAN sobre IPv6;

- 2.5.157 Deve implementar IPv6 Neighbor Discover (ND);
- 2.5.158 Deve implementar ICMP v6;
- 2.5.159 Deve implementar DHCPv6 Snooping;
- 2.5.160 Deve suportar as seguintes aplicações sobre IPv6:
- 2.5.161 DHCPv6 Cliente;
- 2.5.162 Ping6;
- 2.5.163 Tracert6;
- 2.5.164 Telnet v6;
- 2.5.165 IPv6 SNMP;
- 2.5.166 IPv6 SSH;
- 2.5.167 IPv6 SSL;
- 2.5.168 HTTP/HTTPS sobre IPv6;
- 2.5.169 FTP ou TFTP sobre IPv6;
- 2.5.170 Certificações, padronização e documentações:
- 2.5.171 Possuir homologação da ANATEL, de acordo com a resolução nº 715, de 23 de outubro de 2019;
- 2.5.172 O fabricante do produto indicado deve estar listado no relatório do Gartner – Magic Quadrant for Wired and Wireless LAN Access Infrastructure, publicado em março de 2024 -. O relatório Gartner – Magic Quadrant é uma representação gráfica das atividades do mercado tecnológico em um determinado período e fornece uma relação dos agentes mais relevantes do mercado;
- 2.5.173 Possuir Certificação FCC e CE;
- 2.5.174 Deve ser RoHS (Restriction of Certain Hazardous Substances) Compliance;
- 2.5.175 Deve possuir garantia de 60 meses ON-SITE pela Contratada;
- 2.5.176 O tempo de troca em caso de falhas deve ser de no máximo 30 (trinta) dias corridos, na modalidade de RMA Troca balcão;
- 2.5.177 Em caso de troca, o produto reposto deve ser novo e em perfeito estado, igual ou superior ao produto enviado;
- 2.5.178 O produto entregue pela contratada deve ser novo e acomodado em caixa de papelão;
- 2.5.179 O Proponente deve ser revenda autorizada pelo fabricante;
- 2.5.180 O proponente deve emitir declaração do fabricante atestando ser revenda autorizada a comercializar os produtos em território nacional;
- 2.5.181 Deve ser montável em rack padrão EIA 19’’(dezenove polegadas) e possuir kits completos para instalação bem como ocupar o espaço de 1 (um) U em Rack;
- 2.5.182 Deve acompanhar manuais, cabo de energia, cabo para a porta console e aletas de montagem em rack.

- 2.5.183 Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste lote 02.

2.6 Access Point Tipo I - Indoor

- 2.6.1 Características:
- 2.6.2 Deve possuir 1 (uma) portas Gigabit Ethernet 10/100/1000Base-T Conforme Padrões IEEE 802.3, IEEE 802.3u, IEEE 802.3ab;
- 2.6.3 A interface deverá ser Full-Duplex, auto sensing com conector RJ45 fêmea e implementar mecanismos de autoconfiguração;
- 2.6.4 A interface deverá suportar o padrão IEEE 802.3af ou IEEE 802.3at e fonte externa 12vdc;
- 2.6.5 Deve possuir consumo máximo de 14W;
- 2.6.6 Deve possuir botão ou entrada para Reset;
- 2.6.7 Deve vir acompanhado de kit para montagem em teto ou parede;
- 2.6.8 Deve suportar temperatura de operação entre 0° a 40°;
- 2.6.9 Deve suportar operação sob humidade entre 10% e 90% RH sem condensamento;
- 2.6.10 Deve possuir Led para indicar status de funcionamento;
- 2.6.11 Deve acompanhar injetor PoE do mesmo fabricante do access point;
- 2.6.12 Características Wireless:
- 2.6.13 Deve ser do tipo dual band implementando Rádio de 2.4Ghz e Rádio de 5Ghz com operação simultânea de ambos;
- 2.6.14 Deve implementar no mínimo 2402Mbps sobre o rádio 5Ghz;
- 2.6.15 Deve implementar no mínimo 574Mbps sobre o rádio de 2.4Ghz;
- 2.6.16 Deve possuir no mínimo 2 (duas) antenas internas omnidirecional com ganho de 4dBi para 2.4Ghz;
- 2.6.17 Deve possuir no mínimo 2 (duas) antenas internas omnidirecional com ganho de 5dBi para 5Ghz;
- 2.6.18 Deve possuir potência de transmissão conforme FCC: <25dBm (2.4GHz), <25dBm (5GHz);
- 2.6.19 Deve possuir potência de transmissão conforme CE:<20dBm (2.4GHz), <23dBm (5GHz);
- 2.6.20 Deve implementar os padrões E IEEE 802.11a/b/g/n/ac/ax;
- 2.6.21 Deve implementar no padrão 802.11ax 8 Mbps até 2402 Mbps (MCS0- MCS11, NSS = 1 até 2 HE20/40/80/160)
- 2.6.22 Deve permitir a associação de no mínimo 250 (duzentos e cinquenta) usuários;
- 2.6.23 Funcionalidades:
- 2.6.24 Deve possibilitar a criação de no mínimo 8 SSIDs por banda;
- 2.6.25 Deve permitir atrelar o SSID a uma Vlan (Tagged Vlan);

- 2.6.26 Deve suportar criptografia WEP, WPA/WPA2/WPA3-Personal/Enterprise;
- 2.6.27 Deve suportar QoS (WMM);
- 2.6.28 Deve implementar MU-MIMO;
- 2.6.29 Deve implementar Mesh;
- 2.6.30 Deve implementar Beamforming;
- 2.6.31 Deve implementar Airtime Fairness;
- 2.6.32 Deve implementar Band Steering;
- 2.6.33 Deve implementar Rate limit para controle de banda por SSID;
- 2.6.34 Deve implementar Load Balance para ambientes de alta densidade;
- 2.6.35 Deve implementar agendamento de reinicialização;
- 2.6.36 Deve possuir detecção de Rogue APs;
- 2.6.37 Deve implementar IEEE 802.1x;
- 2.6.38 Deve implementar Captive Portal;
- 2.6.39 Deve possibilitar a utilização de captive portal externo e autenticação via Radius;
- 2.6.40 Deve possibilitar a criação de senhas de acesso para visitantes individuais com configuração de duração de conexão através da controladora;
- 2.6.41 Deve implementar a varredura e selecionar o melhor canal de modo automático;
- 2.6.42 Deve ser fornecido controlador compatível com Access Point e todas as licenças de operação;
- 2.6.43 Deve ser possível desabilitar o Led do Access Point;
- 2.6.44 Deve suportar gerenciamento centralizado através de ferramenta de gerenciamento do próprio fabricante a fim de garantir melhor interoperabilidade e acesso aos recursos;
- 2.6.45 Certificações e requisitos:
- 2.6.46 Deve ser do mesmo fabricante da Controladora a fim de garantir a interoperabilidade;
- 2.6.47 O fabricante do produto indicado deve estar listado no relatório do Gartner – Magic Quadrant for Wired and Wireless LAN Access Infrastructure, publicado em Novembro de 2022 -. O relatório Gartner – Magic Quadrant é uma representação gráfica das atividades do mercado tecnológico em um determinado período e fornece uma relação dos agentes mais relevantes do mercado;
- 2.6.48 Deve ser homologado pela Anatel;
- 2.6.49 Deve possuir certificação CE e FCC;
- 2.6.50 Deve ser RoHS (Restriction of Certain Hazardous Substances) Compliance;
- 2.6.51 O Proponente deve ser canal autorizado pelo fabricante;
- 2.6.52 O proponente deve emitir carta atestando ser canal autorizado pelo fabricante;
- 2.6.53 O equipamento deve possuir garantia de 60 meses ON-SITE pela Contratada;
- 2.6.54 A troca de equipamentos defeituosos deve ser do tipo RMA troca balcão com o prazo máximo de 30 (trinta) dias corridos;

- 2.6.55 Em caso de troca em garantia o produto reposto deverá novo e sem uso anterior, do mesmo modelo ou superior;
- 2.6.56 O produto ofertado, deverá ser novo e sem uso anterior;
- 2.6.57 Deve acompanhar o produto todos os itens para seu pleno funcionamento como fonte, kit para montagem em teto ou parede, manuais e licenças de software;
- 2.6.58 Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste lote 02.

2.7 Access Point Tipo II - Indoor

- 2.7.1 Características:
- 2.7.2 Deve possuir 1 (uma) porta Gigabit Ethernet 10/100/1000/2500Mbps conforme Padrões IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3bz;
- 2.7.3 A interface deverá ser Full-Duplex, auto sensing com conector RJ45 fêmea e implementar mecanismos de autoconfiguração;
- 2.7.4 A interface deverá suportar o padrão IEEE 802.3at;
- 2.7.5 Deve possuir consumo máximo de 25.44W;
- 2.7.6 Deve possuir botão ou entrada para Reset;
- 2.7.7 Deve vir acompanhado de kit para montagem em poste ou parede;
- 2.7.8 Deve suportar temperatura de operação entre 0 °C a 40 °C
- 2.7.9 Deve suportar operação sob humidade entre 10% e 90% RH sem condensamento;
- 2.7.10 Deve acompanhar injetor PoE do mesmo fabricante do access point;
- 2.7.11 Características Wireless:
- 2.7.12 Deve ser do tipo Tri-Band implementando Rádio de 2.4GHz, Rádio de 5GHz e Rádio de 6GHz com operação simultânea de ambos;
- 2.7.13 Deve suportar BLE 5.2 com pelo menos 1 (uma) antena de 4.0 dBi.
- 2.7.14 Deve implementar no mínimo 5760 Mbps sobre o rádio de 6GHz;
- 2.7.15 Deve implementar no mínimo 4324Mbps sobre o rádio de 5GHz;
- 2.7.16 Deve implementar no mínimo 574Mbps sobre o rádio de 2.4GHz;
- 2.7.17 Deve possuir no mínimo 2 (duas) antenas internas omnidirecional com ganho de 4dBi para 2.4GHz, 5dBi para 5GHz e 5dBi para 6GHz;
- 2.7.18 Deve possuir potência de transmissão conforme CE: <20 dBm (2.4 GHz, EIRP); <23 dBm (5 GHz, band 1&band 2, EIRP); <28 dBm (5 GHz, band 3, EIRP); <23dBm (6 GHz, EIRP);
- 2.7.19 Deve implementar os padrões IEEE 802.11a/b/g/n/ac/ax/be;
- 2.7.20 Deve permitir a associação de no mínimo 384 usuários;
- 2.7.21 Deve suportar a seguinte taxa de dados:

- 2.7.22 802.11be: 5G Band: 8Mbps to 4324Mbps (MCS0—MCS13, NSS=1 to 2 BE20/40/80/160/240);
- 2.7.23 6G Band: 8Mbps to 5765Mbps (MCS0—MCS13, NSS=1 to 2 BE20/40/80/160/320);
- 2.7.24 802.11ax: 2G Band: 8Mbps to 574Mbps (MCS0—MCS11, NSS=1 to 2 HE20/40);
- 2.7.25 5G Band: 8Mbps to 2402Mbps (MCS0—MCS11, NSS=1 to 2 HE20/40/80/160);
- 2.7.26 6G Band: 8Mbps to 2402Mbps (MCS0—MCS11, NSS=1 to 2 HE20/40/80/160);
- 2.7.27 802.11ac: 6.5Mbps to 2166.7Mbps (MCS0—MCS11, NSS=1 to 2 VHT20/40/80/160);
- 2.7.28 802.11n: 6.5Mbps to 300Mbps (MCS0—MCS15, HT20/40);
- 2.7.29 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps;
- 2.7.30 802.11b: 1, 2, 5.5, 11Mbps;
- 2.7.31 802.11a: 6, 9, 12, 18, 24, 36, 48, 54Mbps;
- 2.7.32 Funcionalidades:
- 2.7.33 Deve possibilitar a criação de no mínimo 8 SSIDs por banda;
- 2.7.34 Deve permitir atrelar o SSID a uma VLAN (Tagged VLAN);
- 2.7.35 Deve suportar criptografia WPA-Personal/Enterprise, WPA2-Personal/Enterprise, WPA3-Personal/Enterprise, OWE;
- 2.7.36 Deve suportar Largura de Banda de 320MHz;
- 2.7.37 Deve suportar OFDMA;
- 2.7.38 Deve suportar Atribuição automática de canais;
- 2.7.39 Deve suportar QoS (WMM);
- 2.7.40 Deve implementar Seamless Roaming;
- 2.7.41 Deve implementar MU-MIMO;
- 2.7.42 Deve implementar Beamforming;
- 2.7.43 Deve implementar Airtime Fairness;
- 2.7.44 Deve implementar Band Steering;
- 2.7.45 Deve suportar Mesh;
- 2.7.46 Deve implementar Rate Limit para controle de banda por SSID;
- 2.7.47 Deve implementar Load Balance para ambientes de alta densidade;
- 2.7.48 Deve implementar agendamento de reinicialização;
- 2.7.49 Deve suportar detecção de Rogue APs;
- 2.7.50 Deve suportar IEEE 802.1x;
- 2.7.51 Deve implementar Captive Portal;
- 2.7.52 Deve possibilitar a utilização de Captive Portal externo e autenticação via Radius;

- 2.7.53 Deve possibilitar a criação de senhas de acesso para visitantes individuais com configuração de duração de conexão através da controladora;
- 2.7.54 Deve implementar a varredura e selecionar o melhor canal de modo automático;
- 2.7.55 Deve ser fornecido controlador compatível com Access Point e todas as licenças de operação;
- 2.7.56 Deve ser possível desabilitar o Led do Access Point;
- 2.7.57 Deve suportar gerenciamento centralizado através de ferramenta de gerenciamento do próprio fabricante a fim de garantir melhor interoperabilidade e acesso aos recursos;
- 2.7.58 Certificações e requisitos:
- 2.7.59 Deve ser do mesmo fabricante da Controladora a fim de garantir a interoperabilidade;
- 2.7.60 O fabricante do produto indicado deve estar listado no relatório do Gartner – Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure, publicado em Março de 2024 -. O relatório Gartner – Magic Quadrant é uma representação gráfica das atividades do mercado tecnológico em um determinado período e fornece uma relação dos agentes mais relevantes do mercado;
- 2.7.61 Deve ser homologado pela Anatel;
- 2.7.62 Deve possuir certificação CE e FCC;
- 2.7.63 Deve ser RoHS (Restriction of Certain Hazardous Substances) Compliance;
- 2.7.64 O Proponente deve ser canal autorizado pelo fabricante;
- 2.7.65 O Proponente deve emitir carta atestando ser canal autorizado pelo fabricante;
- 2.7.66 Deve possuir garantia de 60 meses ON-SITE pela Contratada;
- 2.7.67 A troca de equipamentos defeituosos deve ser do tipo RMA troca balcão com o prazo máximo de 30 (trinta) dias corridos;
- 2.7.68 Em caso de troca em garantia o produto reposto deverá novo e sem uso anterior, do mesmo modelo ou superior;
- 2.7.69 O produto ofertado, deverá ser novo e sem uso anterior;
- 2.7.70 Deve acompanhar o produto todo o kit para montagem em poste ou parede, manuais e licenças de software;
- 2.7.71 Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste lote 02.

2.8 Access Point Tipo III - Outdoor

- 2.8.1 Características:
- 2.8.2 Deve possuir 1 (uma) portas Gigabit Ethernet 10/100/1000Base-T Conforme Padrões IEEE 802.3, IEEE 802.3u, IEEE 802.3ab;
- 2.8.3 A interface deverá ser Full-Duplex, auto sensing com conector RJ45 fêmea e implementar mecanismos de autoconfiguração;
- 2.8.4 A interface deverá suportar o padrão IEEE 802.3 at;

- 2.8.5 Deve ser fornecido o injetor PoE junto ao dispositivo do tipo PoE Passivo 48V ou padrão IEEE 802.3at;
- 2.8.6 Deve possuir consumo máximo de 14.7W;
- 2.8.7 Deve possuir botão ou entrada para Reset;
- 2.8.8 Deve vir acompanhado de kit para montagem em poste ou parede;
- 2.8.9 Deve suportar temperatura de operação entre -30 °C a 70 °C
- 2.8.10 Deve suportar operação sob humidade entre 10% e 90% RH sem condensamento;
- 2.8.11 Deve possuir caixa à prova de intempéries de classificação mínima IP67;
- 2.8.12 Características Wireless:
- 2.8.13 Deve ser do tipo dual band implementando Rádio de 2.4Ghz e Rádio de 5Ghz com operação simultânea de ambos;
- 2.8.14 Deve implementar no mínimo 1201Mbps sobre o rádio 5Ghz;
- 2.8.15 Deve implementar no mínimo 574Mbps sobre o rádio de 2.4Ghz;
- 2.8.16 Deve possuir no mínimo 2 antenas internas dual band omnidirecionais com ganho de no mínimo 4dBi para 2.4 GHz e 5dBi para 5GHz;
- 2.8.17 Deve possuir potência de transmissão conforme FCC: <25dBm (2.4GHz), <25dBm (5GHz);
- 2.8.18 Deve possuir potência de transmissão conforme CE:<20dBm (2.4GHz), <30dBm (5GHz, EIRP);
- 2.8.19 Deve implementar os padrões IEEE 802.11a/b/g/n/ac/ax;
- 2.8.20 Deve permitir a associação de no mínimo 250 usuários;
- 2.8.21 Deve suportar a seguinte taxa de dados:
- 2.8.22 802.11ax: 8 Mbps to 1201 Mbps (MCS0-MCS11, NSS = 1 to 2 HE20/40/80);
- 2.8.23 802.11ac: 6.5 Mbps to 1083.3 Mbps (MCS0-MCS9, NSS = 1 to 2 VHT20/40/80);
- 2.8.24 802.11n: 6.5 Mbps to 300 Mbps (MCS0-MCS15, VHT 20/40);
- 2.8.25 IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps;
- 2.8.26 IEEE 802.11b: 1, 2, 5.5, 11Mbps;
- 2.8.27 IEEE 802. 6, 9, 12, 18, 24, 36, 48, 54 Mbps;
- 2.8.28 Funcionalidades:
- 2.8.29 Deve possibilitar a criação de no mínimo 8 SSIDs por banda;
- 2.8.30 Deve permitir atrelar o SSID a uma Vlan (Tagged Vlan);
- 2.8.31 Deve suportar criptografia WPA-Personal/Enterprise, WPA2-Personal/Enterprise, WPA3-Personal/Enterprise;
- 2.8.32 Deve suportar 1024-QAM;
- 2.8.33 Deve suportar 4× Longer OFDM Symbol;

- 2.8.34 Deve suportar OFDMA;
- 2.8.35 Deve suportar Atribuição automática de canais;
- 2.8.36 Deve suportar QoS (WMM);
- 2.8.37 Deve implementar Seamless Roaming;
- 2.8.38 Deve implementar MU-MIMO;
- 2.8.39 Deve implementar Beamforming;
- 2.8.40 Deve implementar Airtime Fairness;
- 2.8.41 Deve implementar Band Steering;
- 2.8.42 Deve suportar Mesh;
- 2.8.43 Deve implementar Rate limit para controle de banda por SSID;
- 2.8.44 Deve implementar Load Balance para ambientes de alta densidade;
- 2.8.45 Deve implementar agendamento de reinicialização;
- 2.8.46 Deve suportar detecção de Rogue APs;
- 2.8.47 Deve implementar IEEE 802.1x;
- 2.8.48 Deve implementar Captive Portal;
- 2.8.49 Deve possibilitar a utilização de captive portal externo e autenticação via Radius;
- 2.8.50 Deve possibilitar a criação de senhas de acesso para visitantes individuais com configuração de duração de conexão através da controladora;
- 2.8.51 Deve implementar a varredura e selecionar o melhor canal de modo automático;
- 2.8.52 Deve ser fornecido controlador compatível com Access Point e todas as licenças de operação;
- 2.8.53 Deve ser possível desabilitar o Led do Access Point;
- 2.8.54 Deve suportar gerenciamento centralizado através de ferramenta de gerenciamento do próprio fabricante a fim de garantir melhor interoperabilidade e acesso aos recursos;
- 2.8.55 Certificações e requisitos:
- 2.8.56 Deve ser do mesmo fabricante da Controladora a fim de garantir a interoperabilidade;
- 2.8.57 O fabricante do produto indicado deve estar listado no relatório do Gartner – Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure, publicado em Março de 2024 - O relatório Gartner – Magic Quadrant é uma representação gráfica das atividades do mercado tecnológico em um determinado período e fornece uma relação dos agentes mais relevantes do mercado;
- 2.8.58 Deve ser homologado pela Anatel;
- 2.8.59 Deve possuir certificação Wi-Fi Alliance®
- 2.8.60 Deve possuir certificação CE e FCC;
- 2.8.61 Deve ser RoHS (Restriction of Certain Hazardous Substances) Compliance;
- 2.8.62 Deve possuir garantia de 60 meses ON-SITE pela Contratada;

- 2.8.63 A troca de equipamentos defeituosos deve ser do tipo RMA troca balcão com o prazo máximo de 30 (trinta) dias corridos;
- 2.8.64 Em caso de troca em garantia o produto reposto deverá novo e sem uso anterior, do mesmo modelo ou superior;
- 2.8.65 O produto ofertado, deverá ser novo e sem uso anterior;
- 2.8.66 Deve acompanhar o produto todos os itens para seu pleno funcionamento como Injetor PoE 48V ou IEEE 802.3at kit para montagem em poste ou parede, manuais e licenças de software;
- 2.8.67 Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste lote 02.

2.9 Transceiver Tipo I – 1 Gbps SFP SR

- 2.9.1 Deve suportar velocidade de até 1Gbps;
- 2.9.2 Deve ser do tipo SFP, para fibras multimodo;
- 2.9.3 Deve ter conector do tipo LC/UPC Duplex;
- 2.9.4 Deve ter comprimento de onda de 850nm;
- 2.9.5 Deve ser padronizado para fibra dupla;
- 2.9.6 Deve ser para distâncias de conexão de até 550 m;
- 2.9.7 Garantia de 1 (um) ano pelo fabricante;
- 2.9.8 Deve ser acompanhado de 1 (um) Cordão Óptico Duplex Multimodo LC/LC de acordo com as especificações do item 1.5 do material de cabeamento óptico;
- 2.9.9 Deve ser do mesmo fabricante dos switches deste lote 02, a fim de garantir a compatibilidade;

2.10 Transceiver Tipo II – 10 Gbps SFP+ SR

- 2.10.1 Deve ser do padrão SFP+ suportando velocidade de 10 Gbps, IEEE802.3ae;
- 2.10.2 Deve ter comprimento de onda 850nm;
- 2.10.3 Deve possuir conector do tipo LC Duplex;
- 2.10.4 Deve atender ao padrão 10GBASE-SR;
- 2.10.5 Deve ser para distâncias de conexão de até 300 m;
- 2.10.6 Deve ter suporte Hot Swappable;
- 2.10.7 Deve suportar Monitoramento de Diagnóstico Digital (DDM);
- 2.10.8 Garantia de 1 (um) ano pelo fabricante;
- 2.10.9 Deve ser acompanhado de 1 (um) Cordão Óptico Duplex Multimodo LC/LC de acordo com as especificações do item 1.5 do material de cabeamento óptico;
- 2.10.10 Deve ser do mesmo fabricante dos switches deste lote 02, a fim de garantir a compatibilidade;

2.11 Transceiver Tipo III – 10 Gbps SFP+ LR

- 2.11.1 Deve ser do padrão SFP+ suportando velocidade de 10 Gbps, IEEE802.3ae;

- 2.11.2 Deve ter comprimento de onda 1310nm;
- 2.11.3 Deve possuir conector do tipo LC Duplex;
- 2.11.4 Deve atender ao padrão 10GBASE-LR;
- 2.11.5 Deve ser para distâncias de conexão de até 10km;
- 2.11.6 Deve ter suporte Hot Swappable;
- 2.11.7 Deve suportar Monitoramento de Diagnóstico Digital (DDM);
- 2.11.8 Garantia de 1 (um) ano pelo fabricante;
- 2.11.9 Deve ser acompanhado de 1 (um) Cordão Óptico Duplex Monomodo LC/LC de acordo com as especificações do item 1.7 do material de cabeamento óptico;
- 2.11.10 Deve ser do mesmo fabricante dos switches deste lote 02, a fim de garantir a compatibilidade;

2.12 Transceiver Tipo IV – 25 Gbps SFP28 LR

- 2.12.1 Deve ser do padrão SFP28 suportando velocidade de 25 Gbps, IEEE 802.3ae e IEEE 802.3cc;
- 2.12.2 Deve ter comprimento de onda 1310nm;
- 2.12.3 Deve possuir conector do tipo LC/UPC Duplex;
- 2.12.4 Deve atender ao padrão 25GBASE-LR;
- 2.12.5 Deve ser para distâncias de conexão de até 10km;
- 2.12.6 Deve ter suporte Hot Swappable;
- 2.12.7 Deve suportar Monitoramento de Diagnóstico Digital (DDM);
- 2.12.8 Garantia de 1 (um) ano pelo fabricante;
- 2.12.9 Deve ser acompanhado de 1 (um) Cordão Óptico Duplex Monomodo LC/LC de acordo com as especificações do item 1.7 do material de cabeamento óptico;
- 2.12.10 Deve ser do mesmo fabricante dos switches deste lote 02, a fim de garantir a compatibilidade;

2.13 Cabo DAC Tipo I – 25 Gbps SFP28 1 Metro

- 2.13.1 Deve ser do padrão SFP28 suportando velocidade de 25 Gbps;
- 2.13.2 Deve possuir conector 25G SFP28 em ambos as extremidades;
- 2.13.3 Deve possuir comprimento de 1 metro;
- 2.13.4 Deve possuir condutor de cobre banhado a prata ou a ouro;
- 2.13.5 Garantia de 1 (um) ano pelo fabricante;
- 2.13.6 Deve ser do mesmo fabricante dos switches deste lote 02, a fim de garantir a compatibilidade;

2.14 Software de Gerência Centralizado

- 2.14.1 Características:
- 2.14.2 A Controladora centralizada deve ser do mesmo fabricante do Access Points, switches, gateways e de outros equipamentos compatíveis com a solução fornecida;

- 2.14.3 O fabricante do sistema de gestão indicado deve estar listado no relatório do Gartner – Magic Quadrant for Wired and Wireless LAN Access Infrastructure, publicado em março de 2024 -. O relatório Gartner – Magic Quadrant é uma representação gráfica das atividades do mercado tecnológico em um determinado período e fornece uma relação dos agentes mais relevantes do mercado;
- 2.14.4 A controladora deve ser baseada em Software do tipo Cliente/Servidor, com acesso para administração através de página Web HTTP/HTTPS;
- 2.14.5 Deve ser instalável em plataforma: Windows 7,8,10,11, Server, Ubuntu 14.04 / 16.04 / 18.04, 20.04, 22.04 (ou superior), CentOS 6.x / 7.x, Fedora 20 (ou superior) e Debian 8/9.
- 2.14.6 As licenças para pleno funcionamento do software e controle de todos os access points e de outros equipamentos quando compatíveis com a solução deverão estar inclusos;
- 2.14.7 Deverá controlar os recursos dos acess points e de outros equipamentos quando compatíveis com a solução, além de realizar o monitoramento do ambiente wireless;
- 2.14.8 Deve ser possível gerenciar os access points em uma mesma rede (L2) e em diferentes sub-redes (L3);
- 2.14.9 Deve gerenciar de forma ilimitada (sem restrição de quantitativo), simultaneamente com todas as licenças inclusas de forma vitalícia;
- 2.14.10 Deverá trabalhar em modo cluster balanceado para garantir que todos os equipamentos serão gerenciados e considerar em casos de falha de algum dos componentes do cluster que os outros conseguirão manter o ambiente em funcionamento.
- 2.14.11 Funcionalidades:
- 2.14.12 Deve conseguir gerenciar todos os equipamentos instalados na rede (Switches, Access points);
- 2.14.13 Deve possibilitar a criação de diferentes perfis (grupos) de configuração para os access points com no mínimo 100 grupos;
- 2.14.14 Deve permitir a exportação e importação de perfis (grupos) de configuração;
- 2.14.15 Deverá possuir dashboard inicial como no mínimo as seguintes informações: Tráfego da Rede Wireless, número de clientes conectados;
- 2.14.16 Deve ser possível a visualização informativa de número de access points conectados e ativos, desconectados, pendentes no qual ainda não foram gerenciados pelo sistema, número de usuários conectados, número de usuários visitantes;
- 2.14.17 Deve possuir área para upload de planta baixa para distribuição dos access points e área de cobertura. Deve ser possível o upload de arquivos do tipo jpg, jpeg, gif, png, bmp, tiff;
- 2.14.18 Deve ser possível a visualização de todos os access points com no mínimo as seguintes informações:
- 2.14.19 Nome do Access Point;
- 2.14.20 Mac Address do Access Point;
- 2.14.21 Endereço IP;
- 2.14.22 Modelo;
- 2.14.23 Versão de Hardware;
- 2.14.24 Versão de Firmware;

- 2.14.25 Canal de operação;
- 2.14.26 Número de clientes conectados;
- 2.14.27 Deve ser possível realização de Filtro para a localização do Access Point através de MAC Address, Nome, endereço IP;
- 2.14.28 Deve permitir o filtro por status: pendente, isolado, conectado, gerenciado por outros, falha na adoção e desconectado;
- 2.14.29 Deve ser possível as seguintes ações sobre o gateway:
- 2.14.30 Atualizar Firmware manualmente e online;
- 2.14.31 Realizar todas as configurações através de interface gráfica:
- 2.14.32 Redes WAN/LAN;
- 2.14.33 Controle de aplicativos por agendamento de horário;
- 2.14.34 Filtro de conteúdo por categorias;
- 2.14.35 Pesquisa segura em buscadores on-line;
- 2.14.36 Proteção contra intrusões (IDS/IPS);
- 2.14.37 Deve ser possível as seguintes ações sobre o switch:
- 2.14.38 Atualizar Firmware manualmente e online;
- 2.14.39 Configurar VLANs;
- 2.14.40 Reiniciar equipamentos em portas PoE;
- 2.14.41 Criar grupos de VLANs em cada porta;
- 2.14.42 Empilhamento nos switches que suportarem a função;
- 2.14.43 Deve ser possível as seguintes ações sobre o access point:
- 2.14.44 Atualizar Firmware manualmente e online;
- 2.14.45 Reiniciar o access point;
- 2.14.46 Mover para outro grupo (perfil) de configuração;
- 2.14.47 Deve ser possível o monitoramento e configuração dos seguintes parâmetros de modo individuais de cada access Point;
- 2.14.48 Visualizar a taxa de utilização da banda de 2.4GHz, 5GHz e 6GHz com no mínimo as seguintes informações:
- 2.14.49 Frames recebidos;
- 2.14.50 Frames enviados;
- 2.14.51 Nível de interferência;
- 2.14.52 Deve ser possível a visualização do consumo de memória, CPU e a quantos dias o equipamento está ativo;
- 2.14.53 Deve ser possível o monitoramento da interface wireless com as seguintes informações para 2.4GHz, 5GHz e 6GHz:

- 2.14.54 Modo de operação (a,b,g,n,ac, ax e be);
- 2.14.55 Canal;
- 2.14.56 Potência de transmissão;
- 2.14.57 Largura de canal;
- 2.14.58 Pacotes recebidos;
- 2.14.59 Pacotes enviados;
- 2.14.60 Bytes recebidos;
- 2.14.61 Bytes enviados;
- 2.14.62 Pacotes descartados;
- 2.14.63 Contabilização de Erros de recebimento;
- 2.14.64 Contabilização de Erros de envio;
- 2.14.65 Deve ser possível a visualização dos clientes conectados ao access point, também a visualização do MAC address do cliente, qual SSID está conectado;
- 2.14.66 Deve ser possível a visualização dos clientes do tipo visitantes conectados ao access point bem como a visualização do MAC address do cliente, qual SSID está conectado;
- 2.14.67 Deve ser possível a verificação do status da conexão MESH do dispositivo e seus uplinks wireless bem como informações como nome do Access Point conectado como uplink, canal de operação, nível de sinal;
- 2.14.68 Deve ser possível a configuração de no mínimo os seguintes parâmetros do access point:
- 2.14.69 IP Address estático ou Cliente DHCP;
- 2.14.70 Habilitar ou desabilitar de modo individual o rádio de 2.4GHz e 5GHz;
- 2.14.71 Configurar largura de Canal;
- 2.14.72 Seleção de Canal de modo manual ou automático;
- 2.14.73 Modo de operação (a, b, g, n, ac, ax e be);
- 2.14.74 Número máximo de clientes conectados em cada banda;
- 2.14.75 Limitar o nível de conexão dos clientes através de RSSI Treshold;
- 2.14.76 Detecção de Rogue APs;
- 2.14.77 Deve ser possível desconectar o Access point da controladora;
- 2.14.78 Deve ser possível a configuração de funcionalidades como:
- 2.14.79 Fast Roaming;
- 2.14.80 Airtime Fairness;
- 2.14.81 Band Steering;
- 2.14.82 Mesh;

- 2.14.83 Deve ser possível a visualização dos clientes (dispositivos) conectados com pelo menos as seguintes informações:
- 2.14.84 Hostname;
- 2.14.85 Tipo de conexão;
- 2.14.86 Endereço MAC;
- 2.14.87 Endereço IPv4;
- 2.14.88 Endereço IPv6;
- 2.14.89 Usuário 802.1x;
- 2.14.90 VLAN conectada;
- 2.14.91 Acces Point Conectado;
- 2.14.92 SSID conectado;
- 2.14.93 Banda conectada;
- 2.14.94 Taxa de Download;
- 2.14.95 Taxa de Upload;
- 2.14.96 Tempo de atividade;
- 2.14.97 Nível de sinal;
- 2.14.98 Deve ser possível a distinção entre dispositivos clientes e visitantes;
- 2.14.99 Deve ser possível tomar as seguintes ações sobre os clientes conectados:
- 2.14.100 Reconecta-lo à rede;
- 2.14.101 Restringir o acesso do cliente à rede;
- 2.14.102 Configurar limite de download e upload para o cliente;
- 2.14.103 Em caso de clientes do tipo visitante (Guest) deve ser possível cancelar sua autorização à rede;
- 2.14.104 Controle de Acesso:
- 2.14.105 Deve ser possível a criação de listas de controle de acesso baseadas em endereço IP para restrição ou liberação de determinados SSIDs;
- 2.14.106 Deve ser possível a autenticação de clientes visitantes através de:
- 2.14.107 Senha simples;
- 2.14.108 Usuários Locais criados na controladora;
- 2.14.109 Vouchers;
- 2.14.110 SMS;
- 2.14.111 Base Radius Externa;
- 2.14.112 Captive Portal externo;
- 2.14.113 Deve permitir o redirecionamento para determinada página após cliente ser autenticado;

- 2.14.114 Deve possibilitar limitação de tempo de conexão;
- 2.14.115 Deve permitir configuração da página de boas-vindas como plano de fundo e logotipo;
- 2.14.116 Deve ser possível a edição do termo de aceite;
- 2.14.117 Deve permitir no mínimo 16 entradas (Sites) sem a necessidade de autenticação dos visitantes;
- 2.14.118 Deve possui área de acesso exclusiva para operação da rede Guest (usuário visitante);
- 2.14.119 A criação de usuário visitante com as seguintes características:
- 2.14.120 Nome e senha;
- 2.14.121 Tempo de expiração do usuário;
- 2.14.122 Número máximo de dispositivos;
- 2.14.123 Nome e telefone;
- 2.14.124 Limite de download e upload;
- 2.14.125 Franquia de tráfego;
- 2.14.126 Criação de Vouchers de acesso com as seguintes características:
- 2.14.127 Tamanho do código de acesso;
- 2.14.128 Quantidade de Vouchers gerados;
- 2.14.129 Número máximo de dispositivos;
- 2.14.130 Tempo de expiração do Voucher;
- 2.14.131 Limite de download e upload;
- 2.14.132 Deve permitir o filtro de clientes através de MAC Address;
- 2.14.133 Deve implementar WMM para 2.4 e para 5GHz;
- 2.14.134 Administração:
- 2.14.135 Deve ser possível a criação de no mínimo três níveis de usuário com os seguintes níveis de acesso:
- 2.14.136 Usuário observador;
- 2.14.137 Operador com acessos limitados;
- 2.14.138 Administrador com acesso total as funções;
- 2.14.139 Deve ser possível criar agendamento para reinicialização dos access points;
- 2.14.140 A controladora deve permitir a alteração de idioma, sendo uma das opções o português;
- 2.14.141 Deve ser possível criar perfis para agendamento de operação da rede WIFI;
- 2.14.142 Deve possibilitar o Backup e restauração das configurações;
- 2.14.143 Deve possibilitar o Backup automático diário;
- 2.14.144 Em caso de gerenciamento por Software, deve permitir o gerenciamento através de plataforma Cloud acessível através de navegador ou aplicativo para smartphone;

- 2.14.145 Em caso de gerenciamento por Software, deve ser possível desabilitar caso necessário o acesso a plataforma cloud;
- 2.14.146 Deve ser possível alterar a porta de acesso HTTP e HTTPs;

2.15 Serviços de Instalação, Migração e Configuração do Lote

- 2.15.1 Os serviços deverão ser realizados em horário comercial, das 8 (oito) horas às 18 (dezoito) horas, salvo casos em que necessite parada no ambiente que demande janelas de manutenção. Neste último caso, os horários devem ser agendados com antecedência, podendo ser em período noturno (após o horário comercial) e/ou final de semana;
- 2.15.2 Deve ser realizada previamente ao início das atividades uma análise da topologia e arquitetura da rede, considerando os demais equipamentos de segurança no ambiente da CONTRATANTE;
- 2.15.3 Deve ser realizada reunião de pré-kickoff a fim de informar todas as atividades a serem desenvolvidas e alinhar as mesmas entre CONTRATADA e CONTRATANTE;
- 2.15.4 Este item considera a instalação unitária de equipamento, seja ele access point ou switch;
- 2.15.5 Toda a instalação e configurações a serem realizadas devem ser de acordo com as melhores práticas do fabricante da solução;
- 2.15.6 Deve ser considerado 5 (cinco) dias de serviço de forma “In-Loco” e/ou “Remotamente assistido” para instalação e configuração;
- 2.15.7 Este serviço deverá incluir:
- 2.15.8 Lista de cabos e interligações;
- 2.15.9 Conferência e retirada da embalagem;
- 2.15.10 Validação física dos componentes;
- 2.15.11 Instalação física dos equipamentos e interconexão dos mesmos;
- 2.15.12 Ativação dos equipamentos na rede elétrica e testes;
- 2.15.13 Criação de Template de configuração;
- 2.15.14 Criação e definição da topologia a ser usada;
- 2.15.15 Projeto de configuração dos equipamentos, contemplando todas as informações de ativação deles;
- 2.15.16 Configuração lógica dos equipamentos e softwares contratados;
- 2.15.17 Criação das VLAN´s e roteamento necessário;
- 2.15.18 Testes funcionais e eventual atualização e otimização da configuração dos equipamentos (drivers, firmwares, etc);
- 2.15.19 Integrar a solução fornecida, realizando todas as atividades necessárias ao bom funcionamento de toda a solução integrada;
- 2.15.20 Testes gerais das configurações realizadas;
- 2.15.21 Validação do ambiente como um todo;
- 2.15.22 Deverá ser entregue documentação detalhada ao final da realização dos trabalhos contendo o passo-a-passo de toda instalação e configuração dos equipamentos envolvidos no projeto;

2.16 Repasse de Conhecimento

- 2.16.1 Após a implantação/instalação dos equipamentos e softwares, a contratada deverá fornecer e/ou ministrar a transferência de conhecimento necessária para a operação dos sistemas fornecidos nas dependências da contratante, nas seguintes condições:
- 2.16.2 A transferência de conhecimento deverá ser realizada em dias úteis, no período 8:00h as 18:00h (horário local);
- 2.16.3 A carga horária para o repasse de conhecimento para toda a solução implementada deve ser de no mínimo 40h podendo ser realizada remoto ou on-site;
- 2.16.4 Documentação geral do projeto, incluindo-se todos os itens, com todas as configurações feitas;
- 2.16.5 Definição dos testes de avaliação de funcionalidade, aderência e performance da solução se necessário;
- 2.16.6 O treinamento será do tipo hands-on para repasse tecnológico dos equipamentos e softwares instalados, bem como da customização realizada no ambiente.
- 2.16.7 O corpo técnico da contratante deverá acompanhar todos os procedimentos referentes à instalação, configuração dos equipamentos e migração dos dados/serviços;

3. ESPECIFICAÇÕES TÉCNICAS DOS ITENS DE CIBERSEGURANÇA (LOTE 03)

Todos os componentes de conectividade do LOTE 03 devem ser de um único fabricante, visando assegurar a perfeita interoperabilidade e compatibilidade dos produtos entre si, bem como assegurar o desempenho da solução como um todo.

3.1 NEXT GENERATION FIREWALL (NGFW)

- 3.1.1. A solução proposta deve ser capaz de operar no modo Camada 3 (roteamento), bridge e Camada 2 (espelhamento de porta) simultaneamente (sem necessidade de virtualizar o equipamento);
- 3.1.2. A solução proposta será um Firewall NGFW de última geração e não um sistema UTM;
- 3.1.3. A solução proposta deve ter pelo menos uma porta dedicada para console e pelo menos uma porta USB;
- 3.1.4. A solução proposta deve ter pelo menos 8 portas Gigabit Ethernet, que podem ser portas de interface WAN ou LAN;
- 3.1.5. A solução proposta deve ter pelo menos 16 portas SFP, que podem ser portas de interface WAN ou LAN;
- 3.1.6. A solução proposta deve ter pelo menos 6 portas SFP+, que podem ser portas de interface WAN ou LAN;
- 3.1.7. A solução proposta deve ser capaz de usar qualquer uma das portas fixas como uma porta HA;
- 3.1.8. Estar licenciado para 10000 clientes de SSL VPN;
- 3.1.9. A solução proposta deve suportar até 16 Gbps de Threat Protection, ou seja, com funcionalides de IPS, Antivirus/Anti-Malware, Controle de Aplicação e Filtragem de URL habilitadas;
- 3.1.10. A solução proposta deve suportar 17 milhões de sessões simultâneas;
- 3.1.11. A solução proposta deve suportar 690 mil novas sessões por segundo;

- 3.1.12. A solução proposta deve ter um Throughput IPSec VPN a 28 Gbps;
- 3.1.13. A solução proposta deve suportar um Throughput AV de 28 Gbps;
- 3.1.14. A solução proposta deve suportar o IPS Throughput a 34 Gbps;
- 3.1.15. A solução proposta deve ter um espaço de armazenamento mínimo de 1.8TB SSD;
- 3.1.16. Deverá possuir fonte de alimentação redundante capaz de manter a operação total do equipamento mesmo em caso de falha de uma das fontes.
- CARACTERÍSTICAS GERAIS AO CLUSTER DE NGFW
- Serviços de rede:
- 3.1.17. Licenciamento e suporte para 60 meses;
- 3.1.18. A solução proposta deve suportar protocolos de roteamento dinâmico OSPF, BGP e RIPv2.
- 3.1.19. A solução proposta deve suportar o roteamento estático e baseado em políticas (PBR).
- 3.1.20. A solução proposta deve suportar roteamento baseado em aplicativos, a fim de rotear aplicativos como P2P, vídeo on-line, etc. com números dinâmicos de porta para o link WAN selecionado.
- 3.1.21. A solução proposta deve suportar os serviços de rede proxy DHCP, NTP, DNS Server e DNS.
- 3.1.22. A solução proposta deve suportar o roteamento ou o modo de operação NAT.
- 3.1.23. A solução proposta deve ser configurada no modo TAP.
- 3.1.24. A solução proposta deve ser compatível com o modo de operação transparente (bridge)
- 3.1.25. A solução proposta deve suportar o modo de operação misto (NAT, roteamento e bridge)
- 3.1.26. A solução proposta deve suportar os seguintes modos de interface: sniffer, port aggregation, loopback, VLANS (802.1Q e Trunking).
- 3.1.27. A solução proposta deve suportar switching e roteamento (Camada 2 e Camada 3).
- 3.1.28. A solução proposta deve suportar o recurso de switch virtual. Cada switch virtual tem sua própria tabela de endereços MAC.
- 3.1.29. A solução deverá estár no último quadrante magico do gartner para next generation firewall no quadrante de líderes ou visionarios.
- 3.1.30. A solução deverá ter a certificação técnica vigente com a icsa labs.
- 3.1.31. A solução proposta deve suportar o recurso de roteamento virtual. Cada roteador virtual tem sua própria tabela de roteamento.
- 3.1.32. A solução proposta deve suportar a duplicação de tráfego na porta configurada no dispositivo para análise de tráfego, podendo ser baseada em IP de origem, IP de destino, porta de origem, porta de destino, protocolo de rede (TCP, UDP ou ICMP), etc. O espelho da porta pode ser configurado para entrada de tráfego, tráfego de saída, ou ambos.
- 3.1.33. A solução proposta deve suportar SNAT, DNAT, PAT. Deve permitir, por política, a configuração de NAT e configuração central da tabela NAT.
- 3.1.34. A solução proposta deve suportar NAT dinâmico e NAT estático, multi-para-um, um-para-multi NAT e um-para-um NAT.

- 3.1.35. A solução proposta deve suportar NAT444 (CGNAT) e a exportação da tabela de mapeamento estático NAT444 como um arquivo.
- 3.1.36. A solução proposta deve suportar detecção de encaminhamento bidirecional (BFD), interação BFD com rota estática, OSPF ou BGP.
- 3.1.37. A solução proposta deve suportar a expansão do grupo NAT para um endereço IPv4 público para suportar mais de 64K endereços IP privados.
- 3.1.38. A solução proposta deve suportar NAT46, NAT64, DNS64.
- 3.1.39. A solução proposta deve suportar Full Cone NAT, STUN.
- 3.1.40. A solução proposta deve suportar o recurso NetFlow, o dispositivo pode coletar tráfego de entrada do usuário e enviá-lo para o servidor com a ferramenta de análise de dados NetFlow, para detectar, monitorar e coletar tráfego.
- 3.1.41. Suporte para visualização de informações de status de link de várias interfaces ao mesmo tempo para análise comparativa.
- 3.1.42. Suporte para identificar o comportamento de acesso compartilhado na rede.
- Firewall
- 3.1.43. A solução proposta deve suportar objetos de política predefinidos e personalizados. Deve suportar a junção de objetos.
- 3.1.44. A solução proposta deve suportar a política de segurança baseada em aplicativos, a função do usuário e a localização geográfica.
- 3.1.45. A solução proposta deve suportar a ALG para pelo menos os seguintes protocolos: MSRCP, PPTP, RAS, RSH, RTSP, SIP, SQLNetV2, SUNRPC, FTP, TFTP, HTTP, DNS-TCP, DNS-UDP, H. 245, H.323, Q.931, XDMCP
- 3.1.46. A solução proposta deve ser compatível com NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT, STUN.
- 3.1.47. A solução proposta deve permitir a criação de uma única política para controle de aplicativos, controle baseado no usuário, prevenção de ameaças, antivírus, filtragem de arquivos, dentro de uma única política.
- 3.1.48. A solução proposta deve suportar a verificação da redundância da política de segurança.
- 3.1.49. A solução proposta deve suportar a pesquisa de políticas na WebUI.
- 3.1.50. A solução proposta deve ser compatível com a política programada (agendamento), única ou recorrente.
- 3.1.51. A solução proposta deve ser compatível para configurar o grupo de políticas através do WebUI.
- 3.1.52. A solução proposta deve suportar o limite de sessão com base no IP de origem, IP de destino, programação, protocolo de aplicação (mysql, ms-sql, sqlnet, download P2P, vídeo, jogo, etc.) e limitar novas conexões, sessões simultâneas.
- 3.1.53. A solução proposta deve suportar defesa contra ataques de protocolos anormais.
- 3.1.54. Solução proposta deve suportar defesa contra ataques de ARP.

- 3.1.55. A solução proposta deve suportar a proteção DDoS, DNS Query Flood, SYN Flood, UDP Flood, inundações de ICMP, ping of death, smurf, WinNuke, TCP Split Handshake; a ação suportada inclui registro e reinicialização.
- 3.1.56. Deve suportar diferentes configurações para diferentes zonas de segurança.
- Sistema de Prevenção (IPS)
- 3.1.57. Ele deve suportar assinaturas personalizadas, atualizações automáticas de inserção ou extração de assinaturas e uma enciclopédia de ameaças incorporada.
- 3.1.58. A solução deve suportar proteção contra injeção SQL, ataques DC e XSS.
- 3.1.59. A solução deve suportar proteção contra ataques de C&C com limite de solicitação, limite de proxy, limite personalizado, métodos amigáveis aos rastreadores. Suporta 4 métodos de autenticação: JS Cookie, Redirecionar, Access Confirm, CAPCHA
- 3.1.60. A solução deve suportar detecção de anomalias de protocolo, detecção rate-based.
- 3.1.61. A solução deve suportar as seguintes ações de IPS: default, monitoramento, bloqueio, reset (IP do invasor ou IP da vítima, interface de entrada) com tempo de expiração.
- 3.1.62. Os perfis de segurança do IPS devem ser definidos com base na gravidade, sistema operacional, aplicativo ou protocolo.
- 3.1.63. A solução deve suportar isenção de IP de assinaturas IPS específicas.
- 3.1.64. A solução deve suportar o modo de operação de sniffer IDS.
- 3.1.65. A solução deve suportar proteção DoS rate-based para IPv4 e IPv6 com configurações de limiar contra ataques de TCP Syn Flood, TCP/UDP/SCTP port scan, ICMP sweep, e session flooding para TCP/UDP/SCIP/ICMP (fonte/destino).
- 3.1.66. A solução deve suportar a configuração predefinida de perfis IPS
- 3.1.67. A solução proposta deve suportar Reputação IP e bloqueio de IPs de servidores botnet fazendo uso de um banco de dados global de reputação de IPs.
- 3.1.68. A solução proposta deve ser compatível para filtrar assinaturas de IPS, procurando por CVE ID.
- Antivírus
- 3.1.69. A solução deve suportar o Antivírus baseado em fluxo de rede: os protocolos incluem HTTP, SMTP, POP3, IMAP, FTP/SFTP.
- 3.1.70. A solução deve suportar a detecção de vírus para arquivos compactados como RAR, ZIP, GZIP, BZIP2, TAR. Permite a detecção de arquivos compactados em várias camadas, no mínimo 5 camadas de descompressão e personaliza a ação para quando superar os comportamentos.
- 3.1.71. A solução deve suportar ações personalizadas para arquivos compactados criptografados.
- 3.1.72. A solução deve suportar pelo menos 3 ações: fill magic, reset de conexão ou apenas gerar log quando um vírus ou site malicioso for detectado.
- 3.1.73. A solução deve suportar advertência de vírus e sites maliciosos, alertando o usuário de que o site é um site malicioso ou que um vírus foi detectado.
- Filtro de URL
- 3.1.74. A solução deve suportar a inspeção de filtro da web baseado em fluxo.

- 3.1.75. A solução deve suportar filtro da Web definido manualmente com base em URL, conteúdo da Web e cabeçalho MIME.
- 3.1.76. A solução deve suportar os seguintes recursos adicionais de filtro da Web:
- - Filtro Java Applet, ActiveX e/ou cookie.
- - Bloquear o post HTTP
- - Gerar log de palavras-chave de pesquisa
- - Exceção à digitalização de conexões criptografadas em determinadas categorias para privacidade
- 3.1.77. A solução deve suportar substituir o perfil de filtro de URL, para que o administrador possa atribuir temporariamente diferentes perfis ao usuário/grupo/IP
- 3.1.78. A solução deve permitir que se personalize a página de aviso para filtro de URL
- 3.1.79. A solução deve suportar a configuração de filtro de URL com base na zona de segurança.
- Sandbox
- 3.1.80. A solução deve suportar o upload de arquivos maliciosos para a nuvem para análise.
- 3.1.81. A solução deve suportar o upload de arquivos maliciosos de protocolos que incluem HTTP/HTTPS, POP3, IMAP, SMTP e FTP.
- 3.1.82. A solução deve suportar tipos de arquivos que incluem PE, ZIP, RAR, Office, PDF, APK, JAR e SWF
- 3.1.83. A solução deve suportar o endereço de transferência de arquivos e o controle do tamanho do arquivo.
- 3.1.84. A solução deve fornecer um relatório abrangente de análise comportamental para arquivos maliciosos
- 3.1.85. A solução deve suportar resultados de detecção de bloqueio para bloquear uma ameaça desconhecida rapidamente.
- 3.1.86. A solução deve suportar o compartilhamento global de inteligência de ameaças e o bloqueio de ameaças em tempo real.
- Prevenção Botnet C&C
- 3.1.87. A solução deve efetivamente descobrir bots de intranet e evitar novos ataques avançados de ameaças, comparando as informações obtidas com o banco de dados de endereços C&C.
- 3.1.88. A solução deve suportar atualizações regulares de endereço do servidor Botnet.
- 3.1.89. A solução deve suportar dois tipos de banco de dados de endereços C&C: o banco de dados de endereços IP e o banco de dados de domínio.
- 3.1.90. A solução deve suportar a descoberta dos protocolos TCP, HTTP e DNS.
- 3.1.91. A solução deve permitir a criação de uma white list de C&C (IPs e domínio)
- Reputação IP
- 3.1.92. Suporte para filtrar o tráfego de IPs de baixa reputação, incluindo Botnet, Spam, nódulos comprometidos, força bruta, etc.

- 3.1.93. Suporte para registrar, excluir ou bloquear pacotes se o tráfego mal-intencionado atingir a lista de reputação IP.
- 3.1.94. Suporte para atualizar o banco de dados de reputação IP instalando uma licença para este fim.
- 3.1.95. Suporte para filtrar o endereço IP de bots e servidor de botnet.
- Descriptografia SSL
- 3.1.96. A solução deve suportar a identificação do aplicativo para tráfego criptografado SSL
- 3.1.97. A solução deve suportar IPS para tráfego criptografado SSL
- 3.1.98. A solução deve suportar AV para tráfego criptografado SSL
- 3.1.99. A solução deve suportar filtro de URL para tráfego criptografado SSL
- 3.1.100. A solução deve suportar o modo de download por proxy SSL.
- 3.1.101. O proxy SSL é configurado de acordo com a política e não na configuração global (depois de vincular o perfil proxy SSL a uma regra de política, o sistema processará o tráfego que corresponde à regra de acordo com a configuração do perfil).
- 3.1.102. A solução deve suportar a lista de recursos.
- Identificação e controle
- 3.1.103. A solução deve suportar a identificação de pelo menos 10 sistemas operacionais no ponto final: como Windows, IOS, Android, etc.
- 3.1.104. A solução deve suportar consultas baseadas em IP e número de pontos finais.
- 3.1.105. A solução deve suportar mais de 3.000 aplicações, deve suportar filtro de aplicativos por nome, categoria, subcategoria, tecnologia e risco.
- 3.1.106. A solução deve suportar a visualização da descrição, fatores de risco, dependências, portas típicas usadas e URLs para referências adicionais e informações para cada aplicativo no WebUI.
- 3.1.107. A solução deve suportar o bloqueio, a reinicialização, o monitoramento e a configuração de tráfego para aplicativos.
- 3.1.108. A solução deve ser capaz de identificar e controlar aplicações em nuvem, deve fornecer monitoramento multidimensional e estatísticas para aplicações em nuvem, incluindo categoria de risco e recursos.
- 3.1.109. A solução deve suportar o controle de transferência de arquivos com base no nome, tipo e tamanho do arquivo.
- 3.1.110. A solução deve suportar o controle de transferência de arquivos nos seguintes protocolos: HTTP, HTTPS, FTP, SMTP, POP3
- 3.1.111. A solução deve suportar a assinatura de arquivos e identificação de sufixo para mais de 100 tipos de arquivos
- 3.1.112. A solução deve suportar filtragem de conteúdo para protocolos HTTP-GET, HTTP-POST, FTP e SMTP.
- 3.1.113. A solução deve suportar a identificação do IM e a auditoria do comportamento da rede.
- 3.1.114. A solução deve suportar o banco de dados de usuários no local.

- 3.1.115. A solução deve suportar a autenticação do usuário com TACACS+, LDAP, Radius, Active Directory
- 3.1.116. A solução deve suportar a interação com o sistema de autenticação de terceiros através da API aberta.
- 3.1.117. A solução deve suportar autenticação de 2 fatores, seja com suporte de terceiros, servidor de token integrado e SMS
- 3.1.118. A solução deve suportar a sincronização de grupos de usuários baseados em AD e LDAP.
- 3.1.119. A solução deve suportar 802.1X, SSO Proxy
- 3.1.120. A solução deve suportar a página de autenticação da Web personalizada.
- 3.1.121. A solução deve suportar autenticação ativa baseada em interface.
- 3.1.122. A solução deve suportar um único login: Windows AD, Agentless AD SSO Role (AD Polling)
- 3.1.123. A solução deve suportar o protocolo de monitor SSO para sincronização de usuários autorizados.
- 3.1.124. A solução deve suportar o WebAuth baseado em MAC.
- QoS
- 3.1.125. A solução deve suportar o controle máximo ou garantido de largura de banda, em um endereço IP ou usuário.
- 3.1.126. A solução deve suportar o tunelamento com base no domínio de segurança, interface, endereço, usuários ou grupo de usuários, servidores ou pool, aplicativos ou pool de aplicativos, TOSs, VLANs.
- 3.1.127. A solução deve suportar largura de banda alocada por tempo, prioridade ou a mesma largura de banda compartilhada.
- 3.1.128. A solução deve suportar TOS e DiffServ.
- 3.1.129. A solução deve suportar políticas de QoS programadas.
- 3.1.130. A solução deve suportar a alocação flexível e priorizada da largura de banda restante nãousada
- 3.1.131. A solução deve suportar dois níveis de configuração de tráfego que permitem que o tráfego seja configurado em diferentes dimensões, como usuários e aplicativos. A solução deve suportar pelo menos quatro túneis por nível, fornecendo uma hierarquia de controle de tráfego.
- 3.1.132. A solução deve suportar a alocação de largura de banda com base na categoria URL
- 3.1.133. A solução deve suportar endereços IPv6 na função QoS.
- 3.1.134. O monitor iQoS suporta a exibição de tendências de tráfego em carfa, tráfego de download e tráfego total para todos os tubos ou sub-tubos (entendido como tubo para o objeto de controle de tráfego em QoS).
- Balanceamento de Servidores
- 3.1.135. A solução deve suportar o SLB (Balanceamento de Carga do Servidor)
- 3.1.136. A solução deve suportar os algoritmos SLB: Hashing ponderado, menor conexão ponderada e round-robin.

- 3.1.137. A solução deve suportar proteção de sessão, persistência de sessão e monitoramento do status da sessão.
- 3.1.138. A solução deve suportar a verificação de saúde do servidor, o monitoramento da sessão e a proteção da sessão.
- Balanceamento de Links
- 3.1.139. A solução deve suportar o balanceamento de carga LINK bidirecional (LLB)
- 3.1.140. A solução deve suportar LLBs de saída, incluindo roteamento baseado em políticas, ECMP e pesos, roteamento de ISP incorporado e detecção dinâmica da qualidade do link.
- 3.1.141. A solução deve suportar LLB de entrada, compatível com SmartDNS e detecção dinâmica de qualidade de link.
- 3.1.142. A solução deve suportar a comutação automática de link com base na largura de banda, latência, nervosismo, conectividade e aplicação.
- 3.1.143. A solução deve suportar a proteção contra sobrecarga de link, o tráfego mudará para outras ligações quando a ligação atual estiver sobrecarregada; o sistema continuará monitorando a largura de banda dos links e bloqueando novas sessões para o link que está sobrecarregado de acordo com as configurações do limiar.
- 3.1.144. A solução deve suportar a inspeção estatal de link com ARP, PING e DNS.
- VPN
- 3.1.145. A solução deve suportar os seguintes recursos de VPN IPsec:
- - Modo IPSEC Fase 1: modo de proteção agressivo e principal
- - Compatível com IKEv1 e IKEv2 (RFC 4306)
- - Método de autenticação: certificado e chave pré-compartilhada.
- - Suporte à configuração do modo IKE (como servidor ou cliente)
- - DHCP sobre IPSEC
- - Fase 1 / Fase 2 de criptografia: DES, 3DES, AES128, AES192, AES256
- - Fase de Autenticação 1 / Fase 2: MD5, SHA1, SHA256, SHA384, SHA512
- - Fase 1 / Fase 2 Suporte Diffie-Hellman: 1,2,5
- - XAuth como modo servidor e para usuários dial-up.
- - Detecção de repetição.
- - Autokey manter-se vivo para a Fase 2 SA
- 3.1.146. A solução deve suportar vpn IPSec baseada em rotas e políticas.
- 3.1.147. A solução deve suportar os seguintes modos de implantação da VPN IPSEC: gateway para gateway, malha completa, hub e spoke, túnel redundante, terminação VPN no modo transparente.
- 3.1.148. A solução deve suportar SSLVPN para Linux, iOS, Android e Windows XP/Vista/ Windows 10, incluindo sistemas operacionais Windows de 64 bits.
- 3.1.149. A solução deve suportar SSLVPN com um único login que impede logins simultâneos com o mesmo nome de usuário

- 3.1.150. A solução deve suportar o portal SSL limitando os usuários
- 3.1.151. A solução deve suportar SSL. O módulo de encaminhamento da porta VPN criptografa os dados do cliente e os envia para o servidor do aplicativo.
- 3.1.152. A solução deve suportar verificação de integridade do host e verificação do sistema operacional antes da conexão do túnel SSL.
- 3.1.153. A solução deve suportar a verificação do Portal MAC.
- 3.1.154. A solução deve suportar a opção de limpeza de cache antes de encerrar a sessão SSL VPN
- 3.1.155. A solução deve permitir vários logins SSL VPN personalizados associados a grupos de usuários (url paths, design)
- 3.1.156. A solução deve suportar autenticação SSL com uma chave USB
- 3.1.157. A solução deve suportar o modo de servidor e cliente L2TP, L2TP sobre IPSEC e GRE sobre IPSEC
- 3.1.158. A solução deve suportar o PnPVPN para implantação rápida de várias filiais de VPN local a local.
- IPv6
- 3.1.159. A solução deve suportar o gerenciamento de dispositivos sobre iPv6, registro IPv6 e HA no IPV6.
- 3.1.160. A solução deve suportar túneis IPv6, DNS64/NAT64, etc.
- 3.1.161. A solução deve suportar protocolos de roteamento IPv6 para roteamento estático, roteamento de políticas, ISIS, RIPng, OSPFv3 e BGP4+
- 3.1.162. A solução deve suportar vpn IPSec para IPv6.
- 3.1.163. A solução deve suportar IPS IPv6, identificação de aplicativos, filtragem de URL, antivírus, controle de acesso, defesa de ataque ND
- 3.1.164. A solução deve suportar o conjunto estatístico, registro e monitoramento para IPv6.
- 3.1.165. A solução deve ser suportada para configurar e bloquear endereços IPv6.
- Alta disponibilidade (HA)
- 3.1.166. A solução deve ser compatível com os modos Ativo/Ativo e/ou Ativo/Passivo
- 3.1.167. A solução deve suportar interfaces de heartbeat redundantes para HA.
- 3.1.168. A solução deve suportar a sincronização de sessão autônoma.
- 3.1.169. A solução deve suportar failover de alta disponibilidade baseado em interface, HTTP, ICMP, ARP, DNS e rastreamento de objetos baseados em TCP.
- 3.1.170. A solução deve suportar as seguintes opções de implantação do HA:
- - HA com agregação de links;
- - Full mesh HA;
- - HA geograficamente disperso.

- 3.1.171. A solução deve suportar HA no modo peer, para evitar problemas de roteamento assimétrico na implementação do modo Active-Active.
- Logs e Relatórios
- 3.1.172. A solução deve suportar a reversão do sistema operacional, ela deve suportar pelo menos duas cópias de firmware na memória flash do sistema.
- 3.1.173. A solução deve salvar dez versões do arquivo de configuração.
- 3.1.174. A solução deve suportar a exportação de configurações atuais e de backup para destinos externos, incluindo o servidor FTP, o servidor TFTP e o flash USB.
- 3.1.175. A solução deve suportar o SNMP
- 3.1.176. A solução deve ser acessível através da interface integrada do usuário web (WebUI) e da interface de linha de comando (CLI)
- 3.1.177. A solução deve suportar acesso ao gerenciamento de HTTP/HTTPS, SSH, telnet, console
- 3.1.178. A solução deve suportar pelo menos 3 funções de administrador, incluindo administrador, operador e auditor
- 3.1.179. A solução deve ser capaz de proteger o sistema contra ataques de força bruta no nome de usuário e senha
- 3.1.180. A solução deve suportar a política de segurança de senha para contas de administrador.
- 3.1.181. A solução deve suportar a implantação rápida instalando automaticamente usb, executando scripts locais e remotos.
- 3.1.182. A solução deve suportar o SYSLOG padrão e o registro de formato binário; armazenamento de log binário distribuído para vários servidores de log, algoritmo distribuído suporta Round robin, Src IP HASH
- 3.1.183. A solução deve suportar o registro em servidores de memória local ou syslog.
- 3.1.184. A solução deve suportar o registro para alterar a política de segurança.
- 3.1.185. A solução deve suportar um registro confiável usando a opção TCP (RFC 3195)
- 3.1.186. A solução deve suportar o envio de log no formato binário ou de texto.
- 3.1.187. A solução deve suportar a transferência de logs sobre UDP, TCP, protocolo Secure-TCP
- 3.1.188. A solução deve suportar pelo menos três relatórios predefinidos: relatórios de segurança, fluxo e rede.
- 3.1.189. A solução deve suportar relatórios definidos pelo usuário. O relatório pode ser exportado em PDF por e-mail ou FTP.
- 3.1.190. A solução deve suportar o RESTAPI para catálogo de endereços IP, AV, IPS, regra da política, NAT, interface, zona de segurança, roteamento, gerenciamento de atualizações
- Monitoramento
- 3.1.191. Suporta estatísticas de tráfego de aplicativos por usuário
- 3.1.192. A solução deve suportar o monitoramento de estatísticas multidimensionais para aplicativos baseados em riscos, categorias, recursos e tecnologia.

- 3.1.193. A solução deve suportar estatísticas para visita de URL e categoria URL.
- 3.1.194. Suporta estatísticas e análises de tráfego em tempo real
- 3.1.195. Estatísticas de eventos de segurança
- 3.1.196. Suporte de monitoramento definido pelo usuário
- 3.1.197. Suporte para monitorar o status do dispositivo, como CPU, memória, temperatura, etc.
- 3.1.198. Os relatórios podem ser exportados em formatos PDF, Word ou HTML.
- 3.1.199. A solução deve ter monitoramento centralizado para vários dispositivos, incluindo CPU, memória, tráfego, sessões, aplicativos, usuários, ameaças, etc. através de um aplicativo móvel, nos últimos 7 dias.
- 3.1.200. O aplicativo de monitoramento precisará suportar acesso à Web e acesso através de aplicativos em dispositivos móveis
- 3.1.201. O aplicativo de monitoramento fornecerá relatórios personalizados e agendados

3.2 SOLUÇÃO DE NDR (NETWORK DETECTION AND RESPONSE)

- 3.2.1. Entende-se por "Sistema de Detecção e Resposta de Rede (NDR)" como uma solução que primariamente usa técnicas não somente baseadas em assinaturas (Aprendizado de Máquina e Inteligência Artificial, por exemplo) que analisam comportamento de rede para detectar tráfegos suspeitos e ameaças desconhecidas (dia 0). A solução deve ser capaz de analisar e correlacionar diversos incidentes de diversos mecanismos de detecção, dar visibilidade, alarmar, indicar nível de risco e finalmente acionar fluxos de resposta à ameaça.
- 3.2.2. Não serão aceitas soluções do tipo "Next Generation Firewall (NGFW)" por mais que muitas das funcionalidades aqui descritas sejam também realizadas por esse tipo de equipamento. Os NGFWs não são classificados como NDR e geralmente são posicionados no perímetro da rede, o que não é o objetivo do objeto em questão.
- Appliance Física NDR:
- 3.2.3. A solução proposta deve ser em formato appliance.
- 3.2.4. Licenciamento e suporte para 60 meses;
- 3.2.5. O hardware deve ser do mesmo fabricante do software.
- 3.2.6. A solução proposta deve ter pelo menos 8 portas Gigabit Ethernet, 16 SFP e 6 SPF+.
- 3.2.7. A solução proposta pode ser composta de mais de 1 caixa para atendimento de todos os itens especificados na caixa NDR.
- 3.2.8. A solução proposta deve suportar a opção de adiconar 4 portas SFP+ com módulo de expansão.
- 3.2.9. A solução proposta deve suportar pelo menos 1TB SSD de espaço de armazenamento.
- 3.2.10. A solução proposta deve suportar um throughput de detecção de violação de 5 Gbps na detecção bidirecional de tráfego HTTP com todos os recursos de detecção de ameaças ativados
- 3.2.11. A solução proposta deve suportar 2.5 milhões de sessões simultâneas.
- 3.2.12. A solução proposta deve suportar 200 mil novas sessões/segundos com tráfego HTTP.
- Recursos de segurança inteligente

- 3.2.13. A solução deve ter mecanismos de análise comportamental, baseados em aprendizado de máquina, executados localmente no appliance, sem a necessidade de envio de tráfego suspeito para uma plataforma externa que possa ter a mesma capacidade de análise comportamental.
- 3.2.14. A solução deve suportar análise de correlação de ameaças, correlação de ameaças desconhecidas, comportamento anormal e comportamento de aplicações para descobrir ameaças ou ataques potenciais.
- 3.2.15. A solução deve adotar uma metodologia de classificação de ameaças segundo critérios de risco e indicadores de comprometimento, fazendo um uso estruturado de todos os mecanismos de detecção de ameaças presentes.
- 3.2.16. A solução deve permitir que o banco de dados do modelo de comportamento de malware seja atualizado online e em tempo real.
- 3.2.17. A solução deve suportar a detecção de mais de 2.000 famílias de malware conhecidas e desconhecidas, incluindo Vírus, Worms, Trojans, Overflow etc.
- 3.2.18. A solução deve suportar detecção de malware baseada em comportamento.
- 3.2.19. A solução deve ser compatível com detectar ransomware e malware de criptomineração.
- 3.2.20. A solução deve suportar modelagem de comportamento baseada amostras L3-L7 para revelar comportamento de rede anômalo, como varredura HTTP, Spider, SPAM, senha fraca de SSH/FTP para o servidor e o host.
- 3.2.21. A solução deve suportar a detecção de DDoS, incluindo Flooding, Sockstress, Zip of Death, Reflect, DNS Query, DDoS SSL e DDoS de aplicação.
- 3.2.22. A solução deve suportar a inspeção do tráfego de túneis criptografados para aplicações desconhecidos.
- 3.2.23. A solução deve suportar a atualização do banco de dados de modelos de comportamento anormal online em tempo real.
- 3.2.24. A solução deve fornecer análise forense, incluindo análise de ameaças, base de conhecimento, histórico de ameaças e topologia.
- 3.2.25. A solução deve suportar ações do administrador para alterar o status de ameaça, aberto, falso positivo, fixo, ignorar, eventos confirmados
- 3.2.26. A solução deve suportar a limpeza com um clique das ameaças de servidor/PCs e reavaliação da segurança do host.
- 3.2.27. A solução deve suportar lista de permissão de eventos de ameaça, incluindo nome da ameaça, IP de origem/destino, contagem de acertos etc.
- 3.2.28. A solução deve suportar a captura online de pacotes.
- 3.2.29. A solução deve suportar a tecnologia local honeypot para capturar ataques de ameaças de rede e confirmar a origem da ameaça, tipo de ameaça e incidência.
- 3.2.30. A solução deve suportar armadilhas (honeypot) locais para interceptar ataques de ameaças à rede e confirmar a origem da ameaça, o tipo de ameaça e a incidência.
- a. Caso a solução não possua nativamente capacidade de honeypot, poderá incluir solução adicional, desde que não seja software livre e com seu respectivo suporte durante todo o contrato e que possua integração total com a solução principal.

- 3.2.31. A solução deve suportar o recurso de busca de ameaças para coletar evidências extensas e fornecer análises aprofundadas.
- 3.2.32. A solução deve suportar o registro de eventos de ameaças, com Indicadores de Comprometimento, para rastreamento de ameaças, como força bruta de desktop remoto, criação de arquivos suspeitos, processos maliciosos de powershell etc., para melhorar a capacidade de detecção do recurso de rastreamento de ameaças e diminuir falso-positivos.
- Visibilidade de risco/ameaça
- 3.2.33. A solução deve suportar a exibição de ameaças de intranet para os servidores (ativos críticos), bem como a detecção de tráfego anormal relacionado a eles.
- 3.2.34. A solução deve suportar a visibilidade de ameaças para hosts de risco, incluindo nome do host, SO, navegador, tipo de serviço para registrar ameaças de host e tráfego anormal.
- 3.2.35. A solução deve suportar visibilidade para informações básicas com base no host, índice de risco, ameaças e tráfego anormal.
- 3.2.36. A solução deve suportar visibilidade de ameaças, incluindo nome de ameaça, tipo de ameaça, nível de risco, base de conhecimento, pacote forense e assim por diante.
- 3.2.37. A solução deve fornecer todas as estatísticas de ranking de eventos de ameaça com base em indicadores de compromisso e na tendência de eventos de ameaça em pelo menos duas semanas.
- 3.2.38. A solução deve suportar mostrar o caminho do ataque de forma gráfica, facilitando o trabalho dos administradores.
- Serviços de rede
- 3.2.39. A solução proposta deve suportar o modo de operação com espelhamento de porta, sem ser intrusiva à rede do cliente.
- 3.2.40. A solução deve ser capaz de se integrar com firewalls da mesma marca, a fim de mitigar ameaças.
- 3.2.41. A Integração com o firewall deve ser possível a criação de regras de maneira automática de bloqueio de IP's permitindo o operador criar uma lista de exceções.
- Controle de aplicativos
- 3.2.42. A solução deve suportar mais de 3,500 aplicações que devem ser filtradas por nome, categoria, subcategoria, tecnologia e risco.
- 3.2.43. A solução deve ser capaz de identificar aplicativos móveis do tipo iOS ou Android.
- 3.2.44. A solução deve ser capaz de identificar aplicações em nuvem e fornecer monitoramento e estatísticas multidimensionais para aplicações em nuvem, incluindo categoria de risco e recursos.
- Detecção de intrusão
- 3.2.45. A solução deve suportar pelo menos 8 mil assinaturas. Deve suportar assinaturas personalizadas, atualizações manuais de inserção ou extração de assinaturas automáticas e uma enciclopédia de ameaças incorporada.
- 3.2.46. A solução deve suportar proteção de ataque contra C&C com limite de solicitação, limite de proxy, limiar personalizado. Deve suportar pelo menos 4 métodos de autenticação: JS Cookie, Redirecionar, Access Confirm, CAPCHA

- 3.2.47. A solução deve suportar detecção de anomalias de protocolo, detecção baseada em rate, incluindo os protocolos HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS, etc.
- 3.2.48. A solução deve permitir que se crie listas de permissão para o módulo IPS.
- 3.2.49. A solução deve ter perfis IPS predefinidos.
- 3.2.50. A solução deve ter a opção de captura de pacotes.
- Antivírus
- 3.2.51. A solução deve suportar pelo menos 10 milhões de assinaturas antivírus, com atualizações manuais ou automáticas de assinatura.
- 3.2.52. A solução deve ser compatível com o Flow Based Antivirus: os protocolos incluem HTTP, SMTP, POP3, IMAP, FTP/SFTP.
- 3.2.53. A solução deve suportar a detecção de vírus para arquivos compactados como RAR, ZIP, GZIP, BZIP2, TAR.
- 3.2.54. A solução deve suportar a detecção de arquivos compactados criptografados.
- C&C Botnet Prevention
- 3.2.55. A solução deve suportar a descoberta eficaz de bots de intranet e a prevenção de novos ataques avançados de ameaças, comparando as informações obtidas com o banco de dados de endereços C&C.
- 3.2.56. A solução deve suportar a atualização automática da biblioteca de assinatura de defesa Botnet/C&C.
- 3.2.57. A solução deve suportar dois tipos de banco de dados de endereços C&C: o banco de dados de endereços IP e o banco de dados de domínio.
- 3.2.58. A solução deve suportar a detecção dos protocolos TCP, HTTP e DNS.
- Defesa de Ataque
- 3.2.59. A solução deve suportar a detecção do DoS/DDoS, SYN Flood, DNS Query Flood, etc.
- 3.2.60. A solução deve suportar a detecção de ataques ARP.
- 3.2.61. A solução deve suportar a detecção de ataques de protocolo anormais.
- Inteligência de Ameaças
- 3.2.62. A solução deve suportar o envio em tempo real das informações de ameaça mais graves encontradas na indústria para o dispositivo a partir da nuvem.
- 3.2.63. Deve suportar o registro e verificação se uma ameaça correspondente ocorreu na rede.
- 3.2.64. Deve suportar fornecer informações detalhadas sobre ameaças e sugestões de soluções.
- Sandbox em nuvem
- 3.2.65. A solução deve ser compatível com o ambiente de execução virtual de malware, baseado em nuvem para encontrar ameaças desconhecidas.
- 3.2.66. A solução deve suportar o upload de arquivos maliciosos para sandbox na nuvem para análise.
- 3.2.67. A solução deve suportar o upload de arquivos maliciosos de protocolos incluindo HTTP/HTTPS, POP3, IMAP4, SMTP eFTP.

- 3.2.68. A solução deve suportar tipos de arquivos, incluindo PE, ZIP, RAR, Office, PDF, APK, JAR e SWF.
- 3.2.69. A solução deve fornecer um relatório completo de análise comportamental para arquivos maliciosos.
- 3.2.70. A solução deve suportar o compartilhamento global de inteligência de ameaças, para detectar a nova ameaça desconhecida.
- Anti-Spam
- 3.2.71. A solução deve suportar classificação e detecção de spam em tempo real
- 3.2.72. A solução deve suportar Spam Confirmado, Spam Massivo, Spam Suspeito, Bulk Válido.
- 3.2.73. A solução deve suportar a detecção, independentemente do idioma, formato ou conteúdo da mensagem.
- 3.2.74. a solução deve suportar os protocolos de e-mail SMTP e POP3
- 3.2.75. A solução deve suportar lista de permissão para e-mails de domínios confiáveis.
- Administração
- 3.2.76. A solução deve ter uma interface web user integrada (WebUI) e interface de linha de comando (CLI).
- 3.2.77. A solução deve suportar acesso ao gerenciamento de HTTP/HTTPS, SSH, Telnet, console.
- 3.2.78. A solução deve ser capaz de proteger o sistema contra-ataques de força bruta no nome de usuário e senha.
- 3.2.79. A solução deve suportar a política de segurança de senha para contas de administrador.
- 3.2.80. A solução deve suportar o monitoramento do servidor e do host da rede interna, identificando o nome, sistema operacional, navegador, tipo e registro estatístico de ameaças de rede.
- Registros e Relatórios
- 3.2.81. A solução deve suportar relatórios definidos pelo usuário. O relatório pode ser exportado pelo menos em formato PDF e/ou enviado para um endereço e-mail ou FTP.
- 3.2.82. A solução deve suportar alarmes de configuração para utilização da CPU, utilização de memória, utilização do espaço em disco, novas conexões ou afins.
- 3.2.83. A solução deve suportar o envio de alarmes por e-mail, SMS.
- 3.2.84. Deve suportar alertas baseados na largura de banda da aplicação e novas conexões.
- 3.2.85. Deve suportar alertas de e-mail e mensagens de texto.
- 3.2.86. Deve suportar logs, incluindo logs para eventos, redes, ameaças, configuração e sessões.
- 3.2.87. Deve suportar SYSLOG padrão e log de formato binário. Suportar armazenamento distribuído de logs binários em vários servidores de log, algoritmo distribuído suporta Round Robin, Src IPHASH.
- 3.2.88. Os logs podem ser exportados via syslog ou e-mail.
- 3.2.89. Deve suportar pelo menos três tarefas de relatórios predefinidas: ameaça, operação de tráfego e sistema, além de relatórios definidos pelo usuário.
- 3.2.90. A solução deve suportar o relatório de ameaças para os PCs/servidores.

3.3 SOLUÇÃO DE EXTENDED DETECTION AND RESPONSE (XDR)

- 3.3.1. Suporta coleta de dados, incluindo netflow, metadados, Syslog, Sysmon, Linux Syslog de dispositivos de segurança;
- 3.3.2. Licenciamento e suporte para 60 meses;
- 3.3.3. Suporta integração de dispositivos de terceiros para coleta de dados;
- 3.3.4. Suporta rastreamento de eventos de ameaças e visualização de ativos de risco e tendências de risco;
- 3.3.5. Suporta visualização distribuída de conexões geográficas de ameaças;
- 3.3.6. Suporta exibição em tela cheia de informações detalhadas e estatísticas para segurança geral, segurança de servidor, segurança de endpoint, vulnerabilidades, segurança de área e eventos de ameaças;
- 3.3.7. Suporta a configuração de regras de detecção de ameaças para verificação, arquivamento, detecção HTTP, protocolos suspeitos, força bruta, DNS, chantagem, mineração, comportamento USB, violação de acesso, senha fraca e ameaças definidas pelo usuário;
- 3.3.8. Detecção de ameaças baseada em regras;
- 3.3.9. Análise de registro de ameaças;
- 3.3.10. análise do comportamento;
- 3.3.11. Análise de correlação;
- 3.3.12. Estatísticas e análises de servidores de risco, terminais de risco e eventos de ameaças;
- 3.3.13. Suporte na coleta de evidências, processamento e marcação de status de eventos de ameaça;
- 3.3.14. Suporte para o gerenciamento de ativos de servidor, ativos de terminal e ativos não classificados;
- 3.3.15. Suporte ao gerenciamento de cluster de servidor, terminal e diferentes tipos de negócios de servidor;
- 3.3.16. Suporta descoberta automática de ativos;
- 3.3.17. Suporta exibição de status do usuário;
- 3.3.18. Suporta informações estatísticas e detalhadas sobre vulnerabilidades;
- 3.3.19. Suporta importação de relatórios de vulnerabilidade de terceiros;
- 3.3.20. Suporte para integração com scanners de terceiros
- 3.3.21. Suporte para gerenciamento de tarefas de digitalização;
- 3.3.22. Notificação de Informações sobre Ameaças CVE;
- 3.3.23. Suporte para o banco de dados de inteligência de domínios DNS, códigos maliciosos, IP, vulnerabilidades, detecções de intrusão e geolocalização;
- 3.3.24. Suporte a atualização offline e online do banco de dados de inteligência manualmente e periodicamente;
- 3.3.25. Suporta listas de permissões globais, DNS e de arquivos;
- 3.3.26. Suporta DNS, código malicioso e listas negras de IP;;

- 3.3.27. Suporta análise de correlação de big data e detecção de killchain
- 3.3.28. Suporta pesquisa centralizada e classificada para eventos de ameaças globais;
- 3.3.29. Suporte para pesquisa por palavras-chave, SPL e condições predefinidas;
- 3.3.30. Suporte ao sistema de gerenciamento de casos;
- 3.3.31. Atualização e revisão do status do caso;
- 3.3.32. Dispositivos/serviços interativos (dispositivos de segurança/serviço de inteligência de ameaças);
- 3.3.33. Suporta integração de dispositivos de terceiros via API RESTful ou SSH;
- 3.3.34. Deverá possuir capacidade de criação de playbooks para SOAR, com playbooks pré-definidos e capacidade de criação de playbooks customizados através da interface gráfica.
- o A funcionalidade de Playbook/SOAR, deverá ainda permitir que estes playbooks sejam utilizados para automação de respostas aos incidentes conforme configuração de gatilhos (triggers).
- o Essas triggers a serem usadas, podem ser eventos/características de ameaças, consulta de inteligência de ameaças, condições de julgamento para resposta automática e ações de processamento de resposta (políticas de emissão, bloqueio de IP ou criação de ordens de serviço), de modo a realizar resposta automática no firewall ou outro dispositivo.
- o Caso a solução não possua nativamente capacidade de criação e uso de playbooks (SOAR), poderá incluir solução adicional, desde que não seja software livre e com seu respectivo suporte durante todo o contrato e que possua integração total com a solução principal.
- 3.3.35. Suportar alarmes baseados em regras de limite e regras de pulso de tráfego;
- 3.3.36. Visualização em tempo real de eventos de ameaças;
- 3.3.37. Suporta notificação de alerta por SMS, e-mail e WebUI;
- 3.3.38. Suporta quatro modelos de relatório: Risco de segurança geral, Risco de segurança de endpoint, Risco de segurança do servidor e Relatório de resposta a incidentes;
- 3.3.39. Suporta a função opcional da tarefa de relatório;
- 3.3.40. Suporte a relatórios periódicos ou sob demanda;
- 3.3.41. Suporte a visualização de eventos “on-line”;
- 3.3.42. Suporte a exportação de relatórios em formato PDF/WORD;
- 3.3.43. Suporte a notificação por e-mail de geração de relatórios;
- 3.3.44. Suporte para gerenciamento de proteção classificada;
- 3.3.45. Suporte ao gerenciamento de autoridade do usuário, Syslog, Netflow, armazenamento de log, informações de teste, configuração de rede, configuração de correio e configuração de licença;
- 3.3.46. Suporta configuração de hosts confiáveis;
- 3.3.47. Suporte de integração com console de gerenciamento centralizado;
- 3.3.48. Logs do sistema de registro;
- 3.3.49. Sincronização com regras de NDR;

- 3.3.50. Compativel com Linux: CentOS 7, Windows: Microsoft Windows 10 e VMware: VMware EXSi 6.7;
- 3.3.51. Deve permitir a seguinte configuração de hardware para a máquina virtual suportando, no mínimo:
- o 15 (quinze) Gbps de throughput de tráfego;
- o 15000 (quinze mil) eventos por segundo (EPS).
- 3.3.52. Caso seja licenciado por dispositivos, deverá estar licenciado para 10000 (dez mil) dispositivos.

3.4 SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DO NDR, XDR e NGFW

- 3.4.1. Todas as fases de planejamento, instalação, configuração e validação deverão ser realizadas com a presença de técnicos da CONTRATADA, os quais deverão possuir capacidade técnica compatível com a complexidade da solução e experiência comprovada na execução dos serviços.
- 3.4.2. Os serviços deverão ser realizados, preferencialmente, em horário comercial, das 08 (oito) horas às 18 (dezoito) horas, salvo nos casos em que haja necessidade de parada no ambiente que demande janelas de manutenção.
- Nesses casos, as atividades deverão ser previamente acordadas com a CONTRATANTE, podendo ser executadas em período noturno, finais de semana ou feriados.
- 3.4.3. Deverá ser realizada, previamente ao início das atividades, análise detalhada da topologia e arquitetura da rede da CONTRATANTE, considerando todos os equipamentos e soluções de segurança existentes no ambiente.
- 3.4.4. Todas as instalações e configurações deverão ser realizadas em conformidade com as melhores práticas recomendadas pelo fabricante da solução, bem como boas práticas de mercado.
- 3.4.5. A CONTRATADA deverá realizar planejamento prévio das atividades de instalação, considerando:
- 3.4.6. Minimização de impactos ao ambiente produtivo;
- 3.4.7. Continuidade dos serviços;
- 3.4.8. Definição de janelas de manutenção, quando necessário;
- 3.4.9. Qualquer atividade que implique interrupção de serviços deverá ser previamente negociada e autorizada pela CONTRATANTE.
- 3.4.10. Deverá ser considerado um pacote estimado de até 80 (oitenta) horas de serviço, podendo ser executado de forma presencial (on-site) e/ou remota assistida, para fins de instalação, configuração e implantação da solução.
- 3.4.11. Os serviços de implantação deverão incluir, mas não se limitar a:
- 3.4.12. Planejamento e Projeto
- 3.4.13. Projeto de configuração dos equipamentos, contemplando todas as informações necessárias à ativação;
- 3.4.14. Criação de templates de configuração;
- 3.4.15. Atividades Físicas
- 3.4.16. Conferência e retirada de embalagens;

- 3.4.17. Validação física dos equipamentos e componentes;
- 3.4.18. Organização do rack para implantação;
- 3.4.19. Instalação física dos equipamentos;
- 3.4.20. Elaboração de lista de cabos e interligações;
- 3.4.21. Implantação e Integração
- 3.4.22. Conexão dos equipamentos à rede da CONTRATANTE;
- 3.4.23. Interligação dos equipamentos à infraestrutura existente;
- 3.4.24. Configuração lógica dos equipamentos;
- 3.4.25. Integração completa com o ambiente de rede e segurança;
- 3.4.26. Configuração da Solução
- 3.4.27. Configuração de ambiente de alta disponibilidade (HA), quando aplicável;
- 3.4.28. Ativação de todas as licenças contratadas;
- 3.4.29. Configuração de alertas, eventos e ações;
- 3.4.30. Instalação e configuração de softwares da solução;
- 3.4.31. Aplicação de atualizações (firmware, patches e drivers);
- 3.4.32. Migração e Ajustes
- 3.4.33. Migração de VLANs do ambiente existente, quando aplicável;
- 3.4.34. Migração de regras e políticas pré-existentes, mediante solicitação da CONTRATANTE;
- 3.4.35. Otimização de configurações de segurança;
- 3.4.36. Testes e Validação
- 3.4.37. Ativação dos equipamentos na rede elétrica e lógica;
- 3.4.38. Execução de testes funcionais e operacionais;
- 3.4.39. Ajustes e otimizações após testes;
- 3.4.40. Monitoramento e Logs
- 3.4.41. Configuração e apresentação das funcionalidades de gerenciamento e análise de logs;
- 3.4.42. Validação do correto funcionamento dos mecanismos de monitoramento;
- 3.4.43. A CONTRATADA deverá realizar a integração completa da solução fornecida, executando todas as atividades necessárias para garantir o pleno funcionamento do ambiente integrado.
- 3.4.44. Deverá ser ministrado treinamento do tipo repasse de conhecimento, com carga horária mínima de:
- 3.4.45. 20 (vinte) horas para operação completa da solução;
- 3.4.46. O treinamento deverá contemplar operação, administração, boas práticas e troubleshooting.
- 3.4.47. Ao final da execução dos serviços, a CONTRATADA deverá entregar documentação técnica detalhada, contendo, no mínimo:

- 3.4.48. Arquitetura da solução implantada;
- 3.4.49. Configurações realizadas;
- 3.4.50. Templates utilizados;
- 3.4.51. Procedimentos operacionais;
- 3.4.52. Passo a passo da instalação e configuração;
- 3.4.53. Recomendações de boas práticas;

3.5 SERVIÇOS DE GARANTIA, ASSISTÊNCIA TÉCNICA E SUPORTE TÉCNICO PELO PERÍODO DE 60 (Sessenta) MESES PARA OS EQUIPAMENTOS NDR, XDR E NGFW

- 3.5.1. Os equipamentos fornecidos deverão estar cobertos por garantia que ofereça substituição decorrente de vícios de projeto, fabricação, construção e montagem, pelo período mínimo de 60 (sessenta) meses, a contar da data de sua efetiva instalação.
- 3.5.2. Os itens adquiridos nesse processo deverão possuir garantia do com validade mínima de 60 (sessenta) meses, contados a partir do recebimento definitivo da solução.
- 3.5.3. A assistência técnica de suporte e licenças dos equipamentos e suas funcionalidades contratadas é por um prazo mínimo de 60 (sessenta) meses, a contar da data de sua efetiva ativação englobando todos os componentes do objeto deste edital, incluindo configuração técnica do produto.
- 3.5.4. Deve estar identificado de forma clara na proposta os números identificadores de produtos (part numbers) do fabricante referentes as garantias fornecidas.
- 3.5.5. Os softwares fornecidos deverão estar cobertos por garantia que ofereça atualizações necessárias para a correção de vícios, pelo período especificado no termo de referência, a contar da data do aceite da implementação da solução.
- 3.5.6. Deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correções.
- 3.5.7. Deve ser possível realizar a atualização das assinaturas de proteção da solução, se necessárias.
- 3.5.8. Permitir realizar consultas técnicas ou questionamentos da equipe da CONTRATANTE para sanar dúvidas, repassar conhecimentos, ou ainda obter melhores práticas.
- 3.5.9. As garantias devem prever a reposição de peças e equipamentos. Essa reposição deverá abranger todos os itens que compõem a solução, incluindo módulos ou outros equipamentos fornecidos para atendimento aos requisitos da aquisição
- 3.5.10. Deve ter sistema de atendimento a chamados 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano (modalidade de 24 x 7), com sistema para abertura de chamados de suporte técnico.
- 3.5.11. Os serviços de garantia e de assistência técnica deverão ser prestados por técnicos devidamente habilitados e credenciados pelo fabricante, com nível de certificação compatível com as atividades a serem executadas, e sem qualquer ônus adicional.
- 3.5.12. Dado natureza de redundância 100% dos equipamentos a troca de um equipamento inoperante ou com falha em que o sintoma seja de parado, o atendimento será em 4 horas com troca do mesmo em 7 dias caso necessário.

- 3.5.13. As garantias devem incluir envio de peças e ou equipamentos de reposição, que deverão ser entregues nos locais especificados neste termo de referência, abrangendo-se todos os custos de deslocamento (envio e retorno) das peças e equipamentos de substituição.
- 3.5.14. O serviço de substituição de peças e equipamentos deve ser realizado de forma presencial nas instalações CONTRATANTE.
- 3.5.15. Caso não for possível recuperar o equipamento em até 72 horas após a abertura do chamado, o equipamento (hardware) com problema deverá ser substituído por outro de igual capacidade e capaz de atender as mesmas funcionalidades do adquirido.
- 3.5.16. Disponibilizar todas as atualizações dos softwares e firmwares dos equipamentos, concebidas em data posterior ao seu fornecimento, pelo período mínimo de 60 (sessenta) meses, sem qualquer ônus adicional a Prefeitura de Colombo.
- 3.5.17. Disponibilizar estrutura de suporte técnico por meio de atendimento telefônico, website e e-mail. As ligações telefônicas de atendimento não geram custos adicionais a CONTRATANTE.
- 3.5.18. Todo o chamado aberto deve ter sua resolução técnica registrada no sistema de atendimento do fornecedor da solução.
- 3.5.19. A equipe técnica de sustentação da CONTRATANTE poderá abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico, mediante identificação de acesso ao sistema de registro de chamados do fornecedor da solução.
- 3.5.20. Os chamados devem ser atendidos no idioma português, mesmo quando em ligações telefônicas, website ou e-mail.

3.6 SERVIÇO DE SOC (SECURITY OPERATIONS CENTER)

- 3.6.1. O Serviço de SOC deverá ser executado por um período de 60 (sessenta) meses, em regime de Monitoramento contínuo (24x7), com início de resposta após identificação de incidente em até 1h e contenção inicial do evento crítico em até 2 horas;
- 3.6.2. As estruturas de operação de suporte poderão ser prestadas a partir das instalações da CONTRATADA de forma remota;
- 3.6.3. Em casos de incidentes que necessitarem de deslocamento dos agentes da contratada ocorrerão às custas da CONTRATADA, sem a possibilidade de reembolsos;
- 3.6.4. Serviço de SOC para Firewall de Próxima Geração (Next Generation Firewall - NGFW)
- 3.6.5. A CONTRATADA deverá fazer uso da solução que a CONTRATANTE fornecer como ferramenta de Serviço de Firewall de Próxima Geração durante a vigência do contrato para prestação do serviço;
- 3.6.6. A CONTRATADA deverá realizar as seguintes operações de monitoração da solução de Gerência do Serviço de Firewall de Próxima Geração, utilizando o modelo ITIL como referência, incluindo, mas não se limitando:
- 3.6.7. Serviço de VPN (com funcionalidade SSL, IPsec e outras tecnologias compatíveis);
- 3.6.8. Serviço de IDS/IPS (Sistemas de Detecção e Prevenção de Intrusão);
- 3.6.9. Serviço de controle de aplicações;
- 3.6.10. Serviço de filtro de conteúdo WEB;
- 3.6.11. Serviço de inspeção SSL/TLS;

- 3.6.12. Serviço de filtro de DNS;
- 3.6.13. A CONTRATADA deverá realizar as seguintes operações referentes à segurança quanto à monitoração da solução de Firewall, incluindo, mas não se limitando:
- 3.6.14. Análise de logs e eventos de segurança;
- 3.6.15. Detecção de ameaças e comportamentos anômalos;
- 3.6.16. Gestão de políticas de segurança;
- 3.6.17. Ajustes e otimização de regras de firewall;
- 3.6.18. A CONTRATADA entregará relatório mensal específico para este serviço, contendo análise de eventos, incidentes, performance e recomendações;
- 3.6.19. No Período de Transição Operacional, a CONTRATADA deverá realizar análise completa da solução de NGFW utilizada pela CONTRATANTE e recomendar melhorias, incluindo, mas não se limitando:
- 3.6.20. Revisão de políticas de segurança;
- 3.6.21. Segmentação de rede;
- 3.6.22. Regras de acesso;
- 3.6.23. Configurações de VPN;
- 3.6.24. Estratégias de proteção contra ameaças;
- 3.6.25. Após aprovação da CONTRATANTE, o serviço gerenciado deverá implementar as melhorias propostas.
- 3.6.26. Serviço de SOC para Detecção e Resposta de Rede (Network Detection and Response - NDR)
- 3.6.27. A CONTRATADA deverá fazer uso da solução que a CONTRATANTE fornecer como ferramenta de Detecção e Resposta de Rede durante a vigência do contrato;
- 3.6.28. A CONTRATADA deverá realizar as seguintes operações de monitoração da solução NDR, incluindo, mas não se limitando:
- 3.6.29. Análise contínua de tráfego de rede (north-south e east-west);
- 3.6.30. Detecção de comportamentos anômalos;
- 3.6.31. Identificação de movimentação lateral;
- 3.6.32. Identificação de exfiltração de dados;
- 3.6.33. Análise de fluxos de rede e metadados;
- 3.6.34. A CONTRATADA deverá realizar as seguintes atividades operacionais:
- 3.6.35. Investigação de incidentes baseados em tráfego de rede;
- 3.6.36. Classificação de riscos de rede;
- 3.6.37. Geração de alertas e incidentes de segurança;
- 3.6.38. Integração com NGFW e XDR;
- 3.6.39. Os comportamentos anômalos detectados deverão ser:

- 3.6.40. Transformados em incidentes de segurança; ou
- 3.6.41. Registrados para análise e melhoria contínua;
- 3.6.42. A CONTRATADA deverá prover inteligência de ameaças, incluindo:
- 3.6.43. Pesquisa de novos ataques;
- 3.6.44. Atualização de mecanismos de detecção;
- 3.6.45. Criação de regras de identificação de ameaças;
- 3.6.46. A CONTRATADA entregará relatório mensal específico contendo análise de tráfego, incidentes e recomendações;
- 3.6.47. No Período de Transição Operacional, a CONTRATADA deverá:
- 3.6.48. Revisar configurações da solução;
- 3.6.49. Classificar riscos da rede;
- 3.6.50. Propor melhorias de visibilidade e detecção;
- 3.6.51. Após aprovação da CONTRATANTE, as melhorias deverão ser implementadas.
- 3.6.52. Serviço de SOC para Extended Detection and Response (XDR)
- 3.6.53. A CONTRATADA deverá fazer uso da solução que a CONTRATANTE fornecer como ferramenta de Extended Detection and Response (XDR) durante a vigência do contrato;
- 3.6.54. A CONTRATADA deverá realizar as seguintes operações de administração, gerenciamento e monitoração da solução XDR, incluindo, mas não se limitando:
- 3.6.55. Correlação de eventos de múltiplas fontes (NGFW, NDR, endpoints, servidores);
- 3.6.56. Análise de eventos e geração de alertas;
- 3.6.57. Detecção de ameaças baseada em comportamento e assinaturas;
- 3.6.58. A CONTRATADA deverá executar:
- 3.6.59. Criação e manutenção de regras de detecção;
- 3.6.60. Criação de casos de uso;
- 3.6.61. Automação de resposta a incidentes (playbooks);
- 3.6.62. Integração entre ferramentas de segurança;
- 3.6.63. A CONTRATADA deverá realizar atividades de resposta, incluindo:
- 3.6.64. Contenção de incidentes;
- 3.6.65. Isolamento de ativos comprometidos;
- 3.6.66. Bloqueio de ameaças;
- 3.6.67. A CONTRATADA deverá administrar a plataforma, incluindo:
- 3.6.68. Configuração e manutenção;
- 3.6.69. Gerenciamento de conectores;
- 3.6.70. Inclusão e remoção de ativos;

- 3.6.71. Atualizações e suporte;
- 3.6.72. A CONTRATADA deverá realizar investigação de incidentes, incluindo:
- 3.6.73. Análise de causa raiz;
- 3.6.74. Mapeamento de ataques com base no MITRE ATT&CK;
- 3.6.75. Identificação de vetores de ataque;
- 3.6.76. A CONTRATADA entregará relatório mensal específico contendo:
- 3.6.77. Eventos correlacionados;
- 3.6.78. Incidentes detectados;
- 3.6.79. Tempo de resposta;
- 3.6.80. Recomendações;
- 3.6.81. No Período de Transição Operacional, a CONTRATADA deverá:
- 3.6.82. Revisar regras de correlação;
- 3.6.83. Avaliar integrações;
- 3.6.84. Propor melhorias na detecção e resposta;
- 3.6.85. Após aprovação da CONTRATANTE, a CONTRATADA deverá implementar as melhorias propostas;
- 3.6.86. Todas as regras, automações e configurações implementadas deverão permanecer na solução da CONTRATANTE ao final do contrato.