GOVERNO DO ESTADO DE RONDÔNIA
Secretaria de Estado da Saúde - SESAU

TERMO DE REFERÊNCIA

1. IDENTIFICAÇÃO

1.1. **Unidade Orçamentária:** Secretaria de Estado da Saúde de Rondônia - SESAU/RO.

1.2. **Requisitante**: Coordenadoria de Inovação e Tecnologia da Informação - CITI

2. DA INTRODUÇÃO E BASE LEGAL

2.1. O presente Termo de Referência foi elaborado em atendimento ao disposto no art. 6º, XXIII da Lei nº 14.133, de 2021. O fundamento legal adotado para a presente contratação é Pregão Eletrônico - Registro de Preço, conforme artigo 28, inciso I da **Lei Federal nº 14.133/2021**, adotado para a presente contratação conformidade com regulamento das contratações públicas no âmbito da Administração Pública direta, autárquica e fundacional do Estado de Rondônia aplicado no **Decreto Estadual n° 28.874/2024.**

2.2. Dos Princípios a serem observados: conforme art. 5º da Lei 14.133/2021, eis os princípios a serem observados na sua aplicação:

> Art. 5º Na aplicação desta Lei, serão observados os princípios da legalidade, da impessoalidade, da moralidade, da publicidade, da eficiência, do interesse público, da probidade administrativa, da igualdade, do planejamento, da transparência, da eficácia, da segregação de funções, da motivação, da vinculação ao edital, do julgamento objetivo, da segurança jurídica, da razoabilidade, da competitividade, da proporcionalidade, da celeridade, da economicidade e do desenvolvimento nacional sustentável, assim como as disposições do Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro).

2.3. Modalidade de Licitação: **Pregão, na forma eletrônica**, conforme art. 6º, inc. XLI, da Lei Federal nº 14.133/2021.

2.4. Critério de Julgamento: **MENOR VALOR GLOBAL**, conforme art. 6º, inc. XLI, da Lei Federal nº 14.133/2021.

2.5. Modo de Disputa: **ABERTO**, conforme art. 56, inc. I, da Lei Federal n° 14.133/2021.

3. DEFINIÇÃO DO OBJETO

3.1. Registro de Preços para contratação de solução com fornecimento de equipamentos, licenças de softwares e serviços, para proteção e gerenciamento seguro da rede LAN/WAN da Secretaria de Estado da Saúde – SESAU/RO.

3.2. **DESCRIÇÃO DO OBJETO E QUANTIDADES ESTIMADAS PARA OS SERVIÇOS E METODOLOGIA DE CÁLCULO LISTADOS NO CATÁLOGO DE MATERIAIS (CATMAT) E O CATÁLOGO DE SERVIÇOS (CATSER):**

3.2.1. Considerar os itens listados no Catálogo de Materiais (CATMAT) e o Catálogo de Serviços (CATSER), disponível no link <https://catalogo.compras.gov.br/cnbs-web/busca>, para fins de pesquisa de mercado e de preço e todos os demais itens decorrentes.

ITEM	OBJETO	CATMAT/CATSER	UNIDADE	QUANTIDADE
1	ponto de acesso	609339	UND	246
2	SWITCHES DE ACESSO 24 PORTAS POE – TIPO 1	618778	UND	96
3	SWITCHES DE ACESSO DE 24 PORTAS POE – TIPO 2	618777	UND	96
4	SWITCHES DE ACESSO 48 PORTAS POE – TIPO 1	618780	UND	124
5	SWITCHES DE ACESSO 48 PORTAS POE – TIPO 2	618779	UND	124
6	SWITCHES CONCENTRADOR DE 24 PORTAS	618778	UND	20
7	SWITCHES CONCENTRADOR DE 48 PORTAS	618776	UND	02
8	CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 1	481646	UND	62
9	CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 2	481646	UND	02
10	CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 3	481646	UND	04
11	CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 4	481646	UND	02
12	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÕES COM LICENÇAS PARA CADA 100 DISPOSITIVOS	-	UND	08

GRUPO UNÍCO	13	SOLUÇÃO CENTRALIZADO DE LOGS E RELATÓRIOS COM LICENÇAS PARA ATÉ 25GB/LOG DIA	-	UND	05
	14	TRANSCEIVER SPF-LX	460348	UND	500
	15	TRANSCEIVER SFP+ 10GBASE-SR	462427	UND	2336
	16	TRANSCEIVER 25GE, módulo tipo SFP28-SR	462427	UND	10
	17	TRANSCEIVER 100 GE, módulo tipo QSFP28-SR	618355	UND	10
	18	SERVIÇOS DE INSTALAÇÃO DE PONTO DE ACESSO	609339	UND	246
	19	SERVIÇO DE INSTALAÇÃO DE SWITCHES DE ACESSO 24 PORTAS POE – TIPO 1 E TIPO 2	27111	UND	192
	20	SERVIÇOS DE INSTALAÇÃO DE SWITCHES DE ACESSO 48 PORTAS POE – TIPO 1 E TIPO 2	27111	UND	248
	21	SERVIÇOS DE INSTALAÇÃO DE SWITCH CONCENTRADOR de 24 PORTAS E 48 PORTAS	25576	UND	22
	22	SERVIÇO DE INSTALAÇÃO DE CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 1	16898	UND	62
	23	SERVIÇO DE INSTALAÇÃO DE CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 2	16898	UND	02
	24	SERVIÇO DE INSTALAÇÃO DE CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 3	16898	UND	04
	25	SERVIÇO DE INSTALAÇÃO DE CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 4	16898	UND	02
	26	SERVIÇO DE INSTALAÇÃO DE SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÕES COM LICENÇAS PARA CADA 100 DISPOSITIVOS	26972	UND	08
	27	SERVIÇO DE INSTALAÇÃO DE SOLUÇÃO CENTRALIZADO DE LOGS E RELATÓRIOS COM LICENÇAS PARA ATÉ 25GB/LOG DIA	26972	UND	05
	28	SERVIÇOS DE TREINAMENTO DAS SOLUÇÕES (POR SOLUÇÃO)	26972	UND	01
	29	SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (PONTO DE ACESSO)	26077	UND	246
	30	SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (SWITCHES DE ACESSO 24 PORTAS POE – TIPO 1 E TIPO 2)	26077	UND	192
	31	SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (SWITCHES DE ACESSO 48 PORTAS POE – TIPO 1 E TIPO 2)	26077	UND	248
	32	SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (SWITCH CONCENTRADOR de 24 PORTAS E 48 PORTAS)	26077	UND	22
	33	SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 1)	26077	UND	62
	34	SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 2)	26077	UND	02
	35	SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 3)	26077	UND	04
	36	SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 4)	26077	UND	02

- não foram localizados no catalogo do CATMAT/CATSER.

3.2.2. **DA MEMÓRIA DE CÁLCULO**

3.2.2.1. Os equipamentos de firewall e switches foram cuidadosamente dimensionados de acordo com o volume de tráfego de dados e o número de dispositivos ativos na rede. Da mesma forma, os pontos de acesso Wi-Fi foram planejados levando em consideração a extensão da área a ser coberta, visando assegurar um sinal robusto e eficiente para servidores e usuários das unidades de saúde.

- A **Coordenação de Inovação da Tecnologia da Informação** - CITI - da **Secretaria de Estado da Saúde** fez um levantamento dos ativos de rede.

UNIDADE:	**CEMETRON**			
MARCA	**MODELO**	**PORTAS**	**VELOCIDADE**	**OBS**

3COM	3870	48	Giga	Muito Antigo
Encore	ENH916P-NWY	16	100	Muito Antigo
H3C	S5120	24	Giga	Muito Antigo
H3C	S5500	24	Giga	Muito Antigo
HP	V1905-24	26	Giga	
HP	V1905-24	26	Giga	
HP	V1905-24	26	Giga	
INTELBRAS	SG 2404 Poe	24	Giga	O modelo foi definido pelas características, pois o tombamento está cobrindo o modelo
INTELBRAS	SG5200MR	48	Giga	
INTELBRAS	SG2620 QR	24	Giga	
INTELBRAS	SG2620 QR	24	Giga	
INTELBRAS	SG 2404 SR	24	Giga	
INTELBRAS	SF 2842 MR	28	Giga	
Surecom	EP-824DX-FS	24	100	Muito Antigo
TP-Link	TL-SF1024D	24	100	
Trendnet	TE100-S24R	24	100	Muito Antigo

UNIDADE:	**HICD**			
MARCA	**MODELO**	**PORTAS**	**VELOCIDADE**	**OBS**
INTELBRAS	SF 2400	24	100	
INTELBRAS	SF 2400	24	100	
INTELBRAS	SG 5200 MR	48	Giga	
INTELBRAS	SG 5200 MR	48	Giga	
TRELLIS	SWT24X	24	100	
TRELLIS	SWT24X	24	100	QUEIMADO
MICROTIK	1100 X2AH	13	Giga	QUEIMADO
INTELBRAS	SG 5200	48	Giga	QUEIMADO

UNIDADE:	**CAP** 2			
MARCA	**MODELO**	**PORTAS**	**VELOCIDADE**	**OBS**
INTELBRAS	SF2400 QR	24	100	

UNIDADE:	**CAP**			
MARCA	**MODELO**	**PORTAS**	**VELOCIDADE**	**OBS**
INTELBRAS	5200 MR	48	Giga	

UNIDADE:	**POC**			
MARCA	**MODELO**	**PORTAS**	**VELOCIDADE**	**OBS**

HP	V1910	48	Giga	Central
HP	V1910	48	Giga	Central
HP	V1910	48	Giga	Central
HP	V1910	48	Giga	Central
HP	V1910	48	Giga	Rack 1 - Oftalmo
HP	V1910	48	Giga	Rack 2 - Laboratório
HP	V1910	48	Giga	
HP	V1910	48	Giga	
HP	V1910	48	Giga	
INTELBRAS	SF400 QR+	24	Giga	Rack 2º Andar
INTELBRAS	SF400 QR+	24	Giga	Rack 2º Andar
INTELBRAS	SG2620QR	24	Giga	
DATACOM	DMSWITCH	28	Giga	***portas funcionando 100, emprestado SETIC - Superintendência Estadual de Tecnologia Informação***
TRELLIS	SWT24X	24	100	
INTELBRAS	SF800Q+	8	100	
MYMAX	MSW-S1005D-BK	5	100	
TENDA		8	100	
D-LINK	DES-1005C	5	100	
D-LINK	DES-1008A	8	100	
ENCORE		8	100	
3COM	3CBL UF26 Baseline	26	100	
SageCom	F@ST2705	5	100	

UNIDADE:	**LACEN**			
MARCA	**MODELO**	**PORTAS**	**VELOCIDADE**	**OBS**
TRELLIS DATACOM	24SWT24X	24	100	PORTAS COM DEFEITO
TRELLIS DATACOM	24SWT24X	24	100	PORTAS COM DEFEITO
TRELLIS DATACOM	24SWT24X	24	100	PORTAS COM DEFEITO
KIAOMY	KIAOMY 24PX	24	100	COM DEFEITO
INTELBRAS	SG 52000 MR	48	Giga	PORTAS COM DEFEITO
INTELBRAS	SG 4800	48	Giga	DEFEITO NÃO ATUALIZA E PERDE CONFIGURAÇÃO

UNIDADE:	**SEPOAD**			
MARCA	**MODELO**	**PORTAS**	**VELOCIDADE**	**OBS**
INTELBRAS	SG2620 QR	24		Central
INTELBRAS	2400 QR+	24		Rack Adm
3COM	3870	48		Rack Adm

UNIDADE:	**CETAS**

MARCA	MODELO	PORTAS	VELOCIDADE	OBS
ENCORE	ENH924-AUT	24	100	
INTELBRAS	SF2400 QR	24	100	

UNIDADE:	Hospital Regional São Francisco do Guaporé			
MARCA	**MODELO**	**PORTAS**	**VELOCIDADE**	**OBS**
3Com	3CR17451-91	48	Giga	

UNIDADE:	HEURO - Hospital de Urgência de Emergência de Cacoal			
MARCA	**MODELO**	**PORTAS**	**VELOCIDADE**	**OBS**
MRV	MR2226-2C	24	100	POSSUI LAUDO TÉCNICO DATADO DE 2020 COMO EQUIPAMENTO OBSOLETO
3COM	3CR17161-91	24	100	SEM PORTA DISPONÍVEL
3COM	3C17300	24	100	3 PORTAS QUEIMADAS E AS DEMAIS TODAS EM USO
INTELBRAS	SG 5200 MR	48	Giga	12 PORTAS QUEIMADAS
TP LINK	TL-SG 1024D	24	Giga	
3COM	3CRBSG2893	28	Giga	
3COM	3C16980A	24	100	POSSUI LAUDO TÉCNICO DATADO DE 2020 COMO EQUIPAMENTO OBSOLETO
MULTILASER	RE116	16	100	SEM PORTA DISPONÍVEL
MERCUSYS	MS108G	8	Giga	DESKTOP SWITCH
TP-LINK	LS1008	8	100	DESKTOP SWITCH COM TODAS AS PORTAS EM USO
INTELBRAS	SF 1600 D	16	100	SEM PORTA DISPONÍVEL
3COM	3CBSG2893	28	Giga	EQUIPAMENTO NA SALA DA TI COM TODAS AS PORTAS EM USO
KNUP	KP-E06	16	100	SEM PORTA DISPONÍVEL
MERCUSYS	MS108	8	100	DESKTOP SWITCH
MULTILASER	RE308	8	100	DESKTOP SWITCH
INTELBRAS	SF 800 Q+	8	100	DESKTOP SWITCH

UNIDADE:	PALÁCIO RIO MADEIRA - SESAU			
MARCA	**MODELO**	**PORTAS**	**VELOCIDADE**	**OBS**
INTELBRAS	SG 5200 MR	48	Giga	
INTELBRAS	SG 5200 MR	48	Giga	
INTELBRAS	SG 5200 MR	48	Giga	
INTELBRAS	SG 5200 MR	48	Giga	
INTELBRAS	SG 5200 MR	48	Giga	
INTELBRAS	SG 5200 MR	48	Giga	
INTELBRAS	SG 5200 MR	48	Giga	
INTELBRAS	SG 2404 PoE L2	24	Giga	
INTELBRAS	SG 5204 MR L2+	48	Giga	**EMPRESTADO SEOSP - Secretaria de Estado de Obras e Serviços Públicos**
INTELBRAS	SG 5204 MR L2+	48	Giga	**EMPRESTADO SEOSP - Secretaria de Estado de Obras e Serviços Públicos**

UNIDADE:	**HRC - HOSPITAL REGIONAL DE CACOAL**			
MARCA	MODELO	PORTAS	VELOCIDADE	OBS
3COM	SUPERSTACK 3 4500	26	/1000	CONTEM PORTAS QUEIMADAS/ TODAS AS PORTAS UTILIZADAS
INTELBRAS	SG 5200MR	28	/1000	CONTEM PORTAS QUEIMADAS/ TODAS AS PORTAS UTILIZADAS
HP	1410-24-R	24	/1000	CONTEM PORTAS QUEIMADAS/ TODAS AS PORTAS UTILIZADAS
3COM	BASELINE 2928 (3CRBSG2893)	28	/1000	CONTEM PORTAS QUEIMADAS/ TODAS AS PORTAS UTILIZADAS
3COM	BASELINE 2928 (3CRBSG2893)	28	/1000	CONTEM PORTAS QUEIMADAS/ TODAS AS PORTAS UTILIZADAS
3COM	BASELINE 2928 (3CRBSG2893)	28	/1000	CONTEM PORTAS QUEIMADAS/ TODAS AS PORTAS UTILIZADAS
3COM	BASELINE 2928 (3CRBSG2893)	28	/1000	CONTEM PORTAS QUEIMADAS/ TODAS AS PORTAS UTILIZADAS
3COM	BASELINE 2928 (3CRBSG2893)	28	/1000	CONTEM PORTAS QUEIMADAS/ TODAS AS PORTAS UTILIZADAS
3COM	BASELINE 2928 (3CRBSG2893)	28	/1000	CONTEM PORTAS QUEIMADAS/ TODAS AS PORTAS UTILIZADAS
3COM	BASELINE 2928 (3CRBSG2893)	28	/1000	CONTEM PORTAS QUEIMADAS/ TODAS AS PORTAS UTILIZADAS
3COM	BASELINE 2928 (3CRBSG2893)	28	/1000	CONTEM PORTAS QUEIMADAS/ TODAS AS PORTAS UTILIZADAS
3COM	BASELINE 2928 (3CRBSG2893)	28	/1000	CONTEM PORTAS QUEIMADAS/ TODAS AS PORTAS UTILIZADAS
3COM	SWITCH 4800G SFP	24	/1000	NÃO UTILIZADO POR FALTA DE RECURSO
3COM	BASELINE 2928 (3CRBSG2893)	28	/1000	CONTEM PORTAS QUEIMADAS/ TODAS AS PORTAS UTILIZADAS
GENERICOS QUANTIDADE = 14	SWITCHS DE 8 PORTAS	8	/100	DISTRIBUÍDO POR TODO HOSPITAL PARA SUPRIR SETORES E RACKS COM FALTA DE PORTAS

UNIDADE:			**Hospital e Pronto Socorro João Paulo II - JP II**	
ITEM	MARCA	Nº PORTAS	PATRIMÔNIO/NºSÉRIE	ESTADO
Switch	INTELBRAS	24	OT12011103717	Em uso
Switch	INTELBRAS	48	67619	Em uso
Switch	INTELBRAS	48	67911	Em uso
Switch	3COM	26	9J8FALN7E0332	Em uso
Switch	INTELBRAS	48	RULB4800781CS	Em uso
Switch	3COM	26	SN	Em uso
Switch	COMTAC	24	SN	Em uso
Switch	INTELBRAS	24	67915	Em uso
Switch	INTELBRAS	24	OT12071301171	Em uso
Switch	INTELBRAS	48	71770	Em uso
Switch	INTELBRAS	48	71769	Em uso
Switch	D-LINK	48	67451	Em uso
Switch	INTELBRAS	48	67910	DEFEITO
Switch POE	ENTERESYS	24	340022915D13	Em uso
Switch	TECVOZ		78161	Em uso
Switch	INTELBRAS	24	OT12011112947	Em uso

Switch	HP	24	6600083046342	Em uso
Switch	INTELBRAS	48	RULD370010430	Em uso
Switch	ENTERESYS	24	12454526905A	DEFEITO
Switch POE	TECVOZ		78184	DEFEITO
Switch	INTELBRAS	24	OT12101006452	Em uso

UNIDADE:	**HRB Hospital Regional de Buritis**			
MARCA	MODELO	PORTAS	VELOCIDADE	OBS
3COM	3CR17451-91	48	/1000	ALGUMAS PORTAS QUEIMADAS

UNIDADE:	**GRS 1 - JI PARANÁ**			
MARCA	MODELO	PORTAS	VELOCIDADE	OBS
3COM		24	/100	ALGUMAS PORTAS QUEIMADAS
3COM		24	/100	Em uso

UNIDADE:	**GRS 2 - CACOAL**			
MARCA	MODELO	PORTAS	VELOCIDADE	OBS
TP		24	/100	ALGUMAS PORTAS QUEIMADAS

UNIDADE:	**GRS 3 - VILHENA**			
MARCA	MODELO	PORTAS	VELOCIDADE	OBS
TP		24	/100	ALGUMAS PORTAS QUEIMADAS

UNIDADE:	**GRS 4 - ARIQUEMES**			
MARCA	MODELO	PORTAS	VELOCIDADE	OBS
3COM		24	/100	ALGUMAS PORTAS QUEIMADAS
UNIDADE	**BARCO HOSPITAL**			
MARCA	MODELO	PORTAS	VELOCIDADE	OBS
DLINK		24	/100	ALGUMAS PORTAS QUEIMADAS

UNIDADE:	**HB - Hospital de Base Ary Pinheiro**				
MARCA	MODELO	PORTAS	VELOCIDADE	Quantidade	OBS
		48	100	36	ALGUMAS PORTAS QUEIMADAS
		24	100	52	ALGUMAS PORTAS QUEIMADAS
		16	100	88	ALGUMAS PORTAS QUEIMADAS
		8	100	47	ALGUMAS PORTAS QUEIMADAS

TOTAL GERAL SWITCH ATUALMENTE

DESCRIÇÃO	PORTAS	QUANTIDADE

SWITCHS	05	03
SWITCHS	08	64
SWITCHS	13	01
SWITCHS	16	92
SWITCHS	26	07
SWITCHS	24	100
SWITCHS	28	14
SWITCHS	48	74
TOTAL		355

QUADRO DE DISTRIBUIÇÃO

UNIDADE	CONTROLADOR SEGURO DE REDE WLAN E LAN				SW ACESSO 24P POE	SW ACESSO 48P POE	SW ACESSO 24P FULL POE	SW ACESSO 48P FULL POE	SW CORE FIBER 48P	SW CORE FIBER 24P	PONTO DE ACESSO	TOTAL SW UNIDADE
	TIPO 4	TIPO 3	TIPO 2	TIPO 1	TIPO 1	TIPO 1	TIPO 2	TIPO 2	-	-	-	
Datacenter	2										-	
Edifício Rio Machado (Palácio Rio Madeira)			2			26		26		2	SETIC	26
HBAP Hospital de Base Ary Pinheiro		2			25	20	25	20	2		30	45
HICD Hospital Infantil Cosme e Damião				2	3	4	3	4		2	8	7
POC Policlínica Oswaldo Cruz				2	8	9	8	9		2	16	17
JPII Hospital e Pronto Socorro João Paulo II		2			9	10	9	10		2	18	19
CEMETRON Centro de Medicina Tropical de Rondônia				2	4	11	4	11		2	21	15
CEPEM Centro de Pesquisas de Medicina Tropical de Rondônia				2		2		2			3	2
HCAMP Hospital de Campanha				2	4	2	4	2		2	8	6
HRSFG Hospital Regional de São Francisco				2	1	2	1	2			3	3
HRE Hospital Regional de Extrema				2	1	1	1	1			3	2
HRB Hospital Regional de Buritis				2	1	1	1	1			3	2

HRC Hospital Regional de Cacoal		2			6	8	6	8		2	28	14
HEURO Hospital de Urgência e Emergência Regional de Cacoal		2			4	4	4	4		2	21	8
CDI Centro de Diagnóstico por Imagem				2	1	1	1	1			3	2
CDA Centro de Diálise de Ariquemes				2	5	3	5	3		2	9	8
CERO Centro de Reabilitação de Rondônia				2	1	1	1	1			4	2
AMI Unidade de Assistência Médica Intensiva				2	1	1	1	1			8	2
LEPAC Unidade Raiz do Laboratório Estadual de Patologia e Análises Clínicas				2		1		1			3	1
LACEN Laboratório Central de Saúde Pública				2	3	4	3	4		2	9	7
LAFRON Laboratório de Fronteira				2	1		1				3	1
GERREG Gerência Estadual de Regulação	LOCAL POC											0
CRUE Central Regional de Urgência e Emergência de Porto Velho		LOCAL POC										0
GRS 1 - JI PARANÁ				2	1	1	1	1			2	2
GRS 2 - CACOAL				2		1		1			2	1
GRS 3 - VILHENA				2	1	1	1	1			2	2
GRS 4 - ARIQUEMES				2	1	1	1	1			2	2
GRS 5 - ROLIM DE MOURA				2	1		1				2	1
BARCO HOSPITAL				2		1		1			2	1
CETAS Centro de Educação Técnico - Profissional na Área de Saúde				2	3		3				4	3

CGAF Coordenadoria de Gestão e Assistência Farmacêutica				2	3	2	3	2			4	5
SAMD Diretoria Serviço Assistencial Multidisciplinar Domiciliar		LOCAL HB									2	0
CENE Coordenadoria Estadual Nutrição Enteral				2		1		1			2	1
CAF1 Central de Abastecimento Farmacêutico para Medicamentos				2	1		1				3	1
CAF 2 Central de Abastecimento Farmacêutico para Artigo Médico Hospitalar				2		2		2			3	2
CES Conselho Estadual de Saúde				2	1		1				2	1
CIB Comissão Intergestores Bipartite					1		1				2	1
CAP Coordenadoria de Almoxarifado e Patrimônio				2	1		1				2	1
CAP II Coordenadoria de Almoxarifado e Patrimônio				2	1	2	1	2			2	3
CENTRAL DE TRANSPLANTE localizado dentro do CPOAD		LOCAL CPOAD										0
CEREST Centro de Referência em Saúde do Trabalhador CPOAD		LOCAL CPOAD										0
CPOAD Coordenadoria de Atenção Psicossocial e Políticas sobre Drogas				2	2	1	2	1			4	3
CAPS Centro de Assistência Psicossocial				2	1		1				3	1
TOTAL	2	4	2	62	96	124	96	124	2	20	246	220

3.3. **Classificação do objeto**

3.3.1. O objeto pleiteado nos autos não envolve técnicas desconhecidas no mercado ou requerem inovação tecnológica para a sua execução, tratando-se assim de bem comum, pois é possível estabelecer, por intermédio de especificações utilizadas no mercado, padrões de qualidade e desempenho característicos ao objeto, de modo que é possível a decisão entre os materiais ofertados pelos participantes com base no menor preço.

3.3.2. A classificação como comum não se confunde com a complexidade do objeto. O que deve ser verificada é a possibilidade de seus padrões de desempenho e qualidade serem definidos objetivamente em especificações usualmente adotadas no mercado, o que fica evidente no presente instrumento convocatório.

3.3.3. Corroborando com esse entendimento, transcrevemos o relatado pelo Professor Marçal Justen Filho em seu livro Pregão - Comentários à Legislação do Pregão Comum e Eletrônico:

> "Ou seja, há casos em que a Administração necessita de bens que estão disponíveis no mercado, configurados em termos mais ou menos variáveis. São hipóteses em que é público o domínio das técnicas para a produção do objeto e seu fornecimento ao adquirente (inclusive à Administração), de tal modo que não existe dificuldade em localizar um universo de fornecedores em condições de satisfazer plenamente o interesse público. Em outros casos, o objeto deverá ser produzido sob encomenda ou adequado às configurações de um caso concreto.
> (...)

3.3.4. Para concluir, numa tentativa de definição, poderia dizer-se que bem ou serviço comum é aquele que apresenta sob identidade e características padronizadas e que se encontra disponível, a qualquer tempo, num mercado próprio."

3.3.5. Diante do exposto, e considerando que a Lei n° 14.133/21 define em seu Art. 6º Inciso XIII - "bens e serviços comuns: aqueles cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado", define-se que o objeto da presente contratação é comum.

4. FUNDAMENTAÇÃO DA NECESSIDADE DA CONTRATAÇÃO (JUSTIFICATIVA)

4.1. DA NECESSIDADE DA COORDENADORIA DE INOVAÇÃO E TECNOLOGIA DA INFORMAÇÃO - SESAU - CITI:

A Secretaria de Estado da Saúde – SESAU/RO tem como meta estratégica na Tecnologia da Informação e Comunicação - TIC a disponibilização de ferramentas tecnológicas que garantam o adequado funcionamento do ambiente tecnológico e que colaborem com a melhoria da produtividade dos seus usuários. Portanto, assim como os outros poderes que compõem a estrutura de Estado, a SESAU/RO necessita de proteção e segurança sobre o conteúdo armazenado e manipulado internamente nos respectivos ambientes para que sejam mantidas a confidencialidade, a integridade e a disponibilidade das informações existentes.

Tendo em vista a necessidade de ter uma infraestrutura padronizada adequada para a guarda e operação dos equipamentos de Tecnologia da Informação da SESAU/RO e, buscando atender o compromisso do Governo do Estado de Rondônia em garantir eficiência da gestão pública, é essencial a adequação do Data Center atual visando obter um ambiente computacional seguro para a SESAU/RO.

Esta é uma ação de essencial importância para o processo de estruturação de TIC no âmbito da Secretaria de Estado da Saúde de Rondônia, promovendo o compartilhamento de uma infraestrutura estável, segura, ágil, robusta e moderna.

A solução de rede sem fio será projetada para prover acesso seguro e eficiente à rede de dados, atendendo dispositivos corporativos e pessoais, tais como notebooks e smartphones. Além disso, a rede LAN com fio suportará a infraestrutura dos pontos de acesso sem fio e garantirá a disponibilidade de conexões cabeadas de alta velocidade para aplicações críticas.

SOLUÇÃO PROPOSTA

Capacidade e Escalabilidade:

Atender à crescente demanda por acessos simultâneos, garantindo alta disponibilidade e baixa latência na rede.

Escalabilidade para suportar futuras expansões, incluindo dispositivos IoT como câmeras IP, sensores, e outros equipamentos conectados à rede.

Segurança Avançada:

Os elementos que compõem a rede devem implementar de forma integrada ferramentas de segurança de nova geração, incluindo proteção de rede, sistemas de prevenção de intrusões (IPS) e soluções avançadas de detecção de ameaças para proteger dados sensíveis e manter a integridade da rede, para garantir a segurança da informação fim a fim e possibilitar a visibilidade e controle de tráfego e aplicações, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede.

Políticas de acesso e autenticação robustas para garantir que apenas usuários autorizados e dispositivos seguros possam acessar a rede.

Gestão e Monitoramento Integrados:

Soluções de gerenciamento de rede centralizado que permitem o controle e a visualização completos da

infraestrutura de rede, facilitando a identificação e resolução rápida de problemas.

Ferramentas de monitoramento em tempo real para avaliar o desempenho da rede, uso de banda e detectar padrões anormais de tráfego.

Treinamento e Suporte:

Programas de treinamento para equipes técnicas e usuários finais, garantindo o uso eficiente e seguro da infraestrutura de rede.

Suporte contínuo e manutenção para assegurar a operacionalidade constante e atualizações de segurança.

Custo-Eficiência:

Avaliação do retorno sobre investimento (ROI) e análise de custo-benefício para assegurar que as soluções propostas ofereçam o melhor valor, mantendo o orçamento dentro do previsto.

DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

Com a contratação, pretende-se alcançar os seguintes benefícios:

Disponibilizar uma rede wireless em todos os departamentos e setores das unidades ;

Entregar uma rede wireless confiável para os **servidores e pacientes**.

Entregar um painel de administração unificado para o time de TIC, para que possa gerenciar todos os pontos de acesso;

Oferecer uma rede wireless que atende os requisitos atuais garantindo a qualidade mediante o crescimento futuro;

Oferecer um acesso seguro para todos os usuários, visando garantir a confidencialidade, integridade, disponibilidade e autenticidade.

Essencial para o provimento da Infraestrutura de TIC, a aquisição de solução integrada para gerenciamento do ciclo de vida, proteção, identificação e rastreabilidade dos dados corporativos irá auxiliar na disponibilidade dos serviços e informações críticas fornecidos pela SESAU/RO aos públicos interno e externo.

Esta aquisição é fundamental para a melhoria da inteligência organizacional, integração dos dados, continuidade dos serviços, preservação das informações críticas ao negócio, bem como para resguardar o uso de dados e informações pessoais, e garantir a recuperação e acesso a essas informações, conforme exigência prevista na Lei 13.709/18 - Lei Geral de Proteção de Dados.

Percebe-se claramente que além de um ambiente desatualizado (sem suporte) não há ferramental específico destinado à proteção de dados, além dos elementos de interconexão. São usadas medidas paliativas e/ou rudimentares para que seja possível manter o mínimo necessário de segurança lógica que um ambiente corporativo exige. A aquisição de uma solução de Next Generation Firewall – NGFW, composta com Access Points e Switches integrados, irão garantir que todo escopo de segurança da informação seja protegido contra os mais modernos ataques cibernéticos.

Tais medidas são fundamentais para manter e assegurar a disponibilidade adequada dos serviços de TI, que dão apoio a alta gestão da SESAU/RO, em casos de tentativa de exploração de vulnerabilidade, além de permitir a continuidade das operações, apoiando os demais setores desta instituição, de forma a manter seus dados íntegros, seguros e disponíveis.

Aquisição de hardwares, softwares e licenciamentos para implantação e modernização tecnológica da infraestrutura de segurança da informação, tem o objetivo de não só aumentar a capacidade de proteção de todos os ativos de TI, mas também as informações elencadas como estratégica pela Secretaria de Estado da Saúde de Rondônia, sendo possível o reconhecimento e padronização de uso das aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões de acesso a sistemas, sites web e dados na SESAU/RO. Assim como, a contratação por um maior período (acima de 12-24 meses), faz com que as soluções sejam melhores absorvidas pela equipe técnica de TI, trazendo mais estabilidade e seguranças na gestão, além da ampliação e inteligência embarcada nas soluções contratadas.

A infraestrutura de T.I.C é elemento fundamental para a gestão do ambiente tecnológico da SESAU/RO, e o alcance do bom desempenho de suas atribuições institucionais. Uma solução integrada de gerenciamento do ciclo de vida das informações, é composta por componentes de software que permitem gerenciar e monitorar o fluxo das informações trafegadas, além de uma infraestrutura de hardware, que se destina basicamente ao efetivo processamento desse fluxo.
Nesse mesmo tema, destaca-se que atualmente a SESAU/RO mantém uma diversidade de Soluções de Tecnologia, nos quais vários softwares e equipamentos de diversos fabricantes interagem com serviços providos por uma gama de outros prestadores.

Isso eleva o nível complexidade tecnológica do ambiente computacional da SESAU/RO, isto é, fatores que exigem da Equipe Técnica do CTI, um grande esforço no sentido de torná-lo íntegro e, tanto quanto possível, disponível para os seus usuários internos e externos, cujos trabalhos dependem de forma direta e incisiva do pleno funcionamento e da alta disponibilidade deste ambiente computacional.

Entende-se, portanto, que a atual infraestrutura de segurança da informação da SESAU/RO apresenta sinais claros de necessidade de novos investimentos, considerando-se, nesse caso, as perspectivas de modernização e de expansão

no âmbito da Entidade para atendimento geral.

Dessa forma, a SESAU/RO, por intermédio de sua Coordenadoria de Tecnologia da Informação - CTI, necessita planejar e executar a expansão dos seus recursos tecnológicos, pela qual, tomando como referência os atos normativos e instrumentos legais afetos a esse propósito, bem como os padrões atuais de mercado de hardware, software, associados às políticas para proteção e armazenamento de dados e relacionadas a serviços de infraestrutura de TI, proporcione uma solução integrada para provimento de serviços por meio de alta disponibilidade tecnológica.

Por razões como essas, considera-se que os processos de gestão das demandas institucionais que envolvem TI precisam ser dotados de agilidade, confiança, segurança, bem como de prestação eficaz de serviços e de infraestrutura adequada, esta disponibilizada por meio de softwares, equipamentos e componentes eficientes e funcionais, para suportar os sistemas corporativos e, finalmente, atender às reais necessidades da SESAU/RO e corresponder, positivamente, às expectativas dos assistidos e usuários envolvidos no contexto da Secretaria de Estado da Saúde.

Portanto, em face das razões acima expostas, elaboramos o presente Termo de Referência, com o fim de instruir procedimento administrativo licitatório objetivando contratação de empresa para o fornecimento de Solução de INFRAESTRUTURA DE DATACENTER SEGURO para a Secretaria de Estado da Saúde.

5. ALINHAMENTO COM AS NECESSIDADES TECNOLÓGICAS

5.1. O inciso III do Art. 42 do Decreto nº 28.874/24, ao estabelecer a necessidade de alinhamento com as necessidades tecnológicas e de negócio para as contratações de Soluções de TIC, visa garantir a efetividade e a otimização dos investimentos em tecnologia. As Soluções de TIC, por sua natureza, possuem um caráter técnico e instrumental, diretamente relacionadas à infraestrutura, software e hardware.

A Secretaria de Estado da Saúde em Rondônia (SESAU-RO) é responsável pelo armazenamento e gerenciamento de dados sensíveis e pela gestão de serviços críticos à saúde da população. A secretaria opera com sistemas essenciais, incluindo a dispensação de medicamentos, prontuários eletrônicos, gestão de filas na regulação, resultados de exames e atendimento call center. Esses sistemas são fundamentais para a prestação de cuidados médicos eficazes e para o funcionamento eficiente das unidades de saúde.

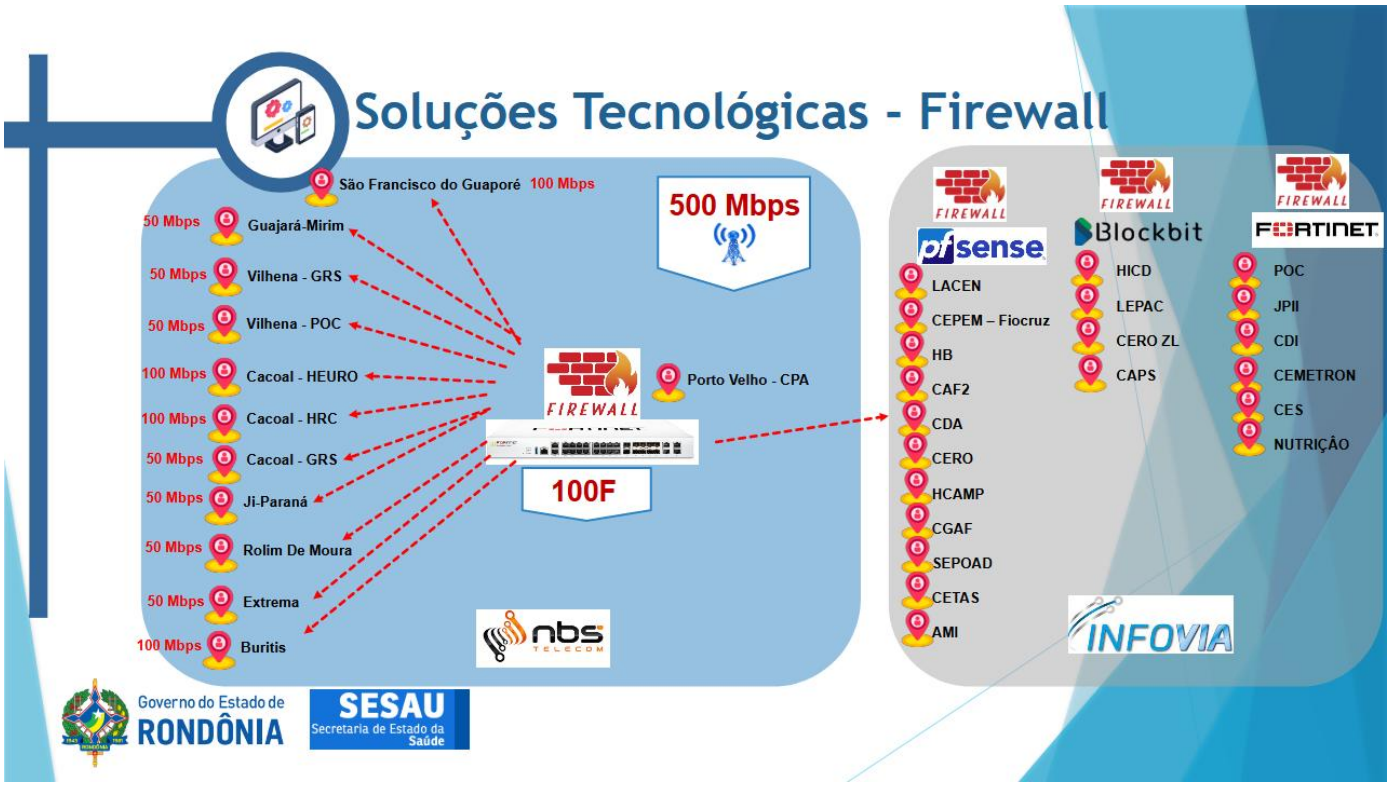
Dado o caráter sensível e a importância dos dados geridos, é imperativo que a infraestrutura de TI da SESAU-RO esteja protegida e gerenciada com o mais alto nível de segurança e confiabilidade. Para garantir a integridade, confidencialidade e disponibilidade dos dados e serviços, propomos uma solução integrada que inclui o fornecimento de equipamentos, licenças de software e serviços especializados.

5.2. Identificação das Necessidades Tecnológicas

5.2.1. A Secretaria de Estado da Saúde de Rondônia (SESAU-RO) opera atualmente em um ambiente de segurança de rede misto, que enfrenta alguns desafios em termos de infraestrutura e gestão. O ambiente é composto por diferentes soluções de firewall, cada uma com suas limitações e problemas específicos.

5.2.2. Atualmente, a SESAU-RO utiliza um firewall Fortinet locado, que não atende plenamente às necessidades de proteção de toda a rede da secretaria, cobrindo apenas alguns pontos específicos. Além disso, a secretaria conta com o uso do **PFSENSE**, uma solução de firewall gratuita, para complementar as deficiências de cobertura do Fortinet.

5.2.3. Outro componente do ambiente de segurança de rede é o **Blockbit**, cuja licença encontra-se vencida e o sistema está desatualizado. Devido a essa situação, a secretaria optou por reaproveitar o hardware do Blockbit para a instalação e execução do **PFSENSE**, buscando manter um nível mínimo de segurança e funcionalidade na rede. Essa solução temporária visa garantir a continuidade dos serviços enquanto não se implementa uma infraestrutura de segurança mais robusta e centralizada que atenda integralmente às necessidades da SESAU-RO.



5.2.4. Diante deste cenário os switches utilizados pela Coordenadoria de Tecnologia da Informação estão desatualizados e não atendem às demandas tecnológicas da secretaria. A infraestrutura de rede conta com um número excessivo de hubs e switches de 5,8 e 16 portas, o que resulta em um alto nível de cascateamento. Essa configuração aumenta significativamente o risco de falhas e contribui para a lentidão da rede, afetando a eficiência e a produtividade dos usuários.

5.2.5. Há uma necessidade urgente de adquirir switches modernos com suporte a **Power over Ethernet (PoE)** para viabilizar a implementação de tecnologias mais avançadas, como a telefonia **VoIP** (Voice over IP) e access points para redes sem fio. Esses equipamentos PoE são fundamentais para fornecer a energia necessária diretamente através da rede para dispositivos como telefones IP e pontos de acesso, eliminando a necessidade de fontes de alimentação separadas e simplificando a infraestrutura de TI.

5.2.6. Os access points atualmente utilizados pela Coordenadoria de Tecnologia da Informação são, em sua maioria, equipamentos de uso doméstico que não foram projetados para lidar com o volume de dados e o número de acessos simultâneos exigidos pelo ambiente corporativo da secretaria. Esses dispositivos frequentemente apresentam problemas como travamentos, reinicializações inesperadas e perda de configurações devido à sobrecarga de dados, comprometendo a estabilidade e a qualidade da conexão de rede.

5.2.7. Atualmente, apenas o PRM Edifício Rio Machado e o Espaço SESAU no Porto Velho Shopping conta com access points de nível empresarial, fornecidos pela SETIC, que são mais robustos e adequados para suportar as demandas de um ambiente corporativo.

5.3. Diante do exposto, conclui-se que a referida contratação se enquadra na previsão do Inciso III do Art. 42 do Decreto nº 28.874/24, que se aplica especificamente às Soluções de TIC. A avaliação das necessidades para a contratação de serviços de saúde deve se basear em critérios próprios da área da saúde, priorizando a qualidade, a efetividade e a resolutividade dos serviços prestados, com foco na promoção da saúde e no bem-estar da população.

6. DA JUSTIFICATIVA PARA O PARCELAMENTO (OU NÃO) DA SOLUÇÃO

6.1. A regra a ser observada pela Administração nas licitações é a do parcelamento do objeto, conforme disposto no Inciso II do art. 47 da Lei nº 14.133/21, quando for tecnicamente viável e economicamente vantajoso. Assim, é imprescindível que a divisão do objeto seja técnica e economicamente viável e não represente perda de economia de escala (Súmula 247 do TCU).

6.2. De outro giro, no entendimento da Procuradoria Geral do Estado junto a SESAU (PGE-SESAU), o Decreto n° 28.874/2024 apresenta no art. 42, IV que esse parcelamento assemelha-se a figura da fragmento da despesa que é algo proibido, mas caso seja utilizado, deve haver justificativa.

6.3. Conforme dispõe o caput do art. 34 da Lei Federal nº 14.133/2021, o julgamento por menor preço e, quando couber, por técnica e preço considerará o menor dispêndio para a Administração, atendidos os parâmetros mínimos de qualidade definidos no edital de licitação.

6.4. Os itens objeto desta aquisição devem ser licitados e adjudicados por um único grupo, considerando sua indivisibilidade, pois tanto as soluções quanto os serviços são de natureza semelhante e possuem uma forte correlação

técnica e tecnológica entre si. Realizar a contratação de todos esses componentes por um único fornecedor é crucial para garantir a compatibilidade e a eficiência operacional de toda a infraestrutura de TI da organização.

6.5. A contratação de diferentes fornecedores para o fornecimento de equipamentos e serviços distintos acarretaria significativos riscos ao projeto. Um dos principais riscos advém da necessidade constante de comunicação e coordenação entre os diversos fornecedores, o que, na prática, muitas vezes se mostra ineficiente e insatisfatório. Essa falta de fluidez na comunicação pode levar a atrasos, falhas de integração e, em última análise, prejudicar o CONTRATANTE. Além disso, é essencial que haja uma integração técnica perfeita entre todos os itens adquiridos. Dividir o fornecimento entre diversos fornecedores aumentaria a complexidade da implementação e os custos de integração, além de aumentar o risco de uma execução inadequada.

6.6. Licitar os itens separadamente poderia prejudicar tanto o conjunto da licitação por questões técnicas quanto a economia de escala por razões econômicas, tornando inviável a operação ideal da solução de conectividade, que envolve serviços complementares. Por outro lado, a contratação dessa solução de forma agrupada deve proporcionar benefícios, como a redução do valor final do contrato, devido à economia de escala. Adicionalmente, esse modelo elimina a complexidade de gerenciar múltiplos fornecedores para diferentes componentes da solução de conectividade.

6.7. Portanto, por se tratar de uma solução integrada de serviços e equipamentos, é fundamental que a execução seja realizada por um único fornecedor. Essa abordagem garante a qualidade do serviço prestado, evitando a segregação do objeto que poderia comprometer a eficácia da solução como um todo. Dessa forma, assegura-se a produtividade, a economicidade e a eficiência na implementação e manutenção dos serviços de TI da organização.

6.8. Desta forma, o agrupamento de elementos que compõem a mesma solução compõe a melhor estratégia da Administração, quando a adjudicação de itens isolados onera o "o trabalho da administração pública, sob o ponto de vista do emprego de recursos humanos e da dificuldade de controle, colocando em risco a economia de escala e a celeridade processual", vide o ACÓRDÃO Nº 5301/2013 – TCU – 2ª Câmara.

6.9. Desta forma do presente objeto mostra-se tecnicamente inviável a sua divisão.

7. PARTICIPAÇÃO DE EMPRESAS SOB A FORMA DE CONSÓRCIO E COOPERATIVAS

7.1. Em regra, a formação de consórcios ou cooperativa é admitida quando o objeto a ser licitado envolve questões de alta complexidade ou de relevante vulto onde para a obtenção de melhor proposta para a Administração exige a reunião de empresas ou profissionais especializados para o alcance do objetivo final da aquisição, ou seja, admite-se a formação de consórcio ou cooperativa em situações de aquisições de objetos em que uma empresa isoladamente não teria condições de suprir os requisitos técnicos e de habilitação do edital.

7.2. O objeto deste Termo de Referência consiste no Registro de Preços para contratação de solução com fornecimento de equipamentos, licenças de softwares e serviços, para proteção e gerenciamento seguro da rede LAN/WAN da Secretaria de Estado da Saúde – SESAU/RO. Tais itens não apresentam características de alta complexidade técnica nem demandam a integração de tecnologias ou especializações diversas que inviabilizem a execução do fornecimento por uma única empresa. Ademais, o mercado brasileiro dispõe de ampla oferta de fornecedores qualificados e plenamente capazes de atender à totalidade do objeto do edital, o que elimina a necessidade de formação de parcerias entre empresas, seja por meio de consórcios ou cooperativas.

7.3. Dessa forma, a vedação à participação de empresas reunidas sob a forma de consórcio ou cooperativa neste processo de contratação fundamenta-se no art. 15 da Lei Federal nº 14.133/2021, que admite essa modalidade de associação apenas em situações onde o objeto licitado apresente alta complexidade ou vulto significativo. Tais condições, conforme demonstrado, não se aplicam ao presente caso, dado o caráter simples e acessível do fornecimento de periféricos de informática.

7.4. Além disso, a decisão encontra respaldo na jurisprudência do Tribunal de Contas da União (TCU), que considera válida a restrição à formação de consórcios desde que justificada tecnicamente. Precedentes como o Acórdão TCU nº 2062/2017 – Plenário reforçam que tal vedação deve assegurar que a competitividade e a eficiência do certame sejam preservadas.

7.5. A vedação à participação de consórcios ou cooperativas neste procedimento licitatório não trará prejuízo à competitividade do certame. Pelo contrário, ela assegura isonomia entre os licitantes, permitindo que as empresas concorram em condições equitativas, sem a necessidade de formação de agrupamentos.

7.6. Diante do exposto, conclui-se que a vedação à participação de consórcios ou cooperativas no presente processo licitatório é técnica e juridicamente adequada, considerando que o objeto da licitação não apresenta complexidade técnica nem exige integração de especializações. A vedação busca assegurar a eficiência e a regularidade do processo de contratação.

8. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

8.1. PONTO DE ACESSO

8.1.1. Ponto de acesso (AP) que permita acesso dos dispositivos à rede wireless e que possua todas as suas configurações centralizadas em controlador wireless;

8.1.2. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;

8.1.3. Deve ser compatível e gerenciado por qualquer modelo de controladora SEGURA de WLAN e LAN - Tipo 01, 02, 03 e 04 deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

8.1.4. Deve identificar automaticamente o controlador wireless ao qual se conectará;

8.1.5. Deve permitir ser gerenciado remotamente através de links WAN;

8.1.6. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;

8.1.7. Deve possuir capacidade tri-band com rádios 2.4GHz, 5GHz e 6GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;

8.1.8. O ponto de acesso deve poder funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7.

8.1.9. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;

8.1.10. Deve permitir a conexão de 400 (quatrocentos) clientes por rádio simultaneamente;

8.1.11. Deve possuir 2 (duas) interfaces Ethernet padrão sendo uma 100/1000/2500 Base-T RJ45 e outra 10/100/1000 Base-T RJ-45 para permitir a conexão com a rede LAN;

8.1.12. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;

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

8.1.14. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;

8.1.15. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Adicionalmente deve possuir entrada de alimentação 12VDC;

8.1.16. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;

8.1.17. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

8.1.18. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

8.1.19. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

8.1.20. Deve permitir operação em modo Mesh;

8.1.21. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;

8.1.22. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;

8.1.23. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);

8.1.24. Deve suportar OFDMA;

8.1.25. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4, 5 e 6GHz servindo clientes wireless 802.11ax

8.1.26. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;

8.1.27. Deve suportar BSS Coloring;

8.1.28. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;

8.1.29. Deve possuir sensibilidade mínima de -93dBm quando operando em 5 e 6GHz com MCS0 (HT20);

8.1.30. Deve possuir antenas internas ao equipamento com ganho mínimo de 4.5 dBi em 2.4GHz, 5GHz e 6GHz;

8.1.31. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;

8.1.32. Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4, 5 e 6 GHz;

8.1.33. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem

a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;

8.1.34. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;

8.1.35. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);

8.1.36. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 8 (oito) SSIDs com operação simultânea por radiofrequência;

8.1.37. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

8.1.38. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;

8.1.39. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

8.1.40. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

8.1.41. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

8.1.42. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

8.1.43. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

8.1.44. Deve implementar o padrão IEEE 802.11e;

8.1.45. Deve implementar o padrão IEEE 802.11h;

8.1.46. Deve implementar o padrão IEEE 802.3az;

8.1.47. Deve suportar ser gerenciado via SNMP;

8.1.48. Deve suportar consultas via REST API;

8.1.49. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;

8.1.50. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 50º C;

8.1.51. Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;

8.1.52. Deve possuir indicadores luminosos (LED) para indicação de status;

8.1.53. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;

8.1.54. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste Termo de Referência deverão ser fornecidos;

8.1.55. Deve possuir certificado emitido pela Wi-Fi Alliance;

8.1.56. Deve estar homologado pela ANATEL na data de execução do pregão;

8.2. **SWITCHES DE ACESSO 24 PORTAS POE– TIPO 1**

8.2.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

8.2.2. Deve ser compatível e gerenciado por qualquer modelo da controladora SEGURA de WLAN e LAN - Tipo 01, 02, 03 e 04 deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

8.2.3. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

8.2.4. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

8.2.5. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 185W;

8.2.6. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de

conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

8.2.7. Deve possuir 1 (uma) interface USB;

8.2.8. Deve possuir capacidade de comutação de pelo menos 120 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo);

8.2.9. Deve suportar 3500 (três mil e quinhentos) VLANs de acordo com o padrão IEEE 802.1Q;

8.2.10. Deve possuir tabela MAC com suporte a 30.000 endereços;

8.2.11. Deve operar com latência igual ou inferior à 1us (microsegundo);

8.2.12. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

8.2.13. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

8.2.14. Deve suportar a comutação de Jumbo Frames;

8.2.15. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

8.2.16. Deve implementar serviço de DHCP Relay;

8.2.17. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;

8.2.18. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);

8.2.19. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

8.2.20. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

8.2.21. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;

8.2.22. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

8.2.23. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

8.2.24. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

8.2.25. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

8.2.26. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

8.2.27. Deverá implementar mecanismo de proteção contra-ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

8.2.28. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

8.2.29. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

8.2.30. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

8.2.31. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

8.2.32. Deve suportar MAC Authentication Bypass (MAB);

8.2.33. Deve implementar RADIUS CoA (Change of Authorization);

8.2.34. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

8.2.35. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

8.2.36. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

8.2.37. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;

8.2.38. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);

8.2.39. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;

8.2.40. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

8.2.41. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

8.2.42. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

8.2.43. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

8.2.44. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

8.2.45. Deve permitir ser gerenciado através de IPv6;

8.2.46. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

8.2.47. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

8.2.48. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

8.2.49. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

8.2.50. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;

8.2.51. Deverá suportar ser configurado e monitorado através de REST API;

8.2.52. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);

8.2.53. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
Deve suportar temperatura de operação de até 45º Celsius;

8.2.54. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

8.2.55. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;

8.2.56. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;

8.3. **SWITCHES DE ACESSO DE 24 PORTAS POE – TIPO 2**

8.3.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

8.3.2. Deve ser compatível e gerenciado por qualquer modelo da controladora SEGURA de WLAN e LAN - Tipo 01, 02, 03 e 04 deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

8.3.3. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

8.3.4. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

8.3.5. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W;

8.3.6. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

8.3.7. Deve possuir 1 (uma) interface USB;

8.3.8. Deve possuir capacidade de comutação de pelo menos 125 Gbps e ser capaz de encaminhar até 185 Mpps (milhões de pacotes por segundo);

8.3.9. Deve suportar 3800 (três mil e oitocentos) VLANs de acordo com o padrão IEEE 802.1Q;

8.3.10. Deve possuir tabela MAC com suporte a 31.000 endereços;

8.3.11. Deve operar com latência igual ou inferior à 1us (microsegundo);
Deve implementar Flow Control baseado no padrão IEEE 802.3X;

8.3.12. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

8.3.13. Deve suportar a comutação de Jumbo Frames;

8.3.14. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

8.3.15. Deve implementar serviço de DHCP Relay;

8.3.16. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;

8.3.17. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);

8.3.18. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

8.3.19. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

8.3.20. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;

8.3.21. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

8.3.22. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

8.3.23. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

8.3.24. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

8.3.25. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

8.3.26. Deverá implementar mecanismo de proteção contra-ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

8.3.27. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

8.3.28. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

8.3.29. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

8.3.30. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

8.3.31. Deve suportar MAC Authentication Bypass (MAB);

8.3.32. Deve implementar RADIUS CoA (Change of Authorization);

8.3.33. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

8.3.34. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

8.3.35. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

8.3.36. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;
Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente

ficará armazenado na tabela de endereços MAC (MAC Table);

8.3.37. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;

8.3.38. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

8.3.39. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

8.3.40. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

8.3.41. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

8.3.42. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

8.3.43. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

8.3.44. Deve permitir ser gerenciado através de IPv6;

8.3.45. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

8.3.46. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

8.3.47. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

8.3.48. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

8.3.49. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;

8.3.50. Deverá suportar ser configurado e monitorado através de REST API;

8.3.51. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);

8.3.52. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;

8.3.53. Deve suportar temperatura de operação de até 45º Celsius;

8.3.54. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

8.3.55. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;

8.3.56. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;

8.4. **SWITCHES DE ACESSO 48 PORTAS POE– TIPO 1**

8.4.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

8.4.2. Deve ser compatível e gerenciado por qualquer modelo da controladora SEGURA de WLAN e LAN - Tipo 01, 02, 03 e 04 deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

8.4.3. Deve possuir 48 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

8.4.4. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

8.4.5. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W;

8.4.6. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

8.4.7. Deve possuir 1 (uma) interface USB;

8.4.8. Deve possuir capacidade de comutação de pelo menos 170 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo);

8.4.9. Deve suportar 3500 (três mil e quinhentos) VLANs de acordo com o padrão IEEE 802.1Q;

8.4.10. Deve possuir tabela MAC com suporte a 30.000 endereços;

8.4.11. Deve operar com latência igual ou inferior à 1us (microsegundo);

8.4.12. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

8.4.13. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

8.4.14. Deve suportar a comutação de Jumbo Frames;

8.4.15. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

8.4.16. Deve implementar serviço de DHCP Relay;

8.4.17. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;

8.4.18. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);

8.4.19. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

8.4.20. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

8.4.21. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;

8.4.22. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

8.4.23. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

8.4.24. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

8.4.25. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

8.4.26. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

8.4.27. Deverá implementar mecanismo de proteção contra-ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

8.4.28. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

8.4.29. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

8.4.30. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

8.4.31. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

8.4.32. Deve suportar MAC Authentication Bypass (MAB);

8.4.33. Deve implementar RADIUS CoA (Change of Authorization);

8.4.34. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

8.4.35. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

8.4.36. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

8.4.37. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;

8.4.38. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);

8.4.39. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;

8.4.40. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

8.4.41. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

8.4.42. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

8.4.43. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

8.4.44. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

8.4.45. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

8.4.46. Deve permitir ser gerenciado através de IPv6;

8.4.47. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

8.4.48. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

8.4.49. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

8.4.50. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

8.4.51. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;

8.4.52. Deverá suportar ser configurado e monitorado através de REST API;

8.4.53. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);

8.4.54. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;

8.4.55. Deve suportar temperatura de operação de até 45º Celsius;

8.4.56. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

8.4.57. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;

8.4.58. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;

8.5. **SWITCHES DE ACESSO 48 PORTAS POE– TIPO 2**

8.5.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

8.5.2. Deve ser compatível e gerenciado por qualquer modelo da controladora SEGURA de WLAN e LAN - Tipo 01, 02, 03 e 04 deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

8.5.3. Deve possuir 48 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

8.5.4. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

8.5.5. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 740W;

8.5.6. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

8.5.7. Deve possuir 1 (uma) interface USB;

8.5.8. Deve possuir capacidade de comutação de pelo menos 172 Gbps e ser capaz de encaminhar até 255 Mpps (milhões de pacotes por segundo);

8.5.9. Deve suportar 3500 (três mil e quinhentos) VLANs de acordo com o padrão IEEE 802.1Q;

8.5.10. Deve possuir tabela MAC com suporte a 31.000 endereços;

8.5.11. Deve operar com latência igual ou inferior à 1us (microsegundo);

8.5.12. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

8.5.13. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

8.5.14. Deve suportar a comutação de Jumbo Frames;

8.5.15. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

8.5.16. Deve implementar serviço de DHCP Relay;

8.5.17. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;

8.5.18. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);

8.5.19. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

8.5.20. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

8.5.21. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;

8.5.22. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

8.5.23. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

8.5.24. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

8.5.25. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

8.5.26. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

8.5.27. Deverá implementar mecanismo de proteção contra-ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

8.5.28. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

8.5.29. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

8.5.30. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

8.5.31. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

8.5.32. Deve suportar MAC Authentication Bypass (MAB);

8.5.33. Deve implementar RADIUS CoA (Change of Authorization);

8.5.34. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

8.5.35. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

8.5.36. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

8.5.37. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;

8.5.38. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);

8.5.39. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address

for removido da interface;

8.5.40. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

8.5.41. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

8.5.42. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

8.5.43. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

8.5.44. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

8.5.45. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

8.5.46. Deve permitir ser gerenciado através de IPv6;

8.5.47. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

8.5.48. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

8.5.49. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

8.5.50. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

8.5.51. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;

8.5.52. Deverá suportar ser configurado e monitorado através de REST API;

8.5.53. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);

8.5.54. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;

8.5.55. Deve suportar temperatura de operação de até 45º Celsius;

8.5.56. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

8.5.57. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;

8.5.58. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;

8.6. **SWITCH CONCENTRADOR DE 24 PORTAS**

8.6.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

8.6.2. Deve ser compatível e gerenciado por qualquer modelo da controladora SEGURA de WLAN e LAN - Tipo 01, 02, 03 e 04 deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

8.6.3. Deve possuir 24 (vinte e quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBaseX operando em 1GbE e 10GbE;

8.6.4. Adicionalmente, deve possuir 2 (dois) slots QSFP28 para conexão de fibras ópticas operando com velocidades de 40 e 100 Gigabit Ethernet;

8.6.5. Deve permitir a configuração das interfaces QSFP28 para que operem com conexões do tipo "breakout" ou "split", modo em que uma determinada porta 40GbE pode operar com 4 conexões em 10GbE. Deve permitir ainda que as portas 100GbE sejam divididas em 4 conexões de 25GbE;

8.6.6. Deverá ser entregue 1 (um) cabo DAC (Direct Atacch Cable) Breakout de 01 (uma) porta 100Gbps QSFP28 para 04 (quatro) portas 25Gbps SFP28 com transceivers e pelo menos 5 metros comprimento;

8.6.7. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

8.6.8. Deve possuir interface dedicada para gerenciamento local do tipo "out-of-band". Esta interface de gerenciamento deverá possuir porta 1000Base-T com conector RJ-45;

8.6.9. Deve possuir, no mínimo, 1 (uma) interface USB;

8.6.10. Deve possuir capacidade de comutação de pelo menos 860 Gbps (Gigabits por segundo) e ser capaz de encaminhar até 1.1 Bpps (bilhões de pacotes por segundo);

8.6.11. Deve suportar, pelo menos, 3800 (três mil e oitocentas) VLANs de acordo com o padrão IEEE 802.1Q;

8.6.12. Deve suportar Q-in-Q, recurso também conhecido como Stacked VLAN ou VLAN sobre VLAN em que é possível configurar duas TAGs de VLAN no mesmo frame;

8.6.13. Deve possuir tabela MAC com suporte a 60.000 endereços;

8.6.14. Deve operar com latência igual ou inferior à 1us (microssegundo);

8.6.15. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

8.6.16. Em conjunto com o Flow Control (IEEE 802.3x) o switch deverá, ao invés de enviar pause frames, definir um limite de banda que poderá ser recebida na interface quando o buffer estiver cheio. O switch deverá medir o volume de utilização do buffer para que o recebimento seja restaurado à capacidade máxima automaticamente;

8.6.17. Deve suportar o padrão IEEE 802.1Qbb (Priority-based Flow Control);

8.6.18. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

8.6.19. Deve suportar Multi-Chassis Link Agregation (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos os switches como uma única interface lógica;

8.6.20. Deve suportar a comutação de Jumbo Frames;

8.6.21. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;

8.6.22. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

8.6.23. Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIP, BGP, OSPF em IPv4 e OSPF em IPv6. É facultada a entrega de licenças caso o software exige licenciamento adicional para ativação dos protocolos;

8.6.24. Deve possuir hardware capaz de suportar roteamento multicast através do protocolo PIM-SSM (Protocol Independent Multicast - Source-Specific Multicast). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos;

8.6.25. Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo;

8.6.26. Deve suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exige licenciamento adicional para ativação do protocolo;

8.6.27. Deve ser capaz de criar múltiplas tabelas de roteamento através de VRF (Virtual Routing and Forwarding). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação deste recurso;

8.6.28. Deve implementar serviço de DHCP Server e DHCP Relay;

8.6.29. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) grupos;

8.6.30. Deve suportar MLD (Multicast Listener Discovery) Snooping para otimizar a transmissão de tráfego multicast em IPv6;

8.6.31. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN);

8.6.32. Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em outro equipamento através de RSPAN e ERSPAN;

8.6.33. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 30 (trinta) instâncias de Multiple Spanning Tree;

8.6.34. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

8.6.35. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;

8.6.36. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

8.6.37. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

8.6.38. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

8.6.39. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

8.6.40. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;

8.6.41. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

8.6.42. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

8.6.43. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF;

8.6.44. Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ);

8.6.45. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

8.6.46. Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados;

8.6.47. Deve implementar mecanismo de proteção contra-ataques do tipo spoofing para mensagens de IPv6 Router Advertisement;

8.6.48. Deverá implementar mecanismo de proteção contra-ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

8.6.49. Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

8.6.50. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

8.6.51. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

8.6.52. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

8.6.53. Deve suportar MAC Authentication Bypass (MAB);

8.6.54. Deve implementar RADIUS CoA (Change of Authorization);

8.6.55. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

8.6.56. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

8.6.57. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

8.6.58. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

8.6.59. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

8.6.60. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

8.6.61. Deve suportar o protocolo PTP (Precision Time Protocol);

8.6.62. Deve implementar Netflow, sFlow ou similar;

8.6.63. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

8.6.64. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

8.6.65. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

8.6.66. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

8.6.67. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

8.6.68. Deve permitir ser gerenciado através de IPv6;

8.6.69. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

8.6.70. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

8.6.71. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

8.6.72. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

8.6.73. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;

8.6.74. Deve possuir ferramenta para captura de pacotes que auxiliarão na identificação de problemas na rede. Deve permitir a utilização de filtros para selecionar o tráfego que deverá ser capturado e permitir a exportação dos pacotes através de arquivo .pcap para análise em software Wireshark;

8.6.75. Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash;

8.6.76. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;

8.6.77. Deve suportar temperatura de operação de até 40º Celsius;

8.6.78. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

8.6.79. Deve ser fornecido com fontes de alimentação redundantes do tipo hot-swap, com capacidade para operar em tensões de 110V e 220V;

8.6.80. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;

8.7. **SWITCH CONCENTRADOR DE 48 PORTAS**

8.7.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

8.7.2. Deve ser compatível e gerenciado por qualquer modelo da controladora SEGURA de WLAN e LAN - Tipo 01, 02, 03 e 04 deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

8.7.3. Deve possuir 48 (quarenta e oito) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE;

8.7.4. Adicionalmente, deve possuir 4 (quatro) slots QSFP28 para conexão de fibras ópticas operando com velocidades de 40 e 100 Gigabit Ethernet;

8.7.5. Deve permitir a configuração das interfaces QSFP28 para que operem com conexões do tipo "breakout" ou "split", modo em que uma determinada porta 40GbE pode operar com 4 conexões em 10GbE. Deve permitir ainda que as portas 100GbE sejam divididas em 4 conexões de 25GbE;

8.7.6. Deverá ser entregue 1 (um) cabo DAC (Direct Atacch Cable) Breakout de 01 (uma) porta 100Gbps QSFP28 para 04 (quatro) portas 25Gbps SFP28 com transceivers e pelo menos 5 metros comprimento;

8.7.7. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

8.7.8. Deve possuir interface dedicada para gerenciamento local do tipo "out-of-band". Esta interface de gerenciamento deverá possuir porta 1000Base-T com conector RJ-45;

8.7.9. Deve possuir, no mínimo, 1 (uma) interface USB;

8.7.10. Deve possuir capacidade de comutação de pelo menos 1.7 Tbps (terabits por segundo) e ser capaz de encaminhar até 1.4 Bpps (bilhões de pacotes por segundo);

8.7.11. Deve suportar, pelo menos, 3800 (três mil e oitocentos) VLANs de acordo com o padrão IEEE 802.1Q;

8.7.12. Deve suportar Q-in-Q, recurso também conhecido como Stacked VLAN ou VLAN sobre VLAN em que é possível configurar duas TAGs de VLAN no mesmo frame;

8.7.13. Deve possuir tabela MAC com suporte a 140.000 endereços;

8.7.14. Deve operar com latência igual ou inferior à 1us (microssegundo);

8.7.15. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

8.7.16. Em conjunto com o Flow Control (IEEE 802.3x) o switch deverá, ao invés de enviar pause frames, definir um limite de banda que poderá ser recebida na interface quando o buffer estiver cheio. O switch deverá medir o volume de utilização do buffer para que o recebimento seja restaurado à capacidade máxima automaticamente;

8.7.17. Deve suportar o padrão IEEE 802.1Qbb (Priority-based Flow Control);

8.7.18. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

8.7.19. Deve suportar Multi-Chassis Link Agregation (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos os switches como uma única interface lógica;

8.7.20. Deve suportar a comutação de Jumbo Frames;

8.7.21. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;

8.7.22. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

8.7.23. Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIP, BGP, OSPF em IPv4 e OSPF em IPv6. É facultada a entrega de licenças caso o software exige licenciamento adicional para ativação dos protocolos;

8.7.24. Deve possuir hardware capaz de suportar roteamento multicast através do protocolo PIM-SSM (Protocol Independent Multicast - Source-Specific Multicast). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos;

8.7.25. Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo;

8.7.26. Deve suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exige licenciamento adicional para ativação do protocolo;

8.7.27. Deve ser capaz de criar múltiplas tabelas de roteamento através de VRF (Virtual Routing and Forwarding). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação deste recurso;

8.7.28. Deve implementar serviço de DHCP Server e DHCP Relay;

8.7.29. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) grupos;

8.7.30. Deve suportar MLD (Multicast Listener Discovery) Snooping para otimizar a transmissão de tráfego multicast em IPv6;

8.7.31. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN);

8.7.32. Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em outro equipamento através de RSPAN e ERSPAN;

8.7.33. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 30 (trinta) instâncias de Multiple Spanning Tree;

8.7.34. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

8.7.35. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;

8.7.36. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

8.7.37. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

8.7.38. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

8.7.39. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

8.7.40. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;

8.7.41. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

8.7.42. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

8.7.43. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;

8.7.44. Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ);

8.7.45. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

8.7.46. Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados;

8.7.47. Deve implementar mecanismo de proteção contra-ataques do tipo spoofing para mensagens de IPv6 Router Advertisement;

8.7.48. Deverá implementar mecanismo de proteção contra-ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

8.7.49. Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

8.7.50. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

8.7.51. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

8.7.52. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

8.7.53. Deve suportar MAC Authentication Bypass (MAB);

8.7.54. Deve implementar RADIUS CoA (Change of Authorization);

8.7.55. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

8.7.56. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

8.7.57. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

8.7.58. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

8.7.59. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

8.7.60. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

8.7.61. Deve suportar o protocolo PTP (Precision Time Protocol);

8.7.62. Deve implementar Netflow, sFlow ou similar;

8.7.63. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

8.7.64. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

8.7.65. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

8.7.66. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

8.7.67. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

8.7.68. Deve permitir ser gerenciado através de IPv6;

8.7.69. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

8.7.70. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

8.7.71. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

8.7.72. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

8.7.73. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;

8.7.74. Deve possuir ferramenta para captura de pacotes que auxiliarão na identificação de problemas na rede. Deve permitir a utilização de filtros para selecionar o tráfego que deverá ser capturado e permitir a exportação dos pacotes através de arquivo .pcap para análise em software Wireshark;

8.7.75. Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash;

8.7.76. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou

alarme no switch;

8.7.77. Deve suportar temperatura de operação de até 40º Celsius;

8.7.78. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

8.7.79. Deve ser fornecido com fontes de alimentação redundantes do tipo hot-swap, com capacidade para operar em tensões de 110V e 220V;

8.7.80. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;

8.8. **CONTROLADORES SEGURO DE REDE WLAN E LAN**

8.8.1. **FUNCIONALIDADES GERAIS**

8.8.1.1. A solução deverá ser capaz de gerenciar os pontos de acesso sem fio deste termo, sendo permitido o atendimento através de composição com outras soluções do mesmo fabricante que possua gerência centralizada

8.8.1.2. Deve permitir a conexão de dispositivos sem fio que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;

8.8.1.3. Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;
A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;

8.8.1.4. Deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;

8.8.1.5. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;

8.8.1.6. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;

8.8.1.7. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso;

8.8.1.8. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

8.8.1.9. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

8.8.1.10. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

8.8.1.11. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;

8.8.1.12. A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;

8.8.1.13. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

8.8.1.14. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

8.8.1.15. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;

8.8.1.16. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;

8.8.1.17. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também

conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baeada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;

8.8.1.18. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;

8.8.1.19. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;

8.8.1.20. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;

8.8.1.21. A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;

8.8.1.22. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;

8.8.1.23. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;

8.8.1.24. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;

8.8.1.25. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

8.8.1.26. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

8.8.1.27. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

8.8.1.28. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;

8.8.1.29. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;
A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;

8.8.1.30. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;

8.8.1.31. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

8.8.1.32. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;

8.8.1.33. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;

8.8.1.34. A solução deve suportar a configuração do BLE (Blueooth Low Energy) nos pontos de acesso que tenham este recurso;

8.8.1.35. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;

8.8.1.36. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;

8.8.1.37. A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;

8.8.1.38. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;

8.8.1.39. A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;

8.8.1.40. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;

8.8.1.41. A solução deve permitir a configuração de regras de firewall baseadas em identidade, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;

8.8.1.42. Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;

8.8.1.43. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

8.8.1.44. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;

8.8.1.45. A solução deve permitir a configuração de múltplas chaves de autenticação PSK para utilização em um determinado SSID;

8.8.1.46. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;

8.8.1.47. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

8.8.1.48. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;

8.8.1.49. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

8.8.1.50. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;

8.8.1.51. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;

8.8.1.52. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;

8.8.1.53. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;

8.8.1.54. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;

8.8.1.55. A solução deve permitir a configuração do captive portal com endereço IPv6;

8.8.1.56. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;

8.8.1.57. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;

8.8.1.58. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;

8.8.1.59. A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;

8.8.1.60. A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;

8.8.1.61. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;

8.8.1.62. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;

8.8.1.63. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;

8.8.1.64. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;

8.8.1.65. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;

8.8.1.66. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;

8.8.1.67. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;

8.8.1.68. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;

8.8.1.69. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;

8.8.1.70. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);

8.8.1.71. A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;

8.8.1.72. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;

8.8.1.73. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;

8.8.1.74. A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;

8.8.1.75. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;

8.8.1.76. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;
A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;

8.8.1.77. A solução deve possuir ferramentas de diagnósticos e debug;

8.8.1.78. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;
A solução deve suportar comunicação com elementos externos através de REST API;

8.8.1.79. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;

8.8.1.80. Deve operar como ponto central para automação e gerenciamento dos switches deste termo, sendo permitido o atendimento através de composição de solução do mesmo fabricante que possua gerência centralizada para switches, devendo atender aos requisitos descritos abaixo:

8.8.1.81. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;

8.8.1.82. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;

8.8.1.83. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;

8.8.1.84. Deve montar a topologia da rede de maneira automática;

8.8.1.85. Deve ser capaz de configurar os switches da rede;

8.8.1.86. Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;

8.8.1.87. Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;

8.8.1.88. Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;

8.8.1.89. Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;

8.8.1.90. Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;

8.8.1.91. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;

8.8.1.92. Através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;

8.8.1.93. Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;
A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);

8.8.1.94. Deve ser capaz de configurar parâmetros SNMP dos switches;

8.8.1.95. A solução deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;

8.8.1.96. A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;

8.8.1.97. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;

8.8.1.98. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;

8.8.1.99. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;

8.8.1.100. Deve prover indicadores de saúde dos elementos críticos do ambiente;

8.8.1.101. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;

8.8.1.102. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;

8.8.2. **QOS, E PRIORIZAÇÃO DE TRÁFEGO**

8.8.2.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube e redes sociais, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

8.8.2.2. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:

8.8.2.3. Endereço de origem;

8.8.2.4. Endereço de destino;

8.8.2.5. Usuário e grupo;

8.8.2.6. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

8.8.2.7. Por porta;

8.8.2.8. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook, entre outros;

8.8.2.9. O QoS deve possibilitar a definição de fila de prioridade;

8.8.2.10. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

8.8.2.11. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

8.8.2.12. Suportar modificação de valores DSCP para o Diffserv;

8.8.2.13. Suportar priorização de tráfego usando informação de ToS (Type of Service);

8.8.2.14. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;

8.8.2.15. Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;

8.8.2.16. Deve possibilitar a definição de bandas distintas para download e upload;

8.8.3. **BALANCEAMENTO DE LINKS**

8.8.3.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

8.8.3.2. A solução deve ser capaz de agregar vários links em uma interface virtual;

8.8.3.3. A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc);

8.8.3.4. A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;

8.8.3.5. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;

8.8.3.6. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);

8.8.3.7. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego,

IP de origem e destino e Transbordo de link (Spillover).
A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:

8.8.3.8. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.

8.8.3.9. Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;

8.8.3.10. Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada;

8.8.3.11. Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;

8.8.3.12. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;
A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);

8.8.3.13. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc);

8.8.3.14. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;

8.8.3.15. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;

8.8.3.16. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;

8.8.3.17. A solução deve possuir recurso para controlar e corrigir erros (FEC) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;

8.8.3.18. A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;

8.8.3.19. A solução deve suportar nativamente conectores com clouds públicas;

8.8.3.20. Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;

8.8.3.21. A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);

8.8.3.22. Deve implementar balanceamento de link por hash do IP de origem;

8.8.3.23. Deve implementar balanceamento de link por hash do IP de origem e destino;

8.8.3.24. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

8.8.3.25. O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de Internet, e alternativamente funcionar como circuito Standby, onde apenas seja acionado na eventualidade de falha no link principal;

8.8.3.26. Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

8.8.3.27. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

8.8.3.28. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

8.8.4. **CRIPTOGRAFIA**

8.8.4.1. Suportar VPN Site-to-Site e Cliente-To-Site;

8.8.4.2. Suportar IPSec VPN;

8.8.4.3. A VPN IPSEc deve suportar 3DES;

8.8.4.4. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;

8.8.4.5. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

8.8.4.6. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

8.8.4.7. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

8.8.4.8. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;

8.8.4.9. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

8.8.4.10. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;

8.8.4.11. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

8.8.4.12. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

8.8.4.13. Atribuição de DNS nos clientes remotos de VPN;

8.8.4.14. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

8.8.4.15. Suportar leitura e verificação de CRL (Certificate Revocation List);

8.8.4.16. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;

8.8.4.17. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;

8.8.4.18. Deverá manter uma conexão segura com o portal durante a sessão;

8.8.4.19. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 8.1 (32 e 64 bit), Windows 10 (32 e 64 bit), Windows 11 e Mac OS X (v10.10 ou superior), CentOS (7 ou superior), Redhat (7 ou superior), Fedora (27 ou superior), Ubuntu (16.04 ou superior), e Android e iOS;

8.8.5. **IDENTIFICAÇÃO DE USUÁRIOS**

8.8.5.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, eDirectory e base de dados local;

8.8.5.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

8.8.5.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;

8.8.5.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

8.8.5.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

8.8.5.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

8.8.5.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no controlador (Captive Portal);

8.8.5.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

8.8.5.9. Deve suportar o envio e recebimento de credenciais via RADIUS;

8.8.5.10. Deve implementar a criação de grupos customizados de usuários no controlador seguro, baseado em atributos do LDAP/AD;

8.8.6. **FILTRAGEM DE DADOS E CONTEÚDO**

8.8.6.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

8.8.6.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

8.8.6.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

8.8.6.4. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;

8.8.6.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

8.8.6.6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

8.8.6.7. Possuir pelo menos 70 (setenta) categorias de URLs;

8.8.6.8. Deve possuir a função de exclusão de URLs do bloqueio;

8.8.6.9. Permitir a customização de página de bloqueio;

8.8.6.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

8.8.6.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

8.8.6.12. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;

8.8.6.13. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

8.8.6.14. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de controlador;

8.8.6.15. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

8.8.6.16. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

8.8.6.17. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

8.8.6.18. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

8.8.6.19. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

8.8.6.20. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

8.8.6.21. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

8.8.6.22. Deve permitir o bloqueio de vulnerabilidades;

8.8.6.23. Deve permitir o bloqueio de exploits conhecidos;

8.8.6.24. Deve incluir proteção contra-ataques de negação de serviços;

8.8.6.25. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

8.8.6.26. Detectar e bloquear a origem de portscans;

8.8.6.27. Bloquear ataques efetuados por worms conhecidos;

8.8.6.28. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

8.8.6.29. Possuir assinaturas para bloqueio de ataques de buffer overflow;

8.8.6.30. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

8.8.6.31. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

8.8.6.32. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

8.8.6.33. Identificar e bloquear comunicação com botnets;

8.8.6.34. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

8.8.6.35. Os eventos devem identificar o país de onde partiu a ameaça;

8.8.6.36. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

8.8.6.37. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

8.8.6.38. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

8.8.6.39. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante;

8.8.6.40. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante e caso o licenciamento/funcionalidade não seja permanente, o fornecedor deverá prover as funcionalidades por 36 (trinta e seis) meses;

8.8.6.41. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

8.8.6.42. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

8.8.6.43. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

8.8.6.44. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

8.8.6.45. Reconhecer pelo menos 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

8.8.6.46. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;

8.8.6.47. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

8.8.6.48. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

8.8.6.49. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

8.8.6.50. Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

8.8.6.51. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;

8.8.6.52. Identificar o uso de táticas evasivas via comunicações criptografadas;

8.8.6.53. Atualizar a base de assinaturas de aplicações automaticamente;

8.8.6.54. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

8.8.6.55. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

8.8.6.56. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

8.8.6.57. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

8.8.6.58. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

8.8.6.59. Deve alertar o usuário quando uma aplicação for bloqueada;

8.8.6.60. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

8.8.6.61. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

8.8.6.62. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;

8.8.6.63. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

8.8.6.64. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

8.8.6.65. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;

8.8.6.66. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

8.8.6.67. Deve permitir forçar o uso de portas específicas para determinadas aplicações;

8.8.7. **FILTRAGEM DE PACOTES DE REDE**

8.8.7.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

8.8.7.2. Os dispositivos de proteção de rede devem possuir suporte a Vlans;

8.8.7.3. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

8.8.7.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;

8.8.7.5. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

8.8.7.6. Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;

8.8.7.7. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

8.8.7.8. Deverá suportar sFlow ou Netflow;

8.8.7.9. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;

8.8.7.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;

8.8.7.11. Deve suportar o protocolo padrão da indústria VXLAN;

8.8.7.12. Deve implementar o protocolo ECMP;

8.8.7.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

8.8.7.14. Enviar log para sistemas de monitoração externos;

8.8.7.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;

8.8.7.16. Deve possui mecanismos de proteção anti-spoofing;

8.8.7.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);

8.8.7.18. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

8.8.7.19. Suportar OSPF graceful restart;

8.8.7.20. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

8.8.7.21. Deve suportar Modo Camada - 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

8.8.7.22. Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

8.8.7.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

8.8.7.24. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs eTabelas FIB;

8.8.7.25. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

8.8.7.26. O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;

8.8.7.27. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;

8.8.7.28. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;

8.8.7.29. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

8.8.7.30. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

8.8.7.31. Deverá suportar controle por zonas de segurança;

8.8.7.32. Deverá suportar controles de políticas por porta e protocolo;

8.8.7.33. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

8.8.7.34. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

8.8.7.35. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

8.8.7.36. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);

8.8.7.37. Deve decriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

8.8.7.38. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

8.8.7.39. Suporte a objetos e regras IPV6;

8.8.7.40. Suporte a objetos e regras multicast;

8.8.7.41. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

8.9. **CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 1**

8.9.1. Deve suportar, no mínimo, 500 (quinhentos) Mbps de performance de prevenção de ameaças, com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, firewall e Anti-Malware para tráfego IPv4 e IPv6;

8.9.2. Deve suportar, no mínimo, 600.000 (quinhentos mil) conexões simultâneas;

8.9.3. Deve suportar, no mínimo, 30.000 (trinta mil) novas conexões por segundo;

8.9.4. Deve Suportar, no mínimo, 04 (quatro) Gbps de throughput VPN IPSec;

8.9.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 180 (cento e oitenta) túneis ou peers do protocolo IKE de VPN IPSEC Site-to-Site simultâneos;

8.9.6. Deve permitir, no mínimo, 230 (duzentos e trinta) túneis de clientes VPN simultâneos;

8.9.7. Deve suportar, no mínimo, 01 (um) Gbps de throughput de IPS;

8.9.8. Deve suportar, no mínimo, 300 (trezentos) Mbps de throughput de Inspeção SSL;

8.9.9. Deve possuir, pelo menos, 05 (cinco) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;

8.9.10. Deve possuir 1(uma) interface de console RJ45;

8.9.11. Deve estar licenciado para gerenciar até 08 (oito) switches e 08 (oito) pontos de acesso sem fio simultaneamente em um único appliance;

8.9.12. Deve estar licenciado, sem custo adicional, no mínimo, para 5 (cinco) sistemas virtuais lógicos (Contextos) por controlador;

8.10. **CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 2**

8.10.1. Deve suportar, no mínimo, 2 (dois) Gbps de performance de prevenção de ameaças, com as seguintes funcionalidades habilitadas simultaneamente: controle de aplicação, IPS, firewall e Anti-Malware;

8.10.2. Deve suportar, no mínimo, 2.800.000 (doi milhões e oitocentos mil) conexões simultâneas;

8.10.3. Deve suportar, no mínimo, 120.000 (cento e vinte mil) novas conexões por segundo;

8.10.4. Deve Suportar, no mínimo, 20 (vinte) Gbps de throughput VPN IPSec;

8.10.5. Deve permitir, no mínimo, 180 (cento e oitenta) túneis ou peers do protocolo IKE de VPN IPSEC Site-to-Site simultâneos;

8.10.6. Deve permitir, no mínimo, 2.400 (dois mil e quatrocentos) túneis de clientes VPN simultâneos;

8.10.7. Deve suportar, no mínimo, 4 (quatro) Gbps de throughput de IPS;

8.10.8. Deve suportar, no mínimo, 2,5 (dois e meio) Gbps de throughput de Inspeção SSL;

8.10.9. Deve possuir, pelo menos, 8 (oito) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;

8.10.10. Deve possuir, pelo menos, 2 (duas) interfaces 10 Gigabit Ethernet 10GE SPF+

8.10.11. Deve possuir 1(uma) interface de console RJ45.

8.10.12. Deve possuir fonte embutida 100 – 240 VAC;

8.10.13. Deve estar licenciado para gerenciar até 20 (vinte) switches e 60 (sessenta) pontos de acesso sem fio simultaneamente em um único appliance;

8.10.14. Deve estar licenciado, no mínimo, para 10 (cinco) sistemas virtuais lógicos (Contextos) por appliances em cluster ativo-passivo;

8.11. **CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 3**

8.11.1. Deve suportar, no mínimo, 2,7 (dois virgula sete) Gbps de performance de prevenção de ameaças, com as seguintes funcionalidades habilitadas simultaneamente: controle de aplicação, IPS, firewall e Anti-Malware;

8.11.2. Deve suportar, no mínimo, 2.900.000 (dois milhões e novecentos mil) conexões simultâneas;

8.11.3. Deve suportar, no mínimo, 130.000 (cento e trinta mil) novas conexões por segundo;

8.11.4. Deve Suportar, no mínimo, 30 (trinta) Gbps de throughput VPN IPSec;

8.11.5. Deve permitir, no mínimo, 1.800 (hum mil e oitocentos) túneis ou peers do protocolo IKE de VPN IPSEC Site-to-Site simultâneos;

8.11.6. Deve permitit, no mínimo, 10.000 (dez mil) túneis de clientes VPN simultâneos;

8.11.7. Deve suportar, no mínimo, 5 (cinco) Gbps de throughput de IPS;

8.11.8. Deve suportar, no mínimo, 2,8 (dois virgula oito) Gbps de throughput de Inspeção SSL;

8.11.9. Deve possuir, pelo menos, 16 (dezesseis) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;

8.11.10. Deve possuir, pelo menos, 2 (duas) interfaces 10 Gigabit Ethernet 10GE Base-T ou SPF+

8.11.11. Deve possuir, pelo menos, 6 (seis) interfaces com suporte a SFP de 1 Gigabit Ethernet;

8.11.12. Deve suportar, pelo menos , 1 (um) interface de gerencia RJ45

8.11.13. Deve possuir 1(uma) interface de console RJ45

8.11.14. Deve possuir fontes redundantes 100 – 240 VAC

8.11.15. Deve estar licenciado para gerenciar até 30 (trinta) switches e 60 (sessenta) pontos de acesso sem fio simultaneamente em um único appliance;

8.11.16. Deve estar licenciado, no mínimo, para 10 (cinco) sistemas virtuais lógicos (Contextos) por appliances em cluster ativo-passivo;

8.12. **CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 4**

8.12.1. Deve suportar, no mínimo, 10 (dez) Gbps de performance de prevenção de ameaças, com as seguintes funcionalidades habilitadas simultaneamente: controle de aplicação, IPS, firewall e Anti-Malware;

8.12.2. Deve suportar, no mínimo, 7.500.000 (sete milhões e quinhentos mil) conexões simultâneas;

8.12.3. Deve suportar, no mínimo, 500.000 (quinhentas mil) novas conexões por segundo;

8.12.4. Deve Suportar, no mínimo, 50 (cinquenta) Gbps de throughput VPN IPSec;

8.12.5. Deve permitir, no mínimo, 1.800 (hum mil e oitocentos) túneis ou peers do protocolo IKE de VPN IPSEC Site-to-Site simultâneos;

8.12.6. Deve permitir, no mínimo, 10.000 (dez mil) túneis de clientes VPN simultâneos;

8.12.7. Deve suportar, no mínimo, 12 (doze) Gbps de throughput de IPS;

8.12.8. Deve suportar, no mínimo, 8 (oito) Gbps de throughput de Inspeção SSL;

8.12.9. Deve possuir, pelo menos, 16 (dezesseis) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;

8.12.10. Deve possuir, pelo menos, 2 (duas) interfaces 10 Gigabit Ethernet 10GE Base-T / SPF+ ou 1 Gigabit SFP;

8.12.11. Deve possuir, pelo menos, 6 (seis) interfaces com suporte a SFP de 1 Gigabit Ethernet;

8.12.12. Deve possuir, pelo menos , 2 (duas) interfaces 25GE SFP28;

8.12.13. Deve suportar, pelo menos , 1 (um) interface de gerencia RJ45;

8.12.14. Deve possuir 1(uma) interface de console RJ45;

8.12.15. Deve possuir fontes redundantes hot swap 100 – 240 VAC;

8.12.16. Deve estar licenciado para gerenciar até 90 (noventa) switches e 500 (quinhentos) pontos de acesso sem fio simultaneamente em um único appliance;

8.12.17. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (cinco) sistemas virtuais lógicos (Contextos) por appliances em cluster ativo-passivo.

8.13. **SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÕES COM LICENÇAS PARA CADA 100 DISPOSITIVOS**

8.13.1. Deve estar dimensionado e licenciado para gerenciar o total de dispositivos através de múltiplas licenças para cada 100 (cem) dispositivos considerando os modelos ofertados neste processo atendendo aos requisitos deste Item;

8.13.2. A solução de gerenciamento centralizado poderá ser ofertada em formato de appliance físico ou appliance virtual, e caso ofertado em formato virtual, será responsabilidade da contratante a disponibilização dos recursos de hardware e software (hypervisor) necessário para funcionamento da solução;

8.13.3. Caso a solução seja entregue em appliance virtual, deverá ser compatível com Hypervisors: VMware ESXi 6.5, Microsoft Hyper-V 2012 / 2016/ 2019 e KVM no Redhat 7.1;

8.13.4. Caso a solução seja entregue em appliance virtual, não deve possuir limite na quantidade de múltiplas vCPU;

8.13.5. Caso a solução seja entregue em appliance virtual, não deve possuir limite para suporte a expansão de memória RAM;

8.13.6. Caso a solução seja ofertada em appliance físico, deverá ser em hardware do próprio fabricante;

8.13.7. A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;

8.13.8. Possibilitar a criação e administração de políticas de filtragem de contéudo, URL e balanceamento de Links e todas as demais funcionalidades solicitadas neste Termo de Referência;

8.13.9. Como parte da visibilidade dos dispositivos gerenciados centralmente, a solução deve ter visibilidade das verificações de saúde do link, desempenho da aplicação, utilização da largura de banda e conformidade com o nível de serviço definido;

8.13.10. Deve ter a capacidade de permitir o provisionamento de comunidades VPN e monitorar as conexões VPN de todos os dispositivos gerenciados a partir de uma única console, além de exibir sua localização geográfica em um mapa;

8.13.11. Permitir criar templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;

8.13.12. Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.

8.13.13. A solução deve permitir o uso de APIs para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;

8.13.14. Deverá garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;

8.13.15. Permitir acesso concorrente de administradores e que seja definida uma cadeia de aprovação das alterações realizadas;

8.13.16. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

8.13.17. Permitir usar palavras chaves ou cores para facilitar identificação de regras;

8.13.18. Permitir localizar em quais regras um objeto (ex. computador, serviço, etc.) está sendo utilizado;

8.13.19. Atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;

8.13.20. Permitir criação de regras que fiquem ativas em horário definido;

8.13.21. Permitir criação de regras com data de expiração;

8.13.22. Realizar o backup das configurações para permitir o retorno de uma configuração salva;

8.13.23. Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras, ou garantir que esta exigência seja plenamente atendida por meio diverso.

8.13.24. Gerar alertas automáticos via Email, SNMP e Syslog;

8.13.25. Deve ser permitido ao administrador transferir os backups para um servidor FTP, SCP ou SFTP.

8.13.26. Permitir backup das configurações e rollback de configuração para a última configuração salva;

8.13.27. Deve possibilitar a visualização e comparação de configurações atuais e configurações anteriores;

8.13.28. Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;

8.13.29. Deve suportar a distribuição e instalação remota de novas versões de software dos equipamentos, de forma remota e centralizada;

8.13.30. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;

8.13.31. Deve suportar autenticação de administradores em base local e de modo remoto por meio de RADIUS, LDAP, TACACS+ e PKI.

8.13.32. A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta.

8.13.33. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances.

8.13.34. Deve suportar o gerenciamento de pontos de acesso de forma centralizada.

8.13.35. Deve suportar o gerenciamento centralizado de switches.

8.13.36. A solução deve possuir garantia e atualizações ao software durante a vigência do contrato;

8.13.37. **SOLUÇÃO CENTRALIZADO DE LOGS E RELATÓRIOS COM LICENÇAS PARA ATÉ 25GB/LOG DIA**

8.13.38. Deve suportar o acesso via SSH, WEB (HTTPS) para gerenciamento da solução;

8.13.39. A solução deve suportar receber, no mínimo, com pacotes de licenças de 25 (cinco) GB de logs diários;

8.13.40. A solução de gerenciamento centralizado poderá ser ofertada em formato de appliance físico ou appliance virtual, e caso ofertado em formato virtual, será responsabilidade da contratante a disponibilização dos recursos de hardware e software (hypervisor) necessário para funcionamento da solução;

8.13.41. Caso a solução seja entregue em appliance virtual, deverá ser compatível com Hypervisors: VMware ESXi 6.5, Microsoft Hyper-V 2012 / 2016/ 2019 e KVM no Redhat 7.1;

8.13.42. Caso a solução seja entregue em appliance virtual, não deve possuir limite na quantidade de múltiplas vCPU;

8.13.43. Caso a solução seja entregue em appliance virtual, não deve possuir limite para suporte a expansão de memória RAM;

8.13.44. Caso a solução seja ofertada em appliance físico, deverá ser em hardware do próprio fabricante;

8.13.45. A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;

8.13.46. A solução deverá ser capaz de armazenar logs por no mínimo 12 (doze) meses;

8.13.47. Permitir acesso simultâneo à administração, bem como criar pelo menos 2 (dois) perfis para administração e monitoramento;

8.13.48. Possuir suporte para SNMP versão 2 e 3;

8.13.49. Permitir a virtualização do gerenciamento e administração dos dispositivos, onde cada administrador tem acesso apenas aos equipamentos autorizados;

8.13.50. Deve permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;

8.13.51. Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;

8.13.52. Suporte a autenticação de usuários de acesso à plataforma via LDAP, Radius ou TACACS+;

8.13.53. Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;

8.13.54. Deve permitir gerar alertas de eventos a partir de logs recebidos;

8.13.55. A solução deve ter relatórios predefinidos;

8.13.56. Permitir importação e exportação de relatórios

8.13.57. Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;

8.13.58. Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;

8.13.59. Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;

8.13.60. Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;

8.13.61. Deve ter a capacidade de personalizar a capa dos relatórios obtidos;

8.13.62. Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;

8.13.63. Deve ter a capacidade de criar relatórios no formato HTML, CSV, XML e PDF;

8.13.64. Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;

8.13.65. Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;

8.13.66. Deve possuir mecanismos de remoção automática para logs antigos;

8.13.67. Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;

8.13.68. Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;

8.13.69. Permitir o envio por e-mail relatórios automaticamente;

8.13.70. Deve permitir que o relatório seja enviado por Email para o destinatário específico;

8.13.71. Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;

8.13.72. Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;

8.13.73. Deve permitir o uso de filtros nos relatórios;

8.13.74. Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;

8.13.75. Permitir especificar o idioma dos relatórios criados;

8.13.76. Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;

8.13.77. Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;

8.13.78. Deve permitir o envio automático dos logs para um servidor FTP externo a solução;

8.13.79. Deve permitir exportar os logs no formato CSV;

8.13.80. Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;

8.13.81. Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;

8.13.82. Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;

8.13.83. Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;

8.13.84. Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;

8.13.85. Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;

8.13.86. Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;

8.13.87. Deve permitir visualizar em tempo real os logs recebidos;

8.13.88. Deve permitir o encaminhamento de log no formato syslog e CEF (Common Event Format);

8.13.89. Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;

8.13.90. Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;

8.13.91. Deve possuir um painel de operações que monitore as principais ameaças à segurança da sua rede;

8.13.92. Deve possuir um painel de operações que monitora o envolvimento do usuário e o uso suspeito da web em sua rede;

8.13.93. Deve possuir um painel de operações que monitora o tráfego da rede, aplicativos e sites web;

8.13.94. Deve possuir um painel de operações que monitoram a atividade da VPN em sua rede;

8.13.95. Deve possuir um painel de operações que monitoram o desempenho dos recursos locais da solução (CPU, Memória);

8.13.96. Deve permitir a criação de painéis personalizados para monitorar operações de segurança e rede;

8.13.97. Deve possuir relatório de uso de aplicações e mídias sociais;

8.13.98. Deve possuir relatório de prevenção de perda de dados (DLP);

8.13.99. Deve possuir relatório de VPN, Prevenção de Intrusão (IPS), análise de ameaças cibernéticas;

8.13.100. Deve possuir relatório diário resumido de eventos e incidentes de segurança;

8.13.101. Deve possuir um relatório de tráfego DNS e e-mail;

8.13.102. Deve possuir relatório das 10 principais aplicações utilizadas na rede;

8.13.103. Deve possuir relatório dos 10 principais sites web utilizados na rede;

8.13.104. Deve possibilitar a visibilidade da utilização do balanceamento inteligente de links (SD-WAN), mostrando informações de utilização das regras por aplicação, largura de banda e níveis de serviços dos links (latência, Jitter e descarte de pacotes);

8.13.105. Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados, o monitoramento de computadores que estão potencialmente comprometidas ou usuários com uso de rede suspeito;

8.13.106. Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados pelos computadores, atribuição de pontuações de risco que definem os vereditos dos níveis de comprometimento como baixo, médio ou alto;

8.13.107. Deve suportar a análise detalhada dos computadores comprometidos e exibir os detalhes das ameaças detectadas;

8.13.108. Deve suportar recursos de automação (playbooks) que, por meio de integrações com soluções de firewall, endpoint, Email, ITSM e eventos pré-determinados, possa tomar ações automáticas visando mitigar riscos;

8.13.109. Deve permitir a correlação de eventos, provendo painéis diversos, bem como possibilitar a criação de novas telas para visualizar os recursos de rede e segurança;

8.13.110. Deve informar o tráfego maior consumo de origem do ambiente wireless;

8.13.111. Deve informar o tráfego maior consumo de destino do ambiente wireless

8.13.112. Deve informar o sumário de uso da rede wireless;

8.13.113. Deve informar a relação de pontos de acessos autorizados;

8.13.114. Deve informar a relação de pontos de acessos não autorizados;

8.13.115. Deve informar a relação dos SSIDs mais utilizados na ordem de bytes enviados e recebidos;

8.13.116. Deve informar a relação dos SSIDs mais utilizados na ordem de tempo por uso de banda;

8.13.117. Deve informar a relação dos clientes wifi por consumo de banda e sessão;

8.13.118. Deve gerar e permitir configurar ações para os seguintes eventos da rede sem fio: atualizações e alertas de AP, incluindo alteração de status de AP e detecção de AP falso ou não autorizado, alteração de status de cliente sem fio adicionado/removido/permitido ou negado, relação sinal-ruído (SNR) ruim/razoável/boa, status de SSID ativo/inativo.

8.14. **TRANSCEIVER SPF-LX**

8.14.0.1. Transceiver SFP compatível com o padrão 1GBase-LX para fibras ópticas multimodos, (fibra OM3) para até 100 metros;

8.14.0.2. Deve possuir conector Duplex LC;

8.14.0.3. Deve ter velocidade de 1GbE;

8.14.0.4. Os transceivers/Dacs a serem fornecidos devem ser totalmente compatíveis com o fabricante do equipamento comprovado em documento técnico a ser apresentado na habilitação;

8.14.0.5. **TRANSCEIVER SFP+ 10GBASE-SR**

8.14.0.6. Transceiver SFP+ para conexão de fibras ópticas multimodo;

8.14.0.7. Deve ser compatível com o padrão 10GBase-SR para fibras ópticas de até 300m (fibra OM3) e fibras ópticas de até 400m (fibra OM4);

8.14.0.8. Deve ter velocidade de 10GbE;

8.14.0.9. Os transceivers/Dacs a serem fornecidos devem ser totalmente compatíveis com o fabricante do equipamento comprovado em documento técnico a ser apresentado na habilitação.

8.14.1. **TRANSCEIVER 25GE, módulo tipo SFP28-SR**

8.14.1.1. Deve ser compatível com o padrão 25GBase-SR para fibras ópticas de até 100m fibras ópticas (fibra OM4);

8.14.1.2. Deve ter velocidade de 25GbE;

8.14.1.3. Deve possuir conector duplex LC;

8.14.1.4. Os transceivers/Dacs a serem fornecidos devem ser totalmente compatíveis com o fabricante do equipamento comprovado em documento técnico a ser apresentado na habilitação.

8.14.2. **TRANSCEIVER 100 GE, módulo tipo QSFP28-SR**

8.14.2.1. Deve ser compatível com o padrão 100GBase-SR para fibras ópticas de até 100m fibras ópticas multi-modo (fibra OM4);

8.14.2.2. Deve ter velocidade de 100GbE;

8.14.2.3. Deve possuir conector duplex LC;

8.14.2.4. Os transceivers/Dacs a serem fornecidos devem ser totalmente compatíveis com o fabricante do equipamento comprovado em documento técnico a ser apresentado na habilitação.

8.15. **SERVIÇOS DE INSTALAÇÃO DE PONTO DE ACESSO**

8.15.1. Entende-se por instalação a montagem física dos equipamentos e acessórios fornecidos, bem como a configuração lógica de todos os equipamentos, incluindo atualização de firmware em última versão disponibilizada pelo fabricante e softwares envolvidos, contemplando a fixação do equipamento, energização e conexão do mesmo para a ativação da conectividade de rede (exceto elétrica), de acordo com o cenário requerido pela CONTRATANTE;

8.15.2. São de responsabilidade da CONTRATADA, entre outras atividades: a desembalagem dos equipamentos, a instalação física incluindo a fixação dos Pontos de Acesso nos locais adequados, a ativação e configuração lógica dos

mesmos, as conexões de rede, atualização de softwares recomendadas e os testes de pré-operação dos Pontos de Acesso, conforme os requisitos e condições descritos neste documento.

8.15.3. A CONTRATANTE deverá providenciar a infraestrutura elétrica caso seja necessário.

8.15.4. Em casos em que o local de instalação não possuir estrutura de pontos de rede lógica para ligação dos equipamentos do contratante, será contratado tal serviço ao respectivo item deste Termo de Referência;

8.15.5. O serviço de instalação deverá ser executado pela CONTRATADA durante o horário comercial compreendido das 8h00 às 18h00, de segunda a sexta-feira, devendo eventualmente, atender à CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de implementações que necessitem ser executados nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente, e de comum acordo entre as partes;

8.15.6. Caberá a CONTRATADA todo o processo de planejamento, a instalação, a configuração, a integração, os testes, a migração e a compatibilidade dos PRODUTOS, que deverão ser integrados à infraestrutura de Tecnologia de Informação existente no local de instalação dos Pontos de Acesso;

8.15.7. A equipe técnica da CONTRATADA que irá executar a instalação deverá trabalhar sob orientação e supervisão direta do profissional responsável pela coordenação das atividades de implantação;

8.15.8. A CONTRATADA, depois de concluído o serviço de instalação dos Pontos de Acesso, deverá realizar, com o acompanhamento dos técnicos da CONTRATANTE, testes de pré-operação para constatar que os Pontos de Acesso foram instalados de acordo com o cenário requerido pela CONTRATANTE;

8.15.9. Todos os instrumentos/equipamentos necessários para a execução do serviço e testes de aceitação do serviço serão fornecidos pela CONTRATADA;

8.15.10. A falta de instalação completa de um ou mais Pontos de Acesso constitui-se em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de instalação de Pontos de Acesso correspondente, enquanto perdurar a instalação incompleta;

8.15.11. Concluídos a instalação e os testes de funcionalidade, a CONTRATADA, deverá elaborar a "DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO" contendo todas as informações da implantação: aspectos e arquitetura implantada, configuração, descrição das características e recursos utilizados, testes e integração aos ambientes de redes locais da instalação;

8.15.12. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA;

8.15.13. A documentação deverá ser entregue em via impressa ou em meio digital;

8.15.14. A documentação será validada pela equipe técnica da CONTRATANTE;

8.15.15. Toda informação manuseada durante a instalação, configuração e testes são de uso exclusivo e restrito da CONTRATANTE. A CONTRATADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE;

8.15.16. A CONTRATADA deverá apresentar a relação nominal dos profissionais, explicitando as respectivas atribuições na execução dos serviços. Para comprovar a qualificação exigida, deverão ser anexados os certificados técnicos dos referidos profissionais, emitidos pelo Fabricante dos Pontos de Acesso;

8.15.17. Caso seja constatada, durante o exercício dos serviços contratados, a falta de qualificação ou inadequação do profissional da CONTRATADA, a mesma deverá proceder a sua imediata substituição a partir da solicitação da CONTRATANTE.

8.16. **SERVIÇO DE INSTALAÇÃO DE SWITCHES DE ACESSO 24 PORTAS POE – TIPO 1 E TIPO 2**

8.16.1. Entende-se por instalação a montagem física dos equipamentos e acessórios fornecidos, bem como a configuração lógica de todos os equipamentos, incluindo atualização de firmware em última versão disponibilizada pelo fabricante e softwares envolvidos, contemplando a fixação do equipamento, energização e conexão do mesmo para a ativação da conectividade de rede (exceto elétrica), de acordo com o cenário requerido pela CONTRATANTE;

8.16.2. São de responsabilidade da CONTRATADA, entre outras atividades: a desembalagem dos equipamentos, a instalação física incluindo a fixação dos Switches nos locais adequados, a ativação e configuração lógica dos mesmos, as conexões de rede, atualização de softwares recomendadas e os testes de pré-operação dos Switches, conforme os requisitos e condições descritos neste documento;

8.16.3. A CONTRATANTE providenciará toda a infraestrutura elétrica e a infraestrutura de dados nos locais de instalação dos Switches;

8.16.4. O serviço de instalação deverá ser executado pela CONTRATADA durante o horário comercial compreendido das 8h00 às 18h00, de segunda a sexta-feira, devendo eventualmente, atender à CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de implementações que necessitem ser executados nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente, e de comum acordo entre as partes;

8.16.5. Caberá a CONTRATADA todo o processo de planejamento, a instalação, a configuração, a integração, os testes, a migração e a compatibilidade dos PRODUTOS, que deverão ser integrados à infraestrutura de Tecnologia de Informação existente no local de instalação dos Switches;

8.16.6. A equipe técnica da CONTRATADA que irá executar a instalação deverá trabalhar sob orientação e supervisão direta do profissional responsável pela coordenação das atividades de implantação;

8.16.7. A CONTRATADA, depois de concluído o serviço de instalação dos Switches, deverá realizar, com o acompanhamento dos técnicos da CONTRATANTE, testes de pré-operação para constatar que os Switches foram instalados de acordo com o cenário requerido pela CONTRATANTE;

8.16.8. Todos os instrumentos/equipamentos necessários para a execução do serviço e testes de aceitação do serviço serão fornecidos pela CONTRATADA;

8.16.9. A CONTRATADA deverá elaborar e manter, no local de serviço, Relatório de Instalação (RI), em formulário timbrado próprio da CONTRATADA, com registros das atividades, anotações de irregularidades encontradas e de todas as ocorrências relativas à execução do contrato, o qual será feito na periodicidade definida pela fiscalização da CONTRATANTE, em 2 (duas) vias, sendo a primeira para uso da CONTRATANTE e a segunda para a CONTRATADA, devendo ser assinado conjuntamente pelo representante da CONTRATADA e pela fiscalização da CONTRATANTE;

8.16.10. A falta de instalação completa de um ou mais Switches constitui-se em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de instalação de Switches correspondente, enquanto perdurar a instalação incompleta;

8.16.11. Concluídos a instalação e os testes de funcionalidade, a CONTRATADA, deverá elaborar a "DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO" contendo todas as informações da implantação: aspectos de arquitetura implantada, configuração, descrição das características e recursos utilizados, testes e integração aos ambientes de redes locais da instalação;

8.16.12. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA;
A documentação deverá ser entregue em via impressa ou em meio digital;

8.16.13. A documentação será validada pela equipe técnica da CONTRATANTE;

8.16.14. Toda informação manuseada durante a instalação, configuração e testes são de uso exclusivo e restrito da CONTRATANTE. A CONTRATADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE;

8.16.15. A CONTRATADA deverá apresentar a relação nominal dos profissionais, explicitando as respectivas atribuições na execução dos serviços. Para comprovar a qualificação exigida, deverão ser anexados os certificados técnicos dos referidos profissionais, emitidos pelo Fabricante dos Switches;

8.16.16. Caso seja constatada, durante o exercício dos serviços contratados, a falta de qualificação ou inadequação do profissional da CONTRATADA, a mesma deverá proceder a sua imediata substituição a partir da solicitação da CONTRATANTE.

8.17. **SERVIÇOS DE INSTALAÇÃO DE SWITCHES DE ACESSO 48 PORTAS POE – TIPO 1 E TIPO 2**

8.17.1. Entende-se por instalação a montagem física dos equipamentos e acessórios fornecidos, bem como a configuração lógica de todos os equipamentos, incluindo atualização de firmware em última versão disponibilizada pelo fabricante e softwares envolvidos, contemplando a fixação do equipamento, energização e conexão do mesmo para a ativação da conectividade de rede (exceto elétrica), de acordo com o cenário requerido pela CONTRATANTE;

8.17.2. São de responsabilidade da CONTRATADA, entre outras atividades: a desembalagem dos equipamentos, a instalação física incluindo a fixação dos Switches nos locais adequados, a ativação e configuração lógica dos mesmos, as conexões de rede, atualização de softwares recomendadas e os testes de pré-operação dos Switches, conforme os requisitos e condições descritos neste documento;

8.17.3. A CONTRATANTE providenciará toda a infraestrutura elétrica e a infraestrutura de dados nos locais de instalação dos Switches;
O serviço de instalação deverá ser executado pela CONTRATADA durante o horário comercial compreendido das 8h00 às 18h00, de segunda a sexta-feira, devendo eventualmente, atender à CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de implementações que necessitem ser executados nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente, e de comum acordo entre as partes;

8.17.4. Caberá a CONTRATADA todo o processo de planejamento, a instalação, a configuração, a integração, os testes, a migração e a compatibilidade dos PRODUTOS, que deverão ser integrados à infraestrutura de Tecnologia de Informação existente no local de instalação dos Switches;

8.17.5. A equipe técnica da CONTRATADA que irá executar a instalação deverá trabalhar sob orientação e supervisão direta do profissional responsável pela coordenação das atividades de implantação;

8.17.6. A CONTRATADA, depois de concluído o serviço de instalação dos Switches, deverá realizar, com o acompanhamento dos técnicos da CONTRATANTE, testes de pré-operação para constatar que os Switches foram instalados

de acordo com o cenário requerido pela CONTRATANTE;

8.17.7. Todos os instrumentos/equipamentos necessários para a execução do serviço e testes de aceitação do serviço serão fornecidos pela CONTRATADA;

8.17.8. A CONTRATADA deverá elaborar e manter, no local de serviço, Relatório de Instalação (RI), em formulário timbrado próprio da CONTRATADA, com registros das atividades, anotações de irregularidades encontradas e de todas as ocorrências relativas à execução do contrato, o qual será feito na periodicidade definida pela fiscalização da CONTRATANTE, em 2 (duas) vias, sendo a primeira para uso da CONTRATANTE e a segunda para a CONTRATADA, devendo ser assinado conjuntamente pelo representante da CONTRATADA e pela fiscalização da CONTRATANTE;

8.17.9. A falta de instalação completa de um ou mais Switches constitui-se em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de instalação de Switches correspondente, enquanto perdurar a instalação incompleta;

8.17.10. Concluídos a instalação e os testes de funcionalidade, a CONTRATADA, deverá elaborar a "DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO" contendo todas as informações da implantação: aspectos de arquitetura implantada, configuração, descrição das características e recursos utilizados, testes e integração aos ambientes de redes locais da instalação;

8.17.11. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA;

8.17.12. A documentação deverá ser entregue em via impressa ou em meio digital;

8.17.13. A documentação será validada pela equipe técnica da CONTRATANTE;

8.17.14. Toda informação manuseada durante a instalação, configuração e testes são de uso exclusivo e restrito da CONTRATANTE. A CONTRATADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE;

8.17.15. A CONTRATADA deverá apresentar a relação nominal dos profissionais, explicitando as respectivas atribuições na execução dos serviços. Para comprovar a qualificação exigida, deverão ser anexados os certificados técnicos dos referidos profissionais, emitidos pelo Fabricante dos Switches;

8.17.16. Caso seja constatada, durante o exercício dos serviços contratados, a falta de qualificação ou inadequação do profissional da CONTRATADA, a mesma deverá proceder a sua imediata substituição a partir da solicitação da CONTRATANTE.

8.18. **SERVIÇOS DE INSTALAÇÃO DE SWITCH CONCENTRADOR de 24 PORTAS E 48 PORTAS**

8.18.1. Entende-se por instalação a montagem física dos equipamentos e acessórios fornecidos, bem como a configuração lógica de todos os equipamentos, incluindo atualização de firmware em última versão disponibilizada pelo fabricante e softwares envolvidos, contemplando a fixação do equipamento, energização e conexão do mesmo para a ativação da conectividade de rede (exceto elétrica), de acordo com o cenário requerido pela CONTRATANTE;

8.18.2. São de responsabilidade da CONTRATADA, entre outras atividades: a desembalagem dos equipamentos, a instalação física incluindo a fixação dos Switches nos locais adequados, a ativação e configuração lógica dos mesmos, as conexões de rede, atualização de softwares recomendadas e os testes de pré-operação dos Switches, conforme os requisitos e condições descritos neste documento;

8.18.3. A CONTRATANTE providenciará toda a infraestrutura elétrica e a infraestrutura de dados nos locais de instalação dos Switches;

8.18.4. O serviço de instalação deverá ser executado pela CONTRATADA durante o horário comercial compreendido das 8h00 às 18h00, de segunda a sexta-feira, devendo eventualmente, atender à CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de implementações que necessitem ser executados nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente, e de comum acordo entre as partes;

8.18.5. Caberá a CONTRATADA todo o processo de planejamento, a instalação, a configuração, a integração, os testes, a migração e a compatibilidade dos PRODUTOS, que deverão ser integrados à infraestrutura de Tecnologia de Informação existente no local de instalação dos Switches;

8.18.6. A equipe técnica da CONTRATADA que irá executar a instalação deverá trabalhar sob orientação e supervisão direta do profissional responsável pela coordenação das atividades de implantação;

8.18.7. A CONTRATADA, depois de concluído o serviço de instalação dos Switches, deverá realizar, com o acompanhamento dos técnicos da CONTRATANTE, testes de pré-operação para constatar que os Switches foram instalados de acordo com o cenário requerido pela CONTRATANTE;

8.18.8. Todos os instrumentos/equipamentos necessários para a execução do serviço e testes de aceitação do serviço serão fornecidos pela CONTRATADA;

8.18.9. A CONTRATADA deverá elaborar e manter, no local de serviço, Relatório de Instalação (RI), em formulário timbrado próprio da CONTRATADA, com registros das atividades, anotações de irregularidades encontradas e de todas as

ocorrências relativas à execução do contrato, o qual será feito na periodicidade definida pela fiscalização da CONTRATANTE, em 2 (duas) vias, sendo a primeira para uso da CONTRATANTE e a segunda para a CONTRATADA, devendo ser assinado conjuntamente pelo representante da CONTRATADA e pela fiscalização da CONTRATANTE;

8.18.10. A falta de instalação completa de um ou mais Switches constitui-se em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de instalação de Switches correspondente, enquanto perdurar a instalação incompleta;

8.18.11. Concluídos a instalação e os testes de funcionalidade, a CONTRATADA, deverá elaborar a "DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO" contendo todas as informações da implantação: aspectos de arquitetura implantada, configuração, descrição das características e recursos utilizados, testes e integração aos ambientes de redes locais da instalação;

8.18.12. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA;

8.18.13. A documentação deverá ser entregue em via impressa ou em meio digital;

8.18.14. A documentação será validada pela equipe técnica da CONTRATANTE;

8.18.15. Toda informação manuseada durante a instalação, configuração e testes são de uso exclusivo e restrito da CONTRATANTE. A CONTRATADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE;

8.18.16. A CONTRATADA deverá apresentar a relação nominal dos profissionais, explicitando as respectivas atribuições na execução dos serviços. Para comprovar a qualificação exigida, deverão ser anexados os certificados técnicos dos referidos profissionais, emitidos pelo Fabricante dos Switches;

8.18.17. Caso seja constatada, durante o exercício dos serviços contratados, a falta de qualificação ou inadequação do profissional da CONTRATADA, a mesma deverá proceder a sua imediata substituição a partir da solicitação da CONTRATANTE.

8.19. **SERVIÇOS DE INSTALAÇÃO DE CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 1**

8.19.1. Entende-se por instalação a montagem física dos equipamentos e acessórios fornecidos, bem como a configuração lógica inicial de todos os equipamentos (startup), incluindo atualização de firmware em última versão disponibilizada pelo fabricante e softwares envolvidos, contemplando a fixação do equipamento, energização e conexão do mesmo para a ativação da conectividade de rede (exceto elétrica), de acordo com o cenário requerido pela CONTRATANTE;

8.19.2. São de responsabilidade da CONTRATADA, entre outras atividades: a desembalagem dos equipamentos, a instalação física incluindo a fixação dos Firewalls nos locais adequados, a ativação e configuração lógica dos mesmos, as conexões de rede, atualização de softwares recomendadas e os testes de pré-operação dos Firewalls, conforme os requisitos e condições descritos neste documento;

8.19.3. As atividades de startup deverão contemplar:

8.19.4. Atualização de firmware para o último nível disponibilizado do fabricante;

8.19.5. Configuração de tabela de roteamento para acesso à internet e a rede da CONTRATANTE;

8.19.6. Configuração de políticas de bloqueio padrão de portas TCP/UDP, baseada na definição da equipe de TI;

8.19.7. Ajustes e testes de acesso;

8.19.8. A CONTRATANTE deverá providenciar a infraestrutura elétrica caso seja necessário;

8.19.9. Em casos em que o local de instalação não possuir estrutura de pontos de rede lógica para ligação dos equipamentos do contratante, será contratado tal serviço em referência ao respectivo material deste Termo de Referência;

8.19.10. O serviço de instalação deverá ser executado pela CONTRATADA durante o horário comercial compreendido das 8h00 às 18h00, de segunda a sexta-feira, devendo eventualmente, atender à CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de implementações que necessitem ser executados nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente, e de comum acordo entre as partes;

8.19.11. Caberá a CONTRATADA todo o processo de planejamento, a instalação, a configuração, a integração, os testes, a migração e a compatibilidade dos PRODUTOS, que deverão ser integrados à infraestrutura de Tecnologia de Informação existente no local de instalação dos Firewalls;

8.19.12. A equipe técnica da CONTRATADA que irá executar a instalação deverá trabalhar sob orientação e supervisão direta do profissional responsável pela coordenação das atividades de implantação;

8.19.13. A CONTRATADA, depois de concluído o serviço de instalação dos Firewalls, deverá realizar, com o acompanhamento dos técnicos da CONTRATANTE, testes de pré-operação para constatar que os Firewalls foram instalados de acordo com o cenário requerido pela CONTRATANTE;

8.19.14. Todos os instrumentos/equipamentos necessários para a execução do serviço e testes de aceitação do serviço serão fornecidos pela CONTRATADA;

8.19.15. A falta de instalação completa de um ou mais equipamentos constitui-se em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de instalação de Firewall correspondente, enquanto perdurar a instalação incompleta;

8.19.16. Concluídos a instalação e os testes de funcionalidade, a CONTRATADA, deverá elaborar a "DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO" contendo todas as informações da implantação: aspectos e arquitetura implantada, configuração, descrição das características e recursos utilizados, testes e integração aos ambientes de redes locais da instalação;

8.19.17. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA;

8.19.18. A documentação deverá ser entregue em via impressa ou em meio digital.

8.19.19. A documentação será validada pela equipe técnica da CONTRATANTE;

8.19.20. Toda informação manuseada durante a instalação, configuração e testes são de uso exclusivo e restrito da CONTRATANTE. A CONTRATADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE;

8.19.21. A CONTRATADA deverá possuir em seu quadro de funcionários pelo menos 1 (um) técnico de TI certificado pelo Fabricante dos Firewalls na solução ofertada;

8.19.22. Os serviços de instalação deverão ser executados e/ou supervisionados por técnico certificado pelo Fabricante dos Firewalls na solução proposta;

8.19.23. A CONTRATADA deverá apresentar a relação nominal dos profissionais, explicitando as respectivas atribuições na execução dos serviços. Para comprovar a qualificação exigida, deverão ser anexados os certificados técnicos dos referidos profissionais, emitidos pelo Fabricante dos Firewalls;

8.19.24. Caso seja constatada, durante o exercício dos serviços contratados, a falta de qualificação ou inadequação do profissional da CONTRATADA, a mesma deverá proceder a sua imediata substituição a partir da solicitação da CONTRATANTE;

8.20. **SERVIÇOS DE INSTALAÇÃO DE CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 2**

8.20.1. Entende-se por instalação a montagem física dos equipamentos e acessórios fornecidos, bem como a configuração lógica inicial de todos os equipamentos (startup), incluindo atualização de firmware em última versão disponibilizada pelo fabricante e softwares envolvidos, contemplando a fixação do equipamento, energização e conexão do mesmo para a ativação da conectividade de rede (exceto elétrica), de acordo com o cenário requerido pela CONTRATANTE;

8.20.2. São de responsabilidade da CONTRATADA, entre outras atividades: a desembalagem dos equipamentos, a instalação física incluindo a fixação dos Firewalls nos locais adequados, a ativação e configuração lógica dos mesmos, as conexões de rede, atualização de softwares recomendadas e os testes de pré-operação dos Firewalls, conforme os requisitos e condições descritos neste documento;

8.20.3. As atividades de startup deverão contemplar:

8.20.4. Atualização de firmware para o último nível disponibilizado do fabricante;

8.20.5. Configuração de tabela de roteamento para acesso à internet e a rede da CONTRATANTE;

8.20.6. Configuração de políticas de bloqueio padrão de portas TCP/UDP, baseada na definição da equipe de TI;

8.20.7. Ajustes e testes de acesso;

8.20.8. A CONTRATANTE deverá providenciar a infraestrutura elétrica caso seja necessário;

8.20.9. Em casos em que o local de instalação não possuir estrutura de pontos de rede lógica para ligação dos equipamentos do contratante, será contratado tal serviço em referência ao respectivo material deste Termo de Referência;

8.20.10. O serviço de instalação deverá ser executado pela CONTRATADA durante o horário comercial compreendido das 8h00 às 18h00, de segunda a sexta-feira, devendo eventualmente, atender à CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de implementações que necessitem ser executados nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente, e de comum acordo entre as partes;

8.20.11. Caberá a CONTRATADA todo o processo de planejamento, a instalação, a configuração, a integração, os testes, a migração e a compatibilidade dos PRODUTOS, que deverão ser integrados à infraestrutura de Tecnologia de Informação existente no local de instalação dos Firewalls;

8.20.12. A equipe técnica da CONTRATADA que irá executar a instalação deverá trabalhar sob orientação e supervisão direta do profissional responsável pela coordenação das atividades de implantação;

8.20.13. A CONTRATADA, depois de concluído o serviço de instalação dos Firewalls, deverá realizar, com o acompanhamento dos técnicos da CONTRATANTE, testes de pré-operação para constatar que os Firewalls foram instalados de acordo com o cenário requerido pela CONTRATANTE;

8.20.14. Todos os instrumentos/equipamentos necessários para a execução do serviço e testes de aceitação do serviço serão fornecidos pela CONTRATADA;

8.20.15. A falta de instalação completa de um ou mais equipamentos constitui-se em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de instalação de Firewall correspondente, enquanto perdurar a instalação incompleta;

8.20.16. Concluídos a instalação e os testes de funcionalidade, a CONTRATADA, deverá elaborar a "DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO" contendo todas as informações da implantação: aspectos e arquitetura implantada, configuração, descrição das características e recursos utilizados, testes e integração aos ambientes de redes locais da instalação;

8.20.17. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA;

8.20.18. A documentação deverá ser entregue em via impressa ou em meio digital.

8.20.19. A documentação será validada pela equipe técnica da CONTRATANTE;

8.20.20. Toda informação manuseada durante a instalação, configuração e testes são de uso exclusivo e restrito da CONTRATANTE. A CONTRATADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE;

8.20.21. A CONTRATADA deverá possuir em seu quadro de funcionários pelo menos 1 (um) técnico de TI certificado pelo Fabricante dos Firewalls na solução ofertada;

8.20.22. Os serviços de instalação deverão ser executados e/ou supervisionados por técnico certificado pelo Fabricante dos Firewalls na solução proposta;

8.20.23. A CONTRATADA deverá apresentar a relação nominal dos profissionais, explicitando as respectivas atribuições na execução dos serviços. Para comprovar a qualificação exigida, deverão ser anexados os certificados técnicos dos referidos profissionais, emitidos pelo Fabricante dos Firewalls;

8.20.24. Caso seja constatada, durante o exercício dos serviços contratados, a falta de qualificação ou inadequação do profissional da CONTRATADA, a mesma deverá proceder a sua imediata substituição a partir da solicitação da CONTRATANTE;

8.21. **SERVIÇOS DE INSTALAÇÃO DE CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 3**

8.21.1. Entende-se por instalação a montagem física dos equipamentos e acessórios fornecidos, bem como a configuração lógica inicial de todos os equipamentos (startup), incluindo atualização de firmware em última versão disponibilizada pelo fabricante e softwares envolvidos, contemplando a fixação do equipamento, energização e conexão do mesmo para a ativação da conectividade de rede (exceto elétrica), de acordo com o cenário requerido pela CONTRATANTE;

8.21.2. São de responsabilidade da CONTRATADA, entre outras atividades: a desembalagem dos equipamentos, a instalação física incluindo a fixação dos Firewalls nos locais adequados, a ativação e configuração lógica dos mesmos, as conexões de rede, atualização de softwares recomendadas e os testes de pré-operação dos Firewalls, conforme os requisitos e condições descritos neste documento;

8.21.3. As atividades de startup deverão contemplar:

8.21.4. Atualização de firmware para o último nível disponibilizado do fabricante;

8.21.5. Configuração de tabela de roteamento para acesso à internet e a rede da CONTRATANTE;

8.21.6. Configuração de políticas de bloqueio padrão de portas TCP/UDP, baseada na definição da equipe de TI;

8.21.7. Ajustes e testes de acesso;

8.21.8. A CONTRATANTE deverá providenciar a infraestrutura elétrica caso seja necessário;

8.21.9. Em casos em que o local de instalação não possuir estrutura de pontos de rede lógica para ligação dos equipamentos do contratante, será contratado tal serviço em referência ao respectivo material deste Termo de Referência;

8.21.10. O serviço de instalação deverá ser executado pela CONTRATADA durante o horário comercial compreendido das 8h00 às 18h00, de segunda a sexta-feira, devendo eventualmente, atender à CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de implementações que necessitem ser executados nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente, e de comum acordo entre as partes;

8.21.11. Caberá a CONTRATADA todo o processo de planejamento, a instalação, a configuração, a integração, os testes, a migração e a compatibilidade dos PRODUTOS, que deverão ser integrados à infraestrutura de Tecnologia de

Informação existente no local de instalação dos Firewalls;

8.21.12. A equipe técnica da CONTRATADA que irá executar a instalação deverá trabalhar sob orientação e supervisão direta do profissional responsável pela coordenação das atividades de implantação;

8.21.13. A CONTRATADA, depois de concluído o serviço de instalação dos Firewalls, deverá realizar, com o acompanhamento dos técnicos da CONTRATANTE, testes de pré-operação para constatar que os Firewalls foram instalados de acordo com o cenário requerido pela CONTRATANTE;

8.21.14. Todos os instrumentos/equipamentos necessários para a execução do serviço e testes de aceitação do serviço serão fornecidos pela CONTRATADA;

8.21.15. A falta de instalação completa de um ou mais equipamentos constitui-se em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de instalação de Firewall correspondente, enquanto perdurar a instalação incompleta;

8.21.16. Concluídos a instalação e os testes de funcionalidade, a CONTRATADA, deverá elaborar a "DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO" contendo todas as informações da implantação: aspectos e arquitetura implantada, configuração, descrição das características e recursos utilizados, testes e integração aos ambientes de redes locais da instalação;

8.21.17. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA;

8.21.18. A documentação deverá ser entregue em via impressa ou em meio digital.

8.21.19. A documentação será validada pela equipe técnica da CONTRATANTE;

8.21.20. Toda informação manuseada durante a instalação, configuração e testes são de uso exclusivo e restrito da CONTRATANTE. A CONTRATADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE;

8.21.21. A CONTRATADA deverá possuir em seu quadro de funcionários pelo menos 1 (um) técnico de TI certificado pelo Fabricante dos Firewalls na solução ofertada;

8.21.22. Os serviços de instalação deverão ser executados e/ou supervisionados por técnico certificado pelo Fabricante dos Firewalls na solução proposta;

8.21.23. A CONTRATADA deverá apresentar a relação nominal dos profissionais, explicitando as respectivas atribuições na execução dos serviços. Para comprovar a qualificação exigida, deverão ser anexados os certificados técnicos dos referidos profissionais, emitidos pelo Fabricante dos Firewalls;

8.21.24. Caso seja constatada, durante o exercício dos serviços contratados, a falta de qualificação ou inadequação do profissional da CONTRATADA, a mesma deverá proceder a sua imediata substituição a partir da solicitação da CONTRATANTE;

8.22. **SERVIÇOS DE INSTALAÇÃO DE CONTROLADOR SEGURO DE REDE WLAN E LAN TIPO 4**

8.22.1. Entende-se por instalação a montagem física dos equipamentos e acessórios fornecidos, bem como a configuração lógica inicial de todos os equipamentos (startup), incluindo atualização de firmware em última versão disponibilizada pelo fabricante e softwares envolvidos, contemplando a fixação do equipamento, energização e conexão do mesmo para a ativação da conectividade de rede (exceto elétrica), de acordo com o cenário requerido pela CONTRATANTE;

8.22.2. São de responsabilidade da CONTRATADA, entre outras atividades: a desembalagem dos equipamentos, a instalação física incluindo a fixação dos Firewalls nos locais adequados, a ativação e configuração lógica dos mesmos, as conexões de rede, atualização de softwares recomendadas e os testes de pré-operação dos Firewalls, conforme os requisitos e condições descritos neste documento;

8.22.3. As atividades de startup deverão contemplar:

8.22.4. Atualização de firmware para o último nível disponibilizado do fabricante;

8.22.5. Configuração de tabela de roteamento para acesso à internet e a rede da CONTRATANTE;

8.22.6. Configuração de políticas de bloqueio padrão de portas TCP/UDP, baseada na definição da equipe de TI;

8.22.7. Ajustes e testes de acesso;

8.22.8. A CONTRATANTE deverá providenciar a infraestrutura elétrica caso seja necessário;

8.22.9. Em casos em que o local de instalação não possuir estrutura de pontos de rede lógica para ligação dos equipamentos do contratante, será contratado tal serviço em referência ao respectivo material deste Termo de Referência;

8.22.10. O serviço de instalação deverá ser executado pela CONTRATADA durante o horário comercial compreendido das 8h00 às 18h00, de segunda a sexta-feira, devendo eventualmente, atender à CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de implementações que necessitem ser executados nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente, e de comum acordo

entre as partes;

8.22.11. Caberá a CONTRATADA todo o processo de planejamento, a instalação, a configuração, a integração, os testes, a migração e a compatibilidade dos PRODUTOS, que deverão ser integrados à infraestrutura de Tecnologia de Informação existente no local de instalação dos Firewalls;

8.22.12. A equipe técnica da CONTRATADA que irá executar a instalação deverá trabalhar sob orientação e supervisão direta do profissional responsável pela coordenação das atividades de implantação;

8.22.13. A CONTRATADA, depois de concluído o serviço de instalação dos Firewalls, deverá realizar, com o acompanhamento dos técnicos da CONTRATANTE, testes de pré-operação para constatar que os Firewalls foram instalados de acordo com o cenário requerido pela CONTRATANTE;

8.22.14. Todos os instrumentos/equipamentos necessários para a execução do serviço e testes de aceitação do serviço serão fornecidos pela CONTRATADA;

8.22.15. A falta de instalação completa de um ou mais equipamentos constitui-se em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de instalação de Firewall correspondente, enquanto perdurar a instalação incompleta;

8.22.16. Concluídos a instalação e os testes de funcionalidade, a CONTRATADA, deverá elaborar a "DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO" contendo todas as informações da implantação: aspectos e arquitetura implantada, configuração, descrição das características e recursos utilizados, testes e integração aos ambientes de redes locais da instalação;

8.22.17. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA;

8.22.18. A documentação deverá ser entregue em via impressa ou em meio digital.

8.22.19. A documentação será validada pela equipe técnica da CONTRATANTE;

8.22.20. Toda informação manuseada durante a instalação, configuração e testes são de uso exclusivo e restrito da CONTRATANTE. A CONTRATADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE;

8.22.21. A CONTRATADA deverá possuir em seu quadro de funcionários pelo menos 1 (um) técnico de TI certificado pelo Fabricante dos Firewalls na solução ofertada;

8.22.22. Os serviços de instalação deverão ser executados e/ou supervisionados por técnico certificado pelo Fabricante dos Firewalls na solução proposta;

8.22.23. A CONTRATADA deverá apresentar a relação nominal dos profissionais, explicitando as respectivas atribuições na execução dos serviços. Para comprovar a qualificação exigida, deverão ser anexados os certificados técnicos dos referidos profissionais, emitidos pelo Fabricante dos Firewalls;

8.22.24. Caso seja constatada, durante o exercício dos serviços contratados, a falta de qualificação ou inadequação do profissional da CONTRATADA, a mesma deverá proceder a sua imediata substituição a partir da solicitação da CONTRATANTE;

8.23. **SERVIÇOS DE INSTALAÇÃO GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÕES PARA DISPOSITIVOS**

8.23.1. Entende-se por instalação lógica inicial de todos os softwares (startup), incluindo atualização de firmware/software em última versão disponibilizada pelo fabricante para os softwares envolvidos, e conexão do mesmo para a ativação da conectividade de rede (exceto elétrica), de acordo com o cenário requerido pela CONTRATANTE.

8.23.2. As atividades de startup deverão contemplar:

8.23.3. Atualização de firmware para o último nível disponibilizado do fabricante;

8.23.4. Configuração de tabela de roteamento para acesso à internet e a rede da CONTRATANTE;

8.23.5. Configuração de políticas de bloqueio padrão de portas TCP/UDP, baseada na definição da equipe de TI;

8.23.6. Ajustes e testes de acesso;

8.23.7. A CONTRATANTE deverá providenciar a infraestrutura elétrica caso seja necessário;

8.23.8. O serviço de instalação deverá ser executado pela CONTRATADA durante o horário comercial compreendido das 8h00 às 18h00, de segunda a sexta-feira, devendo eventualmente, atender à CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de implementações que necessitem ser executados nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente, e de comum acordo entre as partes;

8.23.9. Caberá a CONTRATADA todo o processo de planejamento, a instalação, a configuração, a integração, os testes, a migração e a compatibilidade dos PRODUTOS, que deverão ser integrados à infraestrutura de Tecnologia de Informação existente no local de instalação do Software de Gerenciamento Centralizado;

8.23.10. A equipe técnica da CONTRATADA que irá executar a instalação deverá trabalhar sob orientação e supervisão direta do profissional responsável pela coordenação das atividades de implantação.

8.23.11. A CONTRATADA, depois de concluído o serviço de instalação do Software de Gerenciamento Centralizado, deverá realizar, com o acompanhamento dos técnicos da CONTRATANTE, testes de pré-operação para constatar que os produtos foram instalados de acordo com o cenário requerido pela CONTRATANTE.

8.23.12. Todos os instrumentos/equipamentos necessários para a execução do serviço e testes de aceitação do serviço serão fornecidos pela CONTRATADA.

8.23.13. A falta de instalação completa de um ou mais produtos constitui-se em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de instalação do Software de Gerenciamento Centralizado correspondente, enquanto perdurar a instalação incompleta.

8.23.14. Concluídos a instalação e os testes de funcionalidade, a CONTRATADA, deverá elaborar a "DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO" contendo todas as informações da implantação: aspectos e arquitetura implantada, configuração, descrição das características e recursos utilizados, testes e integração aos ambientes de redes locais da instalação.

8.23.15. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA.
A documentação deverá ser entregue em via impressa ou em meio digital.

8.23.16. A documentação será validada pela equipe técnica da CONTRATANTE.

8.23.17. Toda informação manuseada durante a instalação, configuração e testes são de uso exclusivo e restrito da CONTRATANTE. A CONTRATADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE.

8.23.18. A CONTRATADA deverá possuir em seu quadro de funcionários pelo menos 1 (um) técnico de TI certificado pelo Fabricante do Software de Gerenciamento Centralizado na solução ofertada.

8.23.19. Os serviços de instalação deverão ser executados e/ou supervisionados por técnico certificado pelo Fabricante do Software de Gerenciamento Centralizado na solução proposta.

8.23.20. A CONTRATADA deverá apresentar a relação nominal dos profissionais, explicitando as respectivas atribuições na execução dos serviços. Para comprovar a qualificação exigida, deverão ser anexados os certificados técnicos dos referidos profissionais, emitidos pelo Fabricante do Software de Gerenciamento Centralizado;

8.23.21. Caso seja constatada, durante o exercício dos serviços contratados, a falta de qualificação ou inadequação do profissional da CONTRATADA, a mesma deverá proceder a sua imediata substituição a partir da solicitação da CONTRATANTE.

8.24. **SERVIÇOS DE INSTALAÇÃO DA SOLUÇÃO CENTRALIZADA DE LOGS E RELATÓRIOS COM LICENÇAS PARA ATÉ 25GB/LOG DIA**

8.24.1. Entende-se por instalação lógica inicial de todos os softwares (startup), incluindo atualização de firmware/software em última versão disponibilizada pelo fabricante para os softwares envolvidos, e conexão do mesmo para a ativação da conectividade de rede (exceto elétrica), de acordo com o cenário requerido pela CONTRATANTE.

8.24.2. As atividades de startup deverão contemplar:

8.24.3. Atualização de firmware para o último nível disponibilizado do fabricante;

8.24.4. Configuração de tabela de roteamento para acesso à internet e a rede da CONTRATANTE;

8.24.5. Configuração de políticas de bloqueio padrão de portas TCP/UDP, baseada na definição da equipe de TI;

8.24.6. Ajustes e testes de acesso;

8.24.7. A CONTRATANTE deverá providenciar a infraestrutura elétrica caso seja necessário;

8.24.8. O serviço de instalação deverá ser executado pela CONTRATADA durante o horário comercial compreendido das 8h00 às 18h00, de segunda a sexta-feira, devendo eventualmente, atender à CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de implementações que necessitem ser executados nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente, e de comum acordo entre as partes;

8.24.9. Caberá a CONTRATADA todo o processo de planejamento, a instalação, a configuração, a integração, os testes, a migração e a compatibilidade dos PRODUTOS, que deverão ser integrados à infraestrutura de Tecnologia de Informação existente no local de instalação do Software de Gerenciamento Centralizado;

8.24.10. A equipe técnica da CONTRATADA que irá executar a instalação deverá trabalhar sob orientação e supervisão direta do profissional responsável pela coordenação das atividades de implantação.

8.24.11. A CONTRATADA, depois de concluído o serviço de instalação do Software de Gerenciamento Centralizado, deverá realizar, com o acompanhamento dos técnicos da CONTRATANTE, testes de pré-operação para constatar que os

produtos foram instalados de acordo com o cenário requerido pela CONTRATANTE.

8.24.12. Todos os instrumentos/equipamentos necessários para a execução do serviço e testes de aceitação do serviço serão fornecidos pela CONTRATADA.

8.24.13. A falta de instalação completa de um ou mais produtos constitui-se em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de instalação do Software de Gerenciamento Centralizado correspondente, enquanto perdurar a instalação incompleta.

8.24.14. Concluídos a instalação e os testes de funcionalidade, a CONTRATADA, deverá elaborar a "DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO" contendo todas as informações da implantação: aspectos e arquitetura implantada, configuração, descrição das características e recursos utilizados, testes e integração aos ambientes de redes locais da instalação.

8.24.15. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA.

8.24.16. A documentação deverá ser entregue em via impressa ou em meio digital.

8.24.17. A documentação será validada pela equipe técnica da CONTRATANTE.

8.24.18. Toda informação manuseada durante a instalação, configuração e testes são de uso exclusivo e restrito da CONTRATANTE. A CONTRATADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE.

8.24.19. A CONTRATADA deverá possuir em seu quadro de funcionários pelo menos 1 (um) técnico de TI certificado pelo Fabricante do Software de Gerenciamento Centralizado na solução ofertada.

8.24.20. Os serviços de instalação deverão ser executados e/ou supervisionados por técnico certificado pelo Fabricante do Software de Gerenciamento Centralizado na solução proposta.

8.24.21. A CONTRATADA deverá apresentar a relação nominal dos profissionais, explicitando as respectivas atribuições na execução dos serviços. Para comprovar a qualificação exigida, deverão ser anexados os certificados técnicos dos referidos profissionais, emitidos pelo Fabricante do Software de Gerenciamento Centralizado;

8.24.22. Caso seja constatada, durante o exercício dos serviços contratados, a falta de qualificação ou inadequação do profissional da CONTRATADA, a mesma deverá proceder a sua imediata substituição a partir da solicitação da CONTRATANTE.

8.25. **SERVIÇOS DE TREINAMENTO DAS SOLUÇÕES (POR SOLUÇÃO)**

8.25.1. TREINAMENTO DE REDE SEM FIO, REDE DE ACESSO E SEGURANÇA

8.25.2. Deverá ser fornecido treinamento presencial de toda solução proposta para a equipe da CONTRATANTE;

8.25.3. Carga horária mínima de 80 (oitenta) horas;

8.25.4. Turma para 8 (oito) participantes indicados pela CONTRATANTE;

8.25.5. O instrutor deverá ser certificado pela fabricante dos produtos e para realizar os treinamentos, este deverá ser comprovado mediante apresentação de certificado expedido pela fabricante da solução de segurança da informação;

8.25.6. O material a ser fornecido no treinamento deverá ser o material certificado pelo próprio fabricante, não serão aceitas cópias de apostilas;

8.25.7. Toda a infraestrutura, os custos de material (apostilas, manuais, etc.), alimentação (coffee break), instrutor (deslocamento, hospedagem e vencimentos) ficará a cargo da CONTRATADA;

8.25.8. O treinamento deverá conter em seu conteúdo questões práticas e teóricas sobre o funcionamento e os recursos da solução proposta;

8.25.9. Deverá ser incluído, caso exista, módulos básicos e avançados de modo a cobrir todas as funcionalidades da solução ofertada;

8.25.10. Os cursos deverão ser realizados em horários e data a serem acordados pela CONTRATADA e CONTRATANTE;

8.25.11. A CONTRATADA deverá ofertar as instalações do treinamento na localidade da CONTRATANTE, ou onde está indicar, para a realização dos treinamentos com os requisitos mínimos de infraestrutura de sala de treinamento;

8.25.12. Disponibilizar certificados de conclusão para todos os participantes.

8.26. **SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (POR SOLUÇÃO) - ITENS 29, 30, 31, 32, 33, 34, 35 E 36.**

8.26.1. A Contratada deverá prover suporte técnico, e atualização de versões das licenças fornecidas, pelo prazo de trinta e seis meses, contados da data do recebimento definitivo dessas licenças;

8.26.2. Inclui todas as atualizações de versões, pequenas atualizações de release e reparos de defeitos (bug fixing patches);

8.26.3. A garantia é uma cobertura legal ou contratual oferecida pelo fabricante, que garante o reparo ou substituição de produtos em caso de defeitos de fabricação ou falhas durante um determinado período após a aquisição.

8.26.4. Os serviços de suporte técnico aos produtos deverão incluir, dentre outros:

8.26.5. Orientações sobre uso, configuração e instalação do software ofertado;

8.26.6. Questões sobre compatibilidade e interoperabilidade do produto ofertado (hardware e software);

8.26.7. Interpretação da documentação do software ofertado;

8.26.8. Orientações para identificar a causa de uma falha de software;

8.26.9. Orientação para solução de problemas de “performance” e “tuning” das configurações do software ofertado;

8.26.10. Cobre problemas inerentes ao produto, como defeitos de fabricação ou falhas de desempenho que não sejam causadas por mau uso do consumidor. Não inclui serviços adicionais, como manutenção regular.

8.26.11. Orientação quanto às melhores práticas para implementação do software adquirido;

8.26.12. Apoio na recuperação de ambientes em caso de panes ou perda de dados;

8.26.13. Apoio para execução de procedimentos de atualização para novas versões do software instalado;

8.26.14. A contratada deverá gerar relatório mensal, analítico e sintético, indicando todos os eventos relevantes ocorridos durante o período de execução do mesmo a ser entregue até o 5 (quinto) dia útil do mês subsequente.

8.26.15. Durante o período do contrato o suporte técnico e manutenção, a Contratada deverá atender às solicitações da SESAU/RO, em qualquer horário, respeitando as condições e níveis de serviços especificados a seguir:

8.26.16. SEVERIDADE ALTA: Aplicado quando há indisponibilidade do ambiente tecnológico;

8.26.17. SEVERIDADE MÉDIA: Aplicado quando há falha no uso dos softwares, estando ainda disponíveis, porém apresentando problemas ou instabilidade;

8.26.18. SEVERIDADE BAIXA: Aplicado para instalação, configuração, manutenção preventivas, aplicações de atualização e esclarecimento técnico relativo ao uso das ferramentas.

8.26.19. Os prazos estabelecidos nos níveis de serviços serão contados a partir da abertura do chamado, o qual será classificado conforme as severidades especificadas no item anterior.

8.26.20. **Os prazos máximos para o atendimento dos chamados** obedecerão ao disposto na tabela a seguir, contados a partir da data e hora de abertura do chamado:

- SEVERIDADE ATENDIMENTO SOLUÇÃO / PALIATIVO
- ALTA 2 (DUAS) HORAS 12 (DOZE) HORAS
- MÉDIA 6 (SEIS) HORAS 24 (VINTE E QUATRO) HORAS
- BAIXA 24 (VINTE E QUATRO) HORAS 48 (QUARENTA E OITO) HORAS
- LOCAIS REMOTOS 96 (NOVENTA E SEIS) HORAS 120 (CENTO E VINTE) HORAS

8.26.21. Para os chamados severidade LOCAIS REMOTOS (paralisação TOTAL das funcionalidades elencadas nas especificações técnicas), o início do atendimento deverá ocorrer no máximo em 96 (noventa e seis) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 120 (centro e vinte) horas corridas a contar do início do atendimento.

8.26.22. Para os chamados de severidade ALTA (paralisação de pelo menos 1 (uma) das funcionalidades elencadas nas especificações técnicas), o início do atendimento deverá ocorrer no máximo em 2 (duas) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 12 (doze) horas corridas a contar do início do atendimento.

8.26.23. Para os chamados severidade MÉDIA (degradação na performance, funcionamento ou serviço da solução), o início do atendimento deverá ocorrer no máximo em 6 (seis) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 24 (vinte e quatro) horas corridas a contar do início do atendimento.

8.26.24. Para os chamados severidade BAIXA (quando há comprometimento do desempenho), o início do atendimento deverá ocorrer no máximo em 24 (vinte e quatro) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 48 (quarenta e oito) horas corridas a contar do início do atendimento.

8.26.25. Para os chamados de qualquer severidade, a critério da SESAU/RO, poderá ser agendado o melhor horário para atendimento.

8.26.26. O fechamento de qualquer chamado só poderá ocorrer mediante consulta prévia à SESAU/RO quanto à efetiva solução do problema.

8.26.27. Qualquer chamado fechado, sem anuência da SESAU/RO ou sem que o problema tenha sido resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de aplicação das sanções previstas.

8.26.28. A Contratada manterá cadastro das pessoas indicadas pela SESAU/RO que poderão efetuar abertura e autorizar o fechamento de chamados.

8.26.29. A Contratada deverá fornecer relatório de atendimento técnico, referente a cada chamado, contendo no mínimo as seguintes informações:

8.26.30. Data e hora da abertura do chamado;

8.26.31. Data e hora do início do atendimento;

8.26.32. Responsável pelo atendimento da solicitação;

8.26.33. Motivo da ocorrência (indicação do defeito);

8.26.34. Status do chamado (aberto, em tratamento, fechado etc.);

8.26.35. Data e hora do fechamento do chamado;

8.26.36. Solução adotada (resolução);

8.26.37. O atendimento de suporte para a solução deverá ser do tipo 8 x 7 (oito horas por dia, sete dias por semana), e deverá ser realizado por profissionais especializados.

8.26.38. Não haverá limite para o número de chamados de suporte técnico.

8.26.39. Nos casos em que as manutenções necessitarem de paradas do ambiente, a CONTRATANTE deverá ser imediatamente notificada para que se proceda a aprovação da manutenção, ou para que seja agendada nova data, a ser definida pelo CONTRATANTE, para execução das atividades de manutenção;

9. MODELO DE EXECUÇÃO DO OBJETO

9.1. Execução dos Serviços

9.1.1. A CONTRATANTE no uso de suas atribuições legais nomeará Fiscais de Contrato, sendo indicado pelo representante da área requisitante o servidor que possui conhecimento técnico do objeto da contratação e designado pelo Secretário de Estado da Saúde - SESAU, mediante a Portaria, para acompanhar e fiscalizar a execução contratual, responsabilizando-se pela verificação do efetivo cumprimento das obrigações pactuadas e respectivo ateste das faturas/notas fiscais, juntamente com a comissão de recebimento em confirdade com o Art. 117º da Lei Federal n.º 14.133 de 1º Abril de 2021 e acórdão nº. 4/2006 - TCU e Anexo III - Guia de Fiscalização dos Contratos, deste Termo de Referência.

9.1.2. A prestação dos serviços deverá estar dentro dos parâmetros e rotinas estabelecidas, fornecendo todos os produtos, peças, acessórios, componentes eletrônicos, materiais, utensílios e equipamentos em quantidade, qualidade e tecnologia adequadas, com observância às recomendações aceitas pelas boas técnicas, normas e legislação vigente e em quantidades necessárias à boa execução dos serviços.

9.1.3. A CONTRATANTE fiscalizará a execução do serviço contratado e verificará o cumprimento das especificações solicitadas, no todo ou em parte, no sentido de corresponderem ao desejado ou especificado.

9.1.4. A fiscalização pela CONTRATANTE , não desobriga a CONTRATADA de sua responsabilidade quanto à perfeita execução do objeto deste instrumento;

9.1.5. A ausência de comunicação por parte da CONTRATANTE referente a irregularidades ou falhas, não exime a CONTRATADA das responsabilidades determinadas no Contrato;

9.1.6. A CONTRATADA permitirá e oferecerá condições para a mais ampla e completa fiscalização, durante a vigência do contrato, fornecendo informações, propiciando o acesso à documentação pertinente e atendendo às observações e exigências apresentadas pela fiscalização.

9.1.7. A CONTRATADA se obriga a permitir que auditoria interna da CONTRATANTE e/ou auditoria externa por ela indicada tenham acesso a todos os documentos que digam respeito ao objeto deste instrumento, inclusive auditoria a ser realizada na usina de incineração.

9.1.8. A CONTRATANTE realizará avaliação da qualidade do atendimento, dos resultados concretos dos esforços sugeridos pela CONTRATADA e dos benefícios decorrentes da política de preços por ela praticada.

9.1.9. A avaliação será considerada pela CONTRATANTE para aquilatar a necessidade de solicitar à CONTRATADA que melhore a qualidade dos serviços prestados, para decidir sobre a conveniência de renovar ou, qualquer tempo, rescindir o presente Contrato ou, ainda, para fornecer, quando solicitado pela CONTRATADA, declarações sobre seu desempenho, a fim de servir de prova de capacitação técnica em licitações públicas

9.1.10. A Contratada deverá possuir estoque mínimo de peças para realizar o serviço da manutenção corretiva quando houver a necessidade de troca das mesmas.

9.1.11. Os serviços deverão ser executados em horários que não interfiram no bom andamento da rotina de funcionamento da contratante;

9.2. LOCAL DE ENTREGA:

9.2.1. Os materiais/bens deverão ser entregues na Coordenadoria de Almoxarifado e Patrimônio (SESAU-CAP), conforme item 18.4 deste Termo de Referência.

9.3. **PRAZO DA ENTREGA**

9.3.1. O objeto deverá ser entregue no prazo de até 30 (trinta) dias, a contar da data de recebimento da Ordem de Fornecimento, Ordem de Serviço e/ou Nota de Empenho.

9.4. **MODO/REGRAS PARA O RECEBIMENTO**

9.4.1. Todo o material deverá ser entregue em embalagens individuais, em perfeito estado de conservação, lacrada e adequadas para proteger o conteúdo contra danos durante o transporte, desde o fornecedor até o local da entrega, sob condições que envolvam embarques, desembarques, transportes, por rodovias não pavimentadas, marítimos ou aéreos;

9.4.2. Os procedimentos de recebimento provisório e definitivo do objeto diretamente na unidade requisitante deve ser orientado e acompanhado pela Coordenadoria de Almoxarifado e Patrimônio-CAP/SESAU/RO, de forma a atender os padrões regulares de recebimento e demais encaminhamentos para incorporação do bem ao patrimônio público da Secretaria.

9.4.3. O objeto deverá ser indiscutivelmente novo e sem uso. Não serão aceitos equipamentos e materiais que tenham sido objeto de quaisquer processos de reciclagem e/ou recondicionamento e ainda, os que se apresentarem fora das embalagens originais de seus fabricantes.

9.5. **DO LOCAL DE DESTINAÇÃO E UTILIZAÇÃO DOS BENS**

9.5.1. Os equipamentos serão destinados as unidades que compõem a Secretária de Estado da Saúde, sua distribuição será realizada pela Coordenadora de Tecnologia da Informação conforme necessidade da unidade requisitante.

10. ESPECIFICAÇÃO DA GARANTIA DO PRODUTO

10.1. Será fornecida pelo fabricante ou assistencia técnica autorizada, devendo ser no mínimo de 12 (doze) meses, os itens ofertados deverão ter um período de garantia de 36 (trinta e seis) meses contra defeitos no que diz respeito a defeitos ocultos existentes no objeto passível de o tornar impróprio ao uso a que se destina ou lhe diminuir sensivelmente o valor, de tal modo que o ato negocial não se realizaria se esses defeitos fossem conhecidos.

10.2. A garantia do objeto deverá ser prestada pelo fabricante do equipamento ou por rede de assistência técnica do próprio fabricante, deve possuir garantia do fabricante ou autorizada no Brasil com validade mínima de 36 (trinta e seis).

10.3. Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs.

10.4. Durante o prazo de garantia, deve ser possível realizar a atualização das assinaturas de proteção da solução.

10.5. O período de garantia terá início a contar da data de entrega ou instalação do equipamento, conforme sua natureza técnica, devendo a garantia dar cobertura à eventuais manutenções corretivas e/ou substituição de peças, componentes e acessórios para o funcionamento adequado e pleno do equipamento, sem quaisquer ônus adicionais à administração.

10.6. A CONTRATADA deverá apresentar DECLARAÇÃO de que o equipamento ofertado tem assistência técnica autorizada, com indicação das empresas responsáveis, constando: nome da empresa, endereço comercial e CNPJ. Caso não haja assistência técnica no Estado deverá ser feito mediante de chamado direto com o representante revendedor, para posteriormente ser enviado pelos correios ou outro meio.

10.7. Quando acionada a assistência técnica deverá se utilizar apenas de peças e componentes novos e originais.

10.8. O prazo para substituição de peças danificadas, que estejam dentro do prazo de garantia, será de no máximo de 20 (vinte) dias.

10.9. Durante o período de garantia todas as despesas envolvidas no processo de assistência técnica deverão correr por conta da CONTRATADA, inclusive as despesas com frete de envio e retorno dos materiais.

10.10. O produto ofertado deverá atender também aos dispositivos da Lei nº. 8.078/90 (Código de Defesa do Consumidor) e às demais legislações pertinentes.

10.11. Durante o período de garantia do objeto, a empresa contratada deverá encarregar-se e responsabilizar-se pela retirada, embalagem, frete e entrega do objeto sem quaisquer ônus para a Administração Pública.

10.12. A empresa deverá fornecer certificados de garantia, em português, por meio de documentos próprios, ou anotação impressa, ou carimbada na respectiva Nota Fiscal.

11. VALOR MÁXIMO ESTIMADO UNITÁRIO E GLOBAL DA CONTRATAÇÃO (ESTIMATIVA DE DESPESA)

11.1. O valor estimado para a pretensa contratação será determinado pela pesquisa de preços que será efetuada no mercado pelo Gerência de Pesquisas e Cotações de Preços/GEPEAP da Superintendência Estadual de Compras e Licitações/SUPEL, através do Quadro Comparativo de preços atualizado (0055536029).

11.2. **ITENS 01-17 AQUISIÇÃO**

11.2.1. Valor total estimado: **R$32.068.380,98** (trinta e dois milhões, sessenta e oito mil trezentos e oitenta reais e noventa e oito centavos)**.**

11.3. **ITENS 18 -36 SERVIÇOS**

11.3.1. Valor anual estimado: **R$5.955.905,03** (cinco milhões, novecentos e cinquenta e cinco mil novecentos e cinco reais e três centavos)

11.4. VALOR ESTIMADO TOTAL DA CONTRATAÇÃO

11.4.1. Valor total estimado da contratação: **R$ 37.966.872,05** (trinta e sete milhões, novecentos e sessenta e seis mil oitocentos e setenta e dois reais e cinco centavos).

12. CLASSIFICAÇÃO ORÇAMENTÁRIA DA DESPESA (DOTAÇÃO ORÇAMENTÁRIA)

DESCRIÇÃO DA DESPESA			
OBJETO PROCESSUAL. Contratação de solução com fornecimento de equipamentos, licenças de softwares e serviços, conforme quantidades e exigências estabelecidas neste Termo de Referência, para proteção e gerenciamento seguro da rede LAN/WAN da Secretaria de Estado da Saúde – SESAU/RO, para garantir a segurança da informação fim a fim e que possibilite a visibilidade e controle de tráfego e aplicações, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN .			
Resposta ao:	Memorando 857 (0049337957)		
PROGRAMA DE TRABALHO	**UNIDADE ATENDIDA**	**FONTE DE RECURSO**	**NATUREZA DA DESPESA**
17.012.10.126.1015.2064 - PROMOVER A GESTÃO DE T.I 17.012.10.122.1015.2087 - ASSEGURAR A MANUTENÇÃO ADMINISTRATIVA DA UNIDADE	Coordenadoria de Inovação e Tecnologia da Informação - SESAU - CITI	1.500.0.01002 - Recursos não vinculados de impostos - Saúde 2.500.0.01002 - Recursos não vinculados de impostos do exercício anterior - Saúde	3.3.90.39 - Outros Serviços de Terceiros - PJ 3.3.90.40 - Serviços de Tecnologia da Informação e Comunicação - Pessoa Jurídica

Informação nº 2479/2024/SESAU-NPPS (0049384379)

13. TRATAMENTO DIFERENCIADO A MPE

13.1. Em razão do potencial comprometimento na execução do objeto licitatório devido à indivisibilidade do item, a cota de 25% prevista na Lei Complementar nº 123, de 14 de dezembro de 2006, não será aplicada nesta contratação.

13.2. Igualmente, o critério de exclusividade para Microempresas (ME) e Empresas de Pequeno Porte (EPP) não será implementado, visto que o valor da contratação supera o limite de R$ 80.000,00, conforme disposto no Art. 48, Inciso I, da mencionada lei.

13.3. Sendo assim, não se aplicará o tratamento favorecido às microempresas, empresas de pequeno porte, sociedades cooperativas referidas no Art. 16 da Lei nº 14.133/2021, ao agricultor familiar, ao produtor rural pessoa física e ao microempreendedor individual (MEI), conforme os parâmetros estabelecidos na Lei Complementar nº 123/2006 e no Decreto nº 8.538/2015. Dado que a licitação não se enquadra nos critérios do Art. 47 da Lei nº 123/2006, por não incluir itens divisíveis ou participação exclusiva de ME/EPP, aplica-se o disposto no Art. 49, Inciso III, da referida legislação.

14. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

14.1. A licitação deverá ocorrer na **modalidade pregão em sua via eletrônica** (Art. 65, Decreto Estadual No. 28.874/2024), tratando-se o objeto de serviço-bem de natureza comum, conforme classificação do objeto atestada neste termo de referência.

14.2. A forma de seleção e critério de julgamento será pelo **Menor Valor Global**, conforme o item justificativa de parcelamento da solução deste termo de referência.

14.3. O modo de disputa será **aberto** com apresentação de propostas por meio de lances públicos, sucessivos e decrescentes.

15. DA PROPOSTA

15.1. As propostas serão processadas e julgadas pelo **MENOR VALOR GLOBAL.**

15.2. As propostas apresentadas ao pregão deverão ter prazo de validade mínimo de 90 (noventa) dias a partir da data de apresentação da proposta.

15.3. A proposta deverá constar o preço unitário e total para cada item, expressos em moeda corrente nacional, nele incluídas todas as despesas/custos com materiais, ferramentas, mão de obra, impostos, taxas, seguro, frete, transporte, depreciação, emolumentos e quaisquer outros custos que, direta ou indiretamente venha ocorrer.

15.4. As propostas devem considerar integralmente as especificações técnicas comuns de cada item contido no termo de referência e Solicitação de aquisição de materiais e serviços-SAMS, não cabendo às proponentes quaisquer tipo de adaptação que promovam alterações nas especificações técnicas dos objetos.

15.5. PROSPECTO/FOLDER/CATÁLOGO/ENCARTES/FOLHETOS TÉCNICOS EM PORTUGUÊS OU LINKS OFICIAIS QUE O DISPONIBILIZEM, onde constem as especificações técnicas e a caracterização dos mesmos, permitindo a consistente avaliação dos itens.

15.6. As propostas apresentadas no presente certame deverão condizer à totalidade dos quantitativos respectivos dos iten(s) de interesse das licitantes, não sendo admitido quantidade mínima de unidade de bens a ser cotada, e, não sendo admitido a possibilidade dos licitantes oferecerem propostas em quantitativos inferiores aos máximos previstos no edital, conforme elencado no Art. 82, incisos II e IV, da Lei 14.133/2021.

15.7. Relativamente a oferta de preços, conforme dispõe o art. 82, inciso III, **não serão admitidos** preços diferentes, uma vez que para as pesquisas de preços, não incluiu-se preços do comércio LOCAL/DE MUNICÍPIOS

DISTINTOS, como forma de obter uma estimativa que contemple os custos necessários, em razão dos aspectos relacionados a localização geográfica.

16. DA EXIGÊNCIA DE AMOSTRAS

16.1. Para o objeto deste TR, a aceitação das propostas não está condicionada a apresentação de amostras, considerando a relevância do produto e o dispêndio financeiro necessário, sendo que a avaliação do produto será verificada por ocasião da entrega, estando tais produtos sujeitos a recusa de recebimento definitivo, caso não corresponda às condições e especificações mínimas definidas nos autos.

17. REQUISITOS DE HABILITAÇÃO

17.1. RELATIVOS À HABILITAÇÃO JURÍDICA

a) No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

b) Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio http://www.portaldoempreendedor.gov.br/;

c) No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

d) No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

e) No caso de cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei nº 5.764, de 1971;

f) No caso de agricultor familiar: Declaração de Aptidão ao Pronaf – DAP ou DAP-P válida, ou, ainda, outros documentos definidos pelo Ministério do Desenvolvimento Social, nos termos do Decreto Federal n° 11.802, de 28 de Novembro de 2023.

g) No caso de produtor rural: matrícula no Cadastro Específico do INSS – CEI, que comprove a qualificação como produtor rural pessoa física, nos termos da Instrução Normativa RFB nº 2110, de 17 de Outubro de 2022.

h) No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização, e se for o caso, ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

17.1.1. Os documentos acima deverão estar acompanhados da última alteração ou da consolidação respectiva.

17.2. RELATIVOS À REGULARIDADE FISCAL, SOCIAL E TRABALHISTA

a) Comprovação de inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ);

b) Comprovação de inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) Prova de regularidade perante a Fazenda federal, estadual e/ou municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;

d) Certidão de Regularidade do FGTS, relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;

e) Prova de regularidade perante a Justiça do Trabalho, mediante apresentação de Certidão de Regularidade de Débito – CNDT, para comprovar a inexistência de débitos inadimplidos perante a Justiça do Trabalho, admitida comprovação também, por meio de “certidão positiva com efeito de negativo”, diante da existência de débito confesso, parcelado e em fase de adimplemento.

17.3. RELATIVOS À QUALIFICAÇÃO ECONÔMICO - FINANCEIRA

a) Certidão Negativa de feitos sobre falência – Lei n°. 11.101/05, expedida pelo distribuidor da sede do licitante, expedida nos últimos 90 (noventa) dias caso não conste o prazo de validade.

b) Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, ou o Balanço de Abertura caso a licitante tenha sido constituída em menos de um ano, devidamente autenticado ou registrado no órgão competente, para que o(a) Pregoeiro(a) possa aferir se esta possui Patrimônio Líquido (licitantes constituídos há mais de um ano) ou Capital Social (licitantes constituídos há menos de um ano), de 5% (cinco por cento) do valor estimado para o ITEM(NS) no qual estiver participando.

b.1) o caso do licitante classificado em mais de um item, o aferimento do cumprimento da disposição acima levará em consideração a soma de todos os valores referenciais;

b.2) caso seja constatada a insuficiência de patrimônio líquido ou capital social para a integralidade dos itens/lotes em que o licitante estiver classificado, o Pregoeiro o convocará para que decida sobre a desistência do(s) item(ns) até o devido enquadramento a regra acima disposta;

b.3) as regras descritas nos itens b.1 e b.2 deverão ser observadas em caso de ulterior classificação de licitante que já se consagrou classificado em outro item(ns)/lote(s).

17.3.1. OBS: As exigências de qualificação econômico-financeira encartadas acima estão em harmonia com o que prevê o art. 69 da Lei 14.133/21 sendo necessário, para garantir que a (s) vencedora (as) detenha (am) condições econômicas para executar o futuro contrato.

17.4. **DECLARAÇÕES**

a) Declaração que a empresa não emprega menor de 18 anos, conforme disposto no inciso 33 do art. 7º da Constituição Federal;

b) Declaração da futura contratada de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social;

17.4.1. Tendo em vista que consta em campo próprio do Sistema Gerenciador de Licitação - Comprasnet.

17.5. **OUTRAS DECLARAÇÕES**

17.5.1. Art. 63, Lei 14.133/21. Na fase de habilitação das licitações serão observadas as seguintes disposições:

> IV - será exigida do licitante declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.
>
> § 1º Constará do edital de licitação cláusula que exija dos licitantes, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

17.6. **DOCUMENTAÇÃO RELATIVOS À QUALIFICAÇÃO TÉCNICA:**

17.6.1. Deverá ser demonstrada a Capacidade Técnica para a execução do objeto desta licitação por meio atestado(s), fornecidos por pessoa jurídica de direito público ou privado, comprovando o desempenho da licitante em contrato pertinente e compatível com a natureza do objeto da licitação, conforme o Art. 67 da Lei 14.133 de 01 de abril de 2021, e parâmetros delimitados abaixo:

17.6.2. Os atestados deverão ser compatíveis com o **Item 10 – Controlador Seguro de Rede WLAN e LAN Tipo 3**, apresentando que a empresa forneceu o referido objeto com no mínimo 20% (vinte por cento) do quantidade estimado do item.

17.6.3. A avaliação da qualificação técnica dos licitantes será realizada por comissão designada á qual levará em consideração a documentação apresentada, bem como outros critérios estabelecidos no edital.

17.6.4. A falta de comprovação da capacidade técnica nos termos exigidos no edital implicará na desclassificação do licitante.

17.6.5. Os documentos exigidos para a comprovação da qualificação técnica deverão ser apresentados em original, cópia ou cópia acompanhada do original para conferência pela Comissão de Licitação.

18. DO CONTRATO E SUA EXECUÇÃO

18.1. Conforme disposto no art. 95, inciso II, da Lei 14.133/2021, em caso de compras com entrega imediata e integral dos bens adquiridos e dos quais não resultem obrigações futuras, inclusive quanto a assistência técnica, independentemente de seu valor, o instrumento de contrato poderá ser substituído por instrumento hábil, neste caso a nota de empenho de despesas.

18.2. Portanto, para os objetos deste certame que apresentem garantia estendida, será celebrado contrato.

18.3. **DA FORMALIZAÇÃO DO INSTRUMENTO CONTRATUAL**

18.3.1. Oficialmente convocada pela Administração, com vistas à assinatura do Contrato, ou retirada de documento congênere, é dado a adjudicatária o prazo de 05 (cinco) dias úteis, contados da data da ciência ao chamamento, pela Secretaria de Estado da Saúde de Rondônia - SESAU-RO e firmar o instrumento Contratual ou retirada de documento congênere conforme definido pela administração.

18.3.2. A recusa injustificada da LICITANTE vencedora, assinar o Contrato, ou retirada de documento congênere, dentro do prazo e condições estabelecidas, caracterizará o descumprimento total da obrigação assumida sujeitando-se às penalidades previstas na Lei 14.133/21.

18.3.3. O Licitante Vencedor do Certame fica obrigado a realizar Cadastro de Usuários Externos do seu Representante Legal, no Sistema de Processos do Governo do Estado de Rondônia – S.E.I. (https://www.sei.ro.gov.br), para assinatura eletrônica dos documentos contratuais (Atas de Registro de Preços/Contratos).

18.4. **LOCAL DA EXECUÇÃO DO CONTRATO**

18.5. Os materiais/bens deverão ser entregues na Coordenadoria de Almoxarifado e Patrimônio (SESAU-CAP), no

endereço: Rua Aparício de Moraes, nº 4348, Bairro Industrial, CEP: 76.821-240, Porto Velho/RO. Funcionamento de segunda a sexta-feira das 7h30min às 13h30min para conferência e emissão de cessão de uso.

18.6. **CONVOCAÇÃO E CELEBRAÇÃO DO CONTRATO**

18.6.1. Oficialmente convocada pela Administração com vistas à celebração do Termo Contratual, é dado à contratada o prazo de até 5 (cinco) dias, contadas a partir da data de ciência do chamamento pela Secretaria de Estado da Saúde, para comparecer ao local indicado e proceder à assinatura do instrumento contratual. Antes da assinatura, a contratada deve entregar os documentos que se comprometeu a apresentar previamente à formalização do Termo Contratual.

18.6.2. O prazo de convocação poderá ser prorrogado uma vez, por igual período, quando solicitado pela parte durante o seu transcurso e desde que ocorra motivo justificado aceito pela Administração.

18.7. **DO REAJUSTE E DA REVISÃO DO CONTRATO**

18.7.1. Considerando as necessidades de garantia do equilíbrio econômico-financeiro dos contratos da administração pública deve ser atendido e preceituado nos parâmetros dos Art. 150 ao Art. 168 do Decreto nº 28.874 de 25 de janeiro de 2024.

18.7.2. Para os fins previstos de restabelecimento do equilíbrio econômico-financeiro fica estabelecido como data-base a apresentação da proposta ou previsões restritas, nos casos de repactuação e orçamento de obras, ainda deve ser observado o prazo para apresentação do pedido, expedido no Art. 151 do Decreto nº 28.874/2024.

18.7.3. No que tange aos índices de reajuste a serem aplicados para fins do restabelecimento econômico-financeiro, adotar-se-á o que for mais vantajoso para a Administração, devendo ser observado a existência de índice próprio para o objeto contratual, conforme Art. 156 do Decreto nº 28.874/2024.

18.7.4. No caso concreto aplicar-se o Índice Nacional de Preços ao Consumidor Amplo - IPCA, para fins de reajuste e restabelecimento do equilíbrio econômico-financeiro.

18.8. **DO REAJUSTE**

18.8.1. Conforme previsão no arts. 154 ao 156 do Decreto nº 28.874/24.

18.8.2. É nula de pleno direito qualquer estipulação de reajuste com periodicidade inferior a 1 (um) ano.

18.8.3. Ao final dos 1 (um) ano iniciais de vigência do contrato, caso decidido pela sua prorrogação, os reajustes serão corrigidos com base no Índice Nacional de Preços ao Consumidor Amplo - IPCA, ou outro índice que venha substituí-lo.

18.8.4. O reajuste em sentido estrito, espécie de reajuste nos contratos de obra, fornecimento ou serviço continuado sem dedicação exclusiva de mão de obra, consiste na aplicação de índice de correção monetária estabelecido no contrato, que retratará a variação efetiva do custo de produção, admitida a adoção de índices específicos ou setoriais.

18.8.5. O prazo para resposta ao pedido de restabelecimento do equilíbrio econômico-financeiro, será de até 15 (quinze) dias úteis, a contar do recebimento da solicitação.

18.9. **DA REPACTUAÇÃO**

18.9.1. Conforme previsão no art. 157 do Decreto nº 28.874/24: A repactuação de preços, como espécie de reajuste contratual, deverá ser utilizada nas contratações de serviços continuados com regime de dedicação exclusiva de mão de obra.

18.9.2. Dessa forma, a repactuação não será aplicada a pretensa contratação.

18.10. **REVISÃO**

18.10.1. Conforme previsão no arts. 163 ao 164 do Decreto nº 28.874/24.

18.10.2. A revisão contratual será concedida, a pedido da contratada, para promover o reequilíbrio econômico-financeiro da avença, diante da ocorrência de fatos imprevisíveis, ou previsíveis com consequências incalculáveis, retardadores ou impeditivos da execução do contrato, ou, ainda, em caso de força maior, caso fortuito ou fato do príncipe, configurando álea econômica extraordinária e extracontratual.

18.10.3. O pedido de revisão de contrato deverá ser instruído com os seguintes documentos:

18.10.4. requerimento da contratada devidamente assinado pelo seu responsável;

18.10.5. planilha de custos demonstrando a equação inicial do contrato;

18.10.6. planilha de custos demonstrando a equação atual do contrato;

18.10.7. documentação hábil demonstrando a ocorrência de fatos imprevisíveis, fatos previsíveis, porém de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, ou, ainda, caso de força maior, caso fortuito ou fato do príncipe, que configurem álea econômica extraordinária e extracontratual;

18.10.8. ato do ordenador de despesa do órgão ou entidade que decidir pelo reconhecimento das circunstâncias que autorizam a revisão do contrato;

18.10.9. pesquisa de preços praticados no mercado a fim verificar se o preço reequilibrado permanece atendendo o pressuposto fundamental da licitação, se for o caso.

18.10.10. Parágrafo único. A revisão será formalizada por meio de termo aditivo.

18.10.11. O prazo para resposta ao pedido de revisão para restabelecimento do equilíbrio econômico-financeiro, será de até 15 dias úteis, a contar do recebimento da solicitação.

18.11. **DA ENTREGA E DO RECEBIMENTO**

18.11.1. A entrega deverá ocorrer conforme solicitação via requisição da Secretaria de Saúde até o prazo máximo de 30 (trinta) dias, a contar da data de recebimento da Ordem de Fornecimento, Ordem de Serviço e/ou Nota de Empenho.

18.11.2. A empresa concorrente homologada deverá acusar o recebimento da Ordem de Fornecimento e/ou Nota de Empenho para fornecimento em 48h (quarenta e oito horas), iniciar e comunicar à Administração as providências para cumprimento dos prazos subsequentes.

18.11.3. No caso de não confirmação de recebimento da requisição do objeto pela Secretaria de Estado da Saúde de Rondônia no prazo de 05 (cinco) dias, a requisição será dada como recebida.

18.11.4. A entrega ocorrerá em parcela única, sem parcelamento da entrega.

18.11.5. O recebimento do objeto será realizada por Comissão de Recebimento de Materiais e Serviços designada pela Secretaria de Estado da Saúde de Rondônia, da unidade requisitante e/ou da Coordenadoria de Almoxarifado e Patrimônio-CAP/SESAU/RO, ou ainda por comissão especificamente designada, à critério da Administração, conforme Art. 140, inciso II da Lei Federal nº 14.133/2021.

18.11.6. A Contratante promoverá através de seus representantes, o acompanhamento e a fiscalização da entrega dos produtos sob os aspectos quantitativo e qualitativo, anotando as falhas detectadas e comunicando a Contratada as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte daquela através dos procedimentos de recebimento, que ocorrerão da seguinte forma:

18.11.7. **Provisoriamente** por servidor ou comissão designada pela Coordenadoria de Almoxarifado e Patrimônio-CAP/SESAU/RO, de forma sumária imediatamente depois de efetuada a entrega através de recibo aposto na nota fiscal. O recebimento provisório deve ser concluído dentro do prazo de até 05 (cinco) dias, devendo o CAP/SESAU/RO neste interim tomar as devidas providências para que ocorra o recebimento definitivo juntamente à unidade requisitante, a fim de se proceder a verificação da conformidade dos produtos com as especificações de forma integrada.

18.11.8. **Definitivamente** por Comissão de Recebimento de Materiais e Serviços designada da unidade requisitante, ou por comissão especificamente designada, depois de concluída a vistoria, encerrado o prazo de observação que não poderá exceder 10 (dez) dias, e, mediante termo detalhado que comprove adequação do objeto ao requerido e aprovado pela Administração, o atendimento das exigências contratuais e consequente aceitação.

18.11.9. O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança do material, nem ético profissional pela perfeita execução do contrato, dentro dos limites estabelecidos pela Lei ou instrumento contratual;

18.11.10. Em fomento à assertividade na análise técnica do objeto a comissão de recebimento poderá dispor de avaliação complementar de setor especializado ou comissão especialmente designada, caso necessário, por sua conveniência e oportunidade.

18.11.11. Salvo disposição em contrário constante do edital ou de ato normativo, os ensaios, os testes e as demais provas para aferição da boa execução do objeto do contrato exigidos por normas técnicas oficiais correrão por conta do contratado.

18.11.12. A Contratante poderá rejeitar no todo ou em parte os materiais entregues em desacordo com as especificações técnicas do objeto ou com as obrigações assumidas.

18.11.13. Se o fornecedor vencedor tiver comprovadamente dificuldades para entregar os materiais, dentro do prazo estabelecido, não sofrerá multa, caso informe oficialmente com antecedência de mínimo 03 (três) dias úteis, antes de esgotado o prazo inicialmente previsto, apresentando justificativa circunstanciada formal, que deverá ser encaminhada ao Secretário de Estado da Saúde que, por sua vez, decidirá a possibilidade de prorrogação do prazo, ou determinará a cominação das multas cabíveis, que ocorrerá a partir da efetiva notificação;

18.11.14. Se, após o recebimento provisório, for constatado que os materiais foram entregues de forma incompleta ou em desacordo com as especificações ou com a proposta, será interrompido o prazo de recebimento definitivo e suspenso o prazo de pagamento até que seja sanada a situação;

18.11.15. A empresa vencedora ficará obrigada a trocar, às suas expensas, o que for recusado por apresentar-se contraditório as especificações contidas no Termo de Referência;

18.11.16. O objeto deverá ser entregues de acordo com as especificações técnicas e demais disposições constantes no Termo de Referência, não sendo permitido a Comissão, receber os equipamentos fora das especificações pré-definidas.

18.11.17. O objeto deverá ser indiscutivelmente novo e sem uso. Não serão aceitos itens que tenham sido objeto de quaisquer processos de reciclagem ou recondicionamento. Deverão estar acondicionados em embalagem própria conforme ao fabricante, garantindo sua integridade.

18.11.18. A Contratada fica sujeito às sanções administrativas previstas, quando for o caso.

18.12. **DA INSTALAÇÃO/MANUTENÇÃO**

18.12.1. A descrição detalhada dos serviços de instalação referentes a cada objeto pode ser encontrada nos itens 8.14 ao 8.25 deste Termo de Referência, onde são especificados os procedimentos técnicos, requisitos e diretrizes que devem ser seguidos para a execução adequada das atividades.

18.13. **VIGÊNCIA DO CONTRATUAL**

18.13.1. O prazo de vigência do contrato será de 1 (um) ano, podendo o mesmo ser prorrogado por igual período até o limite de 10 (dez) anos, desde que haja interesse das partes, conforme art. 106 e 107 da Lei Federal nº 14.133 de 1° de abril de 2021, com suas alterações e amplitude de legislação aplicável vigente.

18.14. **REAJUSTE DA ATA DE REGISTRO DE PREÇO**

18.14.1. Durante a vigência da Ata de Registro de Preços, os preços serão irreajustáveis.

19. REQUISITOS DA CONTRATAÇÃO

19.1. A Contratação em tela deverá obedecer, no que couber, ao disposto na Lei Federal nº 14.133 de 1° de Abril de 2021 e suas alterações, bem como as seguintes normas:

a) Instrução Normativa nº 58, de 08 de agosto de 2022 - Ministério da Economia;

b) Decreto Estadual nº 28.874, de 25 de janeiro de 2024;

c) Lei Federal nº 8.078, de 11 de setembro de 1990;

d) Lei Federal nº 13.709, de 14 de agosto de 2018;

e) Lei Federal nº 7.232, de 29 de outubro de 1984;

f) Decreto Federal nº 8.793, de 29 de junho de 2016;

g) Resolução da Diretoria Colegiada (RDC) nº 307, de 13 de novembro de 2002;

h) Resolução da Diretoria Colegiada (RDC) nº 53, de 14 de novembro de 2013;

i) ABNT NBR ISO/IEC 27001:2013;

j) ABNT NBR ISO 9001:2015;

k) ABNT NBR 5410:2004;

l) Norma de Segurança do Trabalho NR-17 - Ergonomia;

m)Norma de Segurança do Trabalho NR-10 - Segurança em Instalações e Serviços em Eletricidade.

19.2. **POSSÍVEIS IMPACTOS AMBIENTAIS e CRITÉRIOS DE SUSTENTABILIDADE:**

19.2.1. A presente licitação priorizará propostas que demonstrem compromisso com a sustentabilidade, podendo haver vinculação entre o pagamento e o cumprimento de metas ambientais e sociais, conforme previsto no (art. 5º, art. 11, IV e art. 144 da Lei 14.133/2021) e no (art. 34, II Decreto Estadual Nº 28.874/24).

19.2.2. A aquisição dos itens podem ter diversos impactos ambientais em diferentes fases do ciclo de vida dos produtos, desde a extração das matérias-primas até o descarte final.

19.2.3. Aqui estão alguns dos principais impactos ambientais associados a esses produtos:

19.2.4. A aquisição de itens de informática tem diversos impactos ambientais, tanto durante a produção, quanto ao longo do ciclo de vida dos produtos. Aqui estão alguns dos principais impactos ambientais associados a esses produtos:

19.2.4.1. Produção e Extração de Recursos Naturais:

- Mineração de metais raros e minerais: A fabricação de dispositivos de informática, como computadores, celulares e outros eletrônicos, exige a extração de minerais e metais raros, como lítio, cobalto, coltan (utilizado em baterias), silício e outros. A mineração desses materiais pode causar desmatamento, perda de biodiversidade, poluição do solo e da água, além de gerar conflitos sociais em regiões onde a mineração é intensiva.
- Emissão de gases de efeito estufa (GEE): O processo de extração e processamento de minerais exige grandes quantidades de energia, o que contribui para as emissões de GEE, acelerando as mudanças climáticas.

19.2.4.2. 2. Fabricação e Processos Industriais:

- Emissões de carbono: A fabricação de dispositivos eletrônicos envolve o uso de processos industriais intensivos em energia, o que gera emissões de CO2. Isso inclui a produção de semicondutores, o processo de montagem e a soldagem de componentes, que também consomem grandes quantidades de água e geram resíduos.
- Resíduos industriais: Muitos produtos eletrônicos geram resíduos tóxicos durante sua fabricação, como solventes, produtos químicos pesados (como mercúrio e cádmio), e plástico (muitas vezes não reciclado).

19.2.4.3. 3. Transporte e Logística:

- Emissões de carbono associadas ao transporte: Os dispositivos de informática, assim como seus componentes, geralmente percorrem grandes distâncias, desde as fábricas até os consumidores finais. O transporte contribui para a emissão de gases poluentes devido ao uso de combustíveis fósseis.
- Embalagens: A embalagem de dispositivos eletrônicos muitas vezes envolve materiais como plástico, espuma de poliestireno e papelão. Embora parte dessas embalagens possa ser reciclada, elas ainda representam um impacto no uso de recursos naturais e geram lixo.

19.2.4.4. 4. Uso e Consumo:

- Consumo de energia: Durante seu uso, os dispositivos de informática consomem energia elétrica. O impacto ambiental dependerá da fonte dessa energia, sendo maior se a eletricidade for gerada a partir de fontes não-renováveis (como carvão ou petróleo). Além disso, a eficiência energética dos dispositivos varia, e modelos menos eficientes tendem a consumir mais energia ao longo do tempo.
- Obsolescência programada: Muitos dispositivos têm uma vida útil limitada, muitas vezes planejada pelos fabricantes (obsolescência programada), o que resulta em um aumento na demanda por novos produtos, gerando mais resíduos e aumentando a necessidade de novos recursos.

19.2.4.5. 5. Descarte e Resíduos Eletrônicos (e-waste):

- Lixo eletrônico (e-waste): Quando os dispositivos de informática chegam ao fim de sua vida útil, muitos acabam em aterros sanitários ou são mal reciclados, liberando substâncias tóxicas como mercúrio, cádmio e lítio. O descarte inadequado desses produtos pode contaminar o solo e a água, além de prejudicar a saúde humana.
- Reciclagem: Embora a reciclagem de eletrônicos seja uma prática crescente, apenas uma pequena fração dos produtos é efetivamente reciclada de maneira adequada. A reciclagem de dispositivos eletrônicos pode ajudar a reduzir o impacto ambiental, mas muitos itens ainda não são coletados ou processados de forma eficiente.

19.2.4.6. 6. Soluções para Reduzir os Impactos:

- Reciclagem e reutilização: Incentivar a reciclagem de eletrônicos e o reaproveitamento de componentes é uma forma importante de reduzir os impactos ambientais. Muitas empresas estão começando a implementar programas de devolução de produtos antigos ou reaproveitamento de materiais.
- Design sustentável: A indústria de tecnologia tem avançado na busca por designs mais sustentáveis, com dispositivos mais fáceis de reciclar e compostos por materiais mais ecológicos.
- Eficiência energética: Optar por dispositivos mais eficientes em termos de consumo de energia pode reduzir significativamente os impactos ambientais durante o uso. Além disso, o incentivo à utilização de fontes de energia renovável para alimentar os dispositivos ajuda a diminuir as emissões associadas.

19.2.5. A produção, o uso e o descarte de produtos de informática têm impactos ambientais significativos, envolvendo desde a extração de recursos até a geração de resíduos eletrônicos. No entanto, com práticas de consumo consciente, reciclagem adequada e investimento em tecnologias mais sustentáveis, é possível mitigar muitos desses impactos.

19.2.6. A seguir, estão os possíveis impactos ambientais associados à aquisição dos itens e as medidas que podem ser tomadas para mitigá-los:

19.2.7. Para minimizar possíveis impactos e promover compras mais ambientalmente responsáveis, a Secretaria de Estado da Saúde pode:

19.2.7.1. Adotar critérios socioambientais na licitação:

- Exigir dos fornecedores certificados que comprovem boas práticas socioambientais, como ISO 14001 e FSC.
- Priorizar produtos com selos de sustentabilidade, como o Selo Procel e o Selo Verde.
- Incentivar a compra de produtos reciclados ou feitos com materiais de origem renovável.
- Estabelecer critérios para a embalagem dos produtos, como a utilização de materiais reciclados e a minimização do volume.

19.2.7.2. Optar por produtos duráveis e de alta qualidade:

- Priorizar produtos com maior vida útil, reduzindo a necessidade de reposição frequente e diminuindo a geração de resíduos.
- Escolher produtos com garantia estendida, minimizando a necessidade de descarte precoce e incentivando o reparo.
- Optar por produtos multifuncionais, que realizem diversas tarefas, reduzindo a quantidade de itens

comprados e descartados.

19.2.7.3. Implementar ações de descarte correto:

- Criar um programa de coleta seletiva para os resíduos eletrônicos gerados pela secretaria, garantindo o descarte correto e a reciclagem dos materiais.
- Descartar pilhas e baterias em locais apropriados, evitando a contaminação do solo e da água.
- Promover campanhas de conscientização sobre a importância do descarte correto de resíduos eletrônicos entre os funcionários.

19.2.7.4. Reduzir o consumo de energia:

- Optar por produtos com eficiência energética A, que consomem menos energia e contribuem para a redução da emissão de gases do efeito estufa.
- Desligar os equipamentos quando não estiverem em uso e utilizar temporizadores para otimizar o consumo de energia.
- Investir em fontes de energia renovável, como painéis solares, para reduzir a dependência de combustíveis fósseis.

19.2.7.5. Adotar práticas de consumo consciente:

- Avaliar se a compra do produto é realmente necessária e se existem alternativas mais sustentáveis disponíveis.
- Comprar apenas a quantidade necessária de cada item, evitando o acúmulo de produtos em estoque.
- Optar por produtos reutilizáveis, como canecas e garrafas de água, em vez de descartáveis.

19.2.8. A sustentabilidade deve ser um compromisso de toda a organização.

19.2.9. É importante envolver os funcionários nas iniciativas de sustentabilidade.

19.2.10. Ao investir em um ciclo de vida de produtos mais consciente e responsável, a Secretaria de Estado da Saúde pode contribuir para a preservação do meio ambiente e para a construção de um futuro mais sustentável para todos.

19.2.11. Adquirir itens de informática de forma sustentável envolve considerar não apenas o produto em si, mas também os processos e práticas da empresa produtora. Produtos com certificações ambientais, materiais recicláveis, eficiência energética e que oferecem programas de reciclagem são escolhas mais sustentáveis. Além disso, optar por marcas que promovem boas condições de trabalho e seguem princípios éticos contribui para uma abordagem mais ampla de sustentabilidade, envolvendo também os aspectos sociais e econômicos da produção.

19.2.12. Em suma, a adoção de medidas de mitigação em todas as etapas do ciclo de vida dos produtos pode ajudar a reduzir os impactos ambientais associados à aquisição. Isso requer uma abordagem holística que leve em consideração não apenas a eficiência e a qualidade dos produtos, mas também seu impacto ambiental e social.

20. DAS OBRIGAÇÕES

20.1. DA CONTRATADA:

20.1.1. Além daquelas exigidas na Lei Federal 14.133/2021, e, Lei Estadual 28.874/2024, deverá:

20.1.2. Responsabilizar-se integralmente pelos materiais adquiridos, nos termos da legislação vigente;

20.1.3. Entregar o objeto da aquisição nas especificações contidas neste Termo de Referência;

20.1.4. Entregar o objeto na forma e prazo estipulados neste Termo de Referência;

20.1.5. Entregar o objeto nas quantidades indicadas pelo órgão requisitante;

20.1.6. Os materiais que não atenderem exigências deste edital não serão aceitos e recebidos, devendo ser substituídos imediatamente.

20.1.7. Não promover substituição do produto empenhado, sem anuência expressa da contratante;

20.1.8. Entregar os produtos em embalagem íntegra, sob pena de rescisão do ajuste, independentemente das combinações legais cabíveis;

20.1.9. No Pregão Eletrônico não há quantidade mínima a ser adquirida, tampouco obrigatoriedade de aquisição de todo o quantitativo licitado, e, em caso de eventuais contratos de fornecimento decorrentes da Aquisição, a Contratada se obriga a aceitar as supressões nas quantidades inicialmente previstas respeitando os limites da Lei 14.133/21 e os parâmetros da Lei 28.874/2024, tendo como base os preços constantes da(s) proposta(s) Contratada(s), diante de necessidade comprovada da Administração.

20.1.10. Responsabilizar-se pela substituição do produto entregue em desconformidade com este Termo de Referência, ou impossibilitados de uso devido, perda ou deterioração de suas características, devendo ser trocados no prazo

máximo de 20 (vinte) dias uteis, contados a partir de comunicação formal do responsável. O ônus de todas as despesas decorrentes da efetivação da troca será da Contratada;

20.1.11. Manter durante toda execução da Ata, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

20.1.12. Responsabilizar-se por todos os ônus, encargos, perdas e danos quando for constatado que tenham sido ocasionados em decorrência do fornecimento do objeto;

20.1.13. Considerar em todas as etapas de vinculação e arcar efetivamente com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas e todos os tributos incidentes, sem qualquer ônus à Contratante, devendo efetuar os respectivos pagamentos na forma e nos prazos previstos em Lei;

20.1.14. Indicar um preposto devidamente habilitado, com poderes para representá-lo em tudo o que se relacionar com o fornecimento objeto;

20.1.15. Ficarão a cargo da empresa vencedora os custos de frete, impostos, taxas e etc., que venham a incidir sobre a aquisição objeto deste Termo de Referência;

20.1.16. No momento da entrega a empresa deverá apresentar relação com o material entregue e nota fiscal, contendo marca, especificação e quantidade. Os preços propostos deverão incluir fretes e demais custos diretos e indiretos, inclusive os resultantes da incidência de quaisquer impostos, tributos, contribuições ou obrigações trabalhista, fiscais e previdenciárias a que estiver sujeito.

20.1.17. Garantir a qualidade dos produtos ofertados conforme este Termo de Referência e estipulado nas normas técnicas e regulamentações especializadas relacionadas ao objeto de fornecimento;

20.1.18. A contratada deverá reparar, corrigir, remover, reconstituir ou substituir, às suas expensas, os materiais que forem rejeitados, parcial ou totalmente, por apresentarem vícios, defeitos, incorreções, no prazo máximo de 20 (vinte) dias úteis a contar da data do recebimento da comunicação do fato.

20.1.19. CUMPRIR E FAZER CUMPRIR, todas as diretrizes, normas, regulamentos impostas por este Termo de Referência e seus ANEXOS.

20.2. **DA CONTRATANTE:**

20.2.1. Além daquelas constantes no Termo de Referência e aquelas determinadas por leis, decretos, normas técnicas, regulamentos e demais dispositivos legais, a CONTRATANTE se obrigará:

20.2.2. Fiscalizar, acompanhar, conferir e avaliar o objeto deste Termo de Referência, através de representantes designados pela SESAU, conforme dispõe a Lei Nº 14.133/2021. Promover através da comissão nomeada, o acompanhamento e a fiscalização da entrega e recebimento dos produtos sob os aspectos quantitativo e qualitativo, anotando as inconformidades ou falhas detectadas e comunicando a Contratada as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte daquela;

20.2.3. Garantir o cumprimento de todas as cláusulas contratuais ao bom desempenho do objeto desta contratação;

20.2.4. Aplicar as penalidades regulamentares cabíveis, quando for o caso;

20.2.5. Devolver o material caso não esteja dentro das especificações constantes do presente Termo de Referência, ou impossibilitados de uso devido por perda ou deterioração de suas características;

20.2.6. Efetuar o pagamento à contratada de acordo com as condições de preços e prazos estabelecidos neste Termo de Referência.

20.2.7. Durante o processo licitatório a Contratante deverá verificar a conformidade das propostas em relação aos requisitos estabelecidos neste termo de referência e no edital.

20.2.8. A quantidade mínima a ser solicitada de cada item será de 10% do valor previsto para cada item. Não há obrigatoriedade de aquisição de todo o quantitativo licitado.

20.2.9. Serão considerados pela Contratante para o presente processo licitatório somente os requisitos da contratação indispensáveis, necessários e suficientes à escolha da melhor solução para a Administração Pública, observadas as leis e regulamentações específicas aplicáveis, bem como padrões mínimos de qualidade e desempenho.

21. DA GARANTIA CONTRATUAL

21.1. Para fiel execução dos compromissos aqui ajustados as CONTRATADAS prestarão prévia garantia de 5% (cinco por cento) do valor inicial do Contrato, referente ao lote em que se consagraram vencedoras, como previsto no art. 98 da Lei n° 14.133 de 1° de Abril de 2021.

21.2. A Contratada poderá optar por uma das modalidades de garantia previstas no § 1º do art. 96 da a Lei Federal nº 14.133 de 1° de Abril de 2021.

21.3. A Contratada terá o prazo de 10 (dez) dias, prorrogáveis por igual período, posteriores à assinatura do contrato, para apresentação da garantia contratual.

21.4. A garantia prestada pelo contratado será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, atualizada monetariamente (art. 100° da lei

14.133/21).

22. DA SUBCONTRATAÇÃO

22.1. Nos termos do Art. 122 da Lei n° 14.333/2021 § 2º e § 3º ***NÃO SERÁ PERMITIDA A SUBCONTRATAÇÃO, CESSÃO E/OU TRANSFERÊNCIA*** dos compromissos assumidos no instrumento contratual ou equivalente, constantes deste termo de referência, edital e seus anexos**.**

22.2. É vedada a subcontratação, no todo ou em parte, do objeto a ser contratado por diversos motivos que visam assegurar a qualidade dos serviços e a segurança da rede da SESAU-RO, Ao proibir a subcontratação, a SESAU-RO assegura que todos os serviços sejam executados diretamente pelo contratado, garantindo maior controle sobre a qualidade e o cumprimento dos padrões estabelecidos no contrato. Isso evita a delegação de atividades críticas a terceiros que possam não possuir o mesmo nível de competência técnica ou compromisso com os requisitos do contrato, os serviços de TI, especialmente aqueles relacionados à segurança de rede, pode expor a infraestrutura da SESAU-RO a riscos adicionais. A execução dos serviços diretamente pelo contratado, sem intermediários, reduz o número de pessoas com acesso a informações sensíveis e minimiza a possibilidade de vazamentos ou acessos não autorizados. A vedação à subcontratação facilita a identificação e a responsabilização em caso de falhas ou problemas na execução dos serviços. Com a execução direta, a SESAU-RO pode exigir maior responsabilidade e confiabilidade da empresa contratada, garantindo que as soluções implementadas sejam robustas e eficientes.

> Art. 122. Na execução do contrato e sem prejuízo das responsabilidades contratuais e legais, **o contratado poderá subcontratar partes da obra, do serviço ou do fornecimento até o limite autorizado, em cada caso, pela Administração.**
>
> ...
>
> § 2º Regulamento ou edital de licitação **poderão vedar, restringir ou estabelecer condições para a subcontratação.**
>
> § 3º Será vedada a subcontratação de pessoa física ou jurídica, se aquela ou os dirigentes desta mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou se deles forem cônjuge, companheiro ou parente em linha reta, colateral, ou por afinidade, até o terceiro grau, devendo essa proibição constar expressamente do edital de licitação.

23. MODELO DE GESTÃO DE CONTRATO

23.1. A resolução N. 01/2024/SESAU-SC (0048586915) estabelece a necessidade de normatização da gestão e fiscalização dos contratos no âmbito da Secretaria de Estado da Saúde de Rondônia, em conformidade com a Lei nº 14.133, de 1º de abril de 2021.

23.2. Esta resolução impõe a obrigatoriedade de que a gestão e a fiscalização dos contratos sejam realizadas seguindo as diretrizes especificadas na própria resolução N. 01/2024/SESAU-SC.

> RESOLVE:
>
> Art. 1º – Aprovar o Manual de Gestão e Fiscalização de Contratos Administrativos (SEI nº 0047523841) elaborado pela comissão designada na Portaria 4150 (0041658066) de 11 de setembro de 2023.
>
> Art. 2º – Instituir no Âmbito da Secretaria de Estado da Saúde a obrigatoriedade da utilização do Manual de Gestão e Fiscalização de Contratos Administrativos (0048122701) na Gestão e Fiscalização dos contratos.
>
> Art. 3º – Deverão ser observados os procedimentos estabelecidos no Manual de forma cumulativa com os demais procedimentos previstos na legislação.
>
> Art. 4º – Esta Resolução entrará em vigor a partir da data de sua publicação.

23.3. Desta forma, a gestão e a fiscalização dos contratos serão realizados conforme o Manual de Gestão e Fiscalização de Contratos Administrativos (0051378718), Anexo II deste Termo de Referência.

24. PAGAMENTO:

24.0.1. O pagamento dos itens 1 ao 17 do quadro 3.2.1, que se referem a aquisição de equipamentos será efetuado de forma INTEGRAL, conforme os equipamentos entregues, mediante a apresentação de Nota Fiscal, emitidas pela Contratada, devidamente atestadas pela Administração.

24.1. O pagamento dos itens 18 a 36 do quadro 3.2.1, o pagamento será efetuado **MENSALMENTE**, conforme o serviço prestado/fornecido, mediante a apresentação de Nota Fiscal, emitidas pela Contratada, devidamente atestadas pela Administração, conforme disposto no art. 140, Inciso I, alínea b da Lei nº 14.133, de 2021.

24.2. Insta salientar que o pagamento seguirá conforme estipulado no Art. 188 do Decreto n.º 28.874/2024, ou seja:

> Art. 188. As solicitações de pagamento deverão ser formalizadas pelo contratado por meio de pedido subscrito pelo seu representante legal, indicando o número do contrato administrativo e os dados para pagamento, instruído com os seguintes documentos:
> I - nota fiscal, fatura ou documento equivalente que ateste o cumprimento do objeto, indicando o valor e o período da prestação do serviço ou do fornecimento;
> II - certidão de regularidade fiscal perante a Fazenda Estadual;
> III - certidão de regularidade previdenciária e trabalhista, além dos documentos comprobatórios do cumprimento das respectivas obrigações nos termos do art. 24 deste Decreto, nos casos de contrato de prestação de serviços contínuos com dedicação exclusiva (ou predominante) de mão de obra;
> IV - comprovante de cumprimento de obrigações previdenciárias, nos casos de contratos de obra;
> V - medição realizada pela fiscalização do contrato, nos casos de obra e serviços de engenharia, e de contratos

submetidos ao referido regime de pagamento por medição;
VI - comprovante de atingimento de metas e respectivo impacto percentual no caso de remuneração variável;
VII - comprovante de percentual de economia produzida, nos casos de contratos de eficiência.
§ 1º Os documentos apresentados deverão ser atestados pela fiscalização do contrato que emitirá parecer conclusivo sobre a viabilidade do pagamento diante do cumprimento do objeto e efetiva correspondência com o valor cobrado, devendo ser autuado processo administrativo no qual serão incluídos cópia do contrato e eventuais termos aditivos, cópia da nota de empenho e mapa de controle de execução contratual.
§ 2º Atestado o cumprimento do objeto do contrato pela fiscalização e a correta instrução do processo, após autorização do ordenador, os autos deverão ser remetidos ao setor responsável pela liquidação da despesa e efetivação do pagamento.
§ 3º Em caso de não cumprimento do inciso II, o contratado deverá ser instado a se manifestar sobre a possibilidade de compensação do crédito com o débito existente, caso em que os autos deverão ser remetidos ao órgão fazendário para as providências cabíveis, com prévia oitiva da Procuradoria - Geral do Estado em caso de débito inscrito em dívida ativa.
§ 4º Em caso de não concordância com a compensação, imediatamente após o pagamento da contraprestação, os autos deverão ser remetidos à Procuradoria-Geral do Estado para adoção das providências cabíveis para recuperação do crédito estadual.
§ 5º Em caso de não cumprimento dos incisos III e IV, o pagamento deverá ser retido até a regularização, observadas as diretrizes fixadas neste Decreto.

24.3. Por conseguinte, a nota fiscal deverá ser emitida em favor do:

a) **Fundo Estadual de Saúde - RO.**

b) **CNPJ Nº: 00.733.062/0001-02.**

c) Endereço: Av. Farquar, 2986, Complexo Rio Madeira, Edifício Rio Machado (Entrada pela PIO XII) – Bairro: Pedrinhas – CEP: 76.801-470 - Porto Velho/RO

24.4. No corpo da Nota Fiscal/Fatura deverá conter:

a) A descrição detalhada do item;

b) Valor e o período do fornecimento do objeto/da prestação do serviço;

c) Identificação de Número do Processo e identificação da Nota de empenho;

d) Identificação do Banco (código), da Agência Bancária, do Número da Conta Bancária, para fins de pagamento, o qual deverá ser efetuado no prazo de até 15 (quinze) dias após a entrega total dos itens/produtos de acordo com a nota de empenho, bem com, das correções fiscais e contábeis, se for o caso.

24.5. O pagamento decorrente de contratações públicas será feito após a habilitação para pagamento, no prazo máximo de 15 (quinze) dias úteis, consoante o disposto no art. 190 do Decreto 28.874/2024.

24.6. No caso das Notas Fiscais apresentarem erros ou dúvidas quanto à exatidão, ou documentação, a Administração Pública poderá pagar apenas a parcela incontroversa no prazo fixado para pagamento, ressalvado o direito da empresa de representar para cobrança, as partes controvertidas com devidas justificativas, nestes casos, a Administração Pública terá o prazo de até 05 (cinco) dias úteis, a partir do recebimento, para efetuar análise e pagamento devidamente atestadas pela Administração.

24.7. Na hipótese da contratada não estar regular perante a Fazenda Estadual, o contratado será instado a se manifestar sobre a possibilidade de compensação do crédito com o débito existente, caso em que os autos serão remetidos ao órgão fazendário para as providências cabíveis, com prévia oitiva da Procuradoria - Geral do Estado em caso de débito inscrito em dívida ativa. Em caso de não concordância com a compensação, imediatamente após o pagamento da contraprestação, os autos serão remetidos à Procuradoria-Geral do Estado para adoção das providências cabíveis para recuperação do crédito estadual.

24.8. Em caso de descumprimento das obrigações trabalhistas e previdenciária, o pagamento será retido até a regularização, sem prejuízo das sanções cabíveis.

24.9. Não será efetuado qualquer pagamento, salvo as parcelas incontroversas, à (s) empresa (s) Contratada (s) enquanto houver pendência de liquidação da obrigação financeira em virtude de penalidade ou inadimplência contratual.

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

$$I = \frac{(TX/100)}{365}$$

EM = I x N x VP, onde:
I = Índice de atualização financeira;
TX = Percentual da taxa de juros de mora anual;
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela em atraso.

24.11. Ocorrendo erro no documento da cobrança, este será devolvido e o pagamento será sustado para que a

Contratada tome as medidas necessárias, passando o prazo para o pagamento a ser contado a partir de data da reapresentação do mesmo. Caso se constate erro ou irregularidade na Nota Fiscal, a Administração, a seu critério, poderá devolvê-la, para as devidas correções, ou aceitá-las, com a glosa da parte que considerar indevida.

24.12. Na hipótese de devolução, a Nota Fiscal será considerada como não apresentada, para fins de atendimento das condições contratuais.

24.13. A administração não pagará nenhum compromisso que lhe venha a ser cobrado diretamente por terceiros, seja ou não instituições financeiras, à exceção de determinações judiciais, devidamente protocoladas no órgão.

24.14. Conforme a Instrução Normativa RFB nº 1.234/2012, alterada pela Instrução Normativa RFB nº 2.145/2023, e com a Instrução Normativa nº 34/2023/SEFIN-COTES, será realizada a retenção na fonte do Imposto de Renda incidente sobre os valores pagos à CONTRATADA, nos casos legalmente previstos, incluindo rendimentos oriundos de fornecimento de bens ou prestação de serviços.

25. SANÇÕES ADMINISTRATIVAS

25.1. Sem prejuízo das sanções cominadas no art. 156, I, III e IV, da Lei nº 14.133 de 1º de abril de 2021, pela inexecução total ou parcial do contrato, a Administração poderá, garantida a prévia e ampla defesa, aplicar à Contratada multa de até 10% (dez por cento) sobre a parte do contrato.

25.2. Se a adjudicatária recusar-se a retirar o instrumento contratual injustificadamente ou se não apresentar situação regular na ocasião dos recebimentos, garantida a prévia e ampla defesa, aplicar à Contratada multa de até 10% (dez por cento) sobre o valor total adjudicado.

25.3. Ficará impedido de licitar e de contratar com o Estado de Rondônia e será descredenciado no SICAF, pelo prazo de até 05 (cinco) anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, garantido o direito à ampla defesa, o licitante que, convocado dentro do prazo de validade de sua proposta:

I - não assinar o contrato;

II - não entregar a documentação exigida no edital;

III - apresentar documentação falsa;

IV - causar o atraso na execução do objeto;

V - não mantiver a proposta;

VI - falhar na execução do contrato;

VII - fraudar a execução do contrato;

VIII - comportar-se de modo inidôneo;

IX - declarar informações falsas; e

X - cometer fraude fiscal.

25.3.1. As sanções descritas no item 25.3, também se aplicam aos integrantes do cadastro de reserva, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido sem justificativa ou com justificativa recusada pela administração pública.

25.3.2. As sanções serão registradas e publicadas no SICAF e Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual - CAGEFIMP.

25.4. A multa descrita no quadro de infrações, eventualmente imposta à Contratada, será automaticamente descontada da fatura a que fizer jus, acrescida de juros moratórios de 1% (um por cento) ao mês. Caso a contratada não tenha nenhum valor a receber do Estado, ser-lhe-á concedido o prazo de 05 (cinco) dia úteis, contados de sua intimação, para efetuar o pagamento da multa. Após esse prazo, não sendo efetuado o pagamento, serão deduzidos da garantia. Mantendo-se o insucesso, seus dados serão encaminhados ao órgão competente para que seja inscrita na dívida ativa, podendo, ainda a Administração proceder à cobrança judicial.

25.5. As multas previstas nesta seção não eximem a adjudicatária ou contratada da reparação dos eventuais danos, perdas ou prejuízos que seu ato punível venha causar à Administração.

25.6. De acordo com a gravidade do descumprimento, poderá ainda a licitante se sujeitar à Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e depois de decorrido o prazo da sanção aplicada com base na legislação vigente.

25.7. A sanção denominada “Advertência” só terá lugar se emitida por escrito e quando se tratar de faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação, cabível somente até a segunda aplicação (reincidência) para a mesma infração, caso não se verifique a adequação da conduta por parte da Contratada, após o que deverão ser aplicadas sanções de grau mais significativo.

25.8. As sanções serão aplicadas sem prejuízo da responsabilidade civil e criminal que possa ser acionada em desfavor da Contratada, conforme infração cometida e prejuízos causados à administração ou a terceiros.

25.9. Para efeito de aplicação de multas, às infrações são atribuídos graus, com percentuais de multa conforme a tabela a seguir, que elenca apenas as principais situações previstas, não eximindo de outras equivalentes que surgirem, conforme o caso:

ITEM	DESCRIÇÃO DA INFRAÇÃO	GRAU	MULTA*
1.	Permitir situação que crie a possibilidade ou cause dano físico, lesão corporal ou consequências letais; por ocorrência.	06	4,0% sobre o valor contratado
2.	Usar indevidamente informações sigilosas a que teve acesso; por ocorrência.	06	4,0% sobre o valor contratado
3.	Destruir ou danificar documentos por culpa ou dolo de seus agentes; por ocorrência.	05	3,2% sobre o valor contratado
4.	Fornecer informação pérfida de serviço ou substituição de material; por ocorrência.	02	0,4% sobre o valor contratado
5.	Recusar-se a executar serviço determinado pela FISCALIZAÇÃO, sem motivo justificado; por ocorrência;	04	1,6% sobre o valor contratado
6.	Executar serviço incompleto, paliativo substitutivo como por caráter permanente, ou deixar de providenciar recomposição complementar; por ocorrência.	02	0,4% sobre o valor contratado
Para os itens a seguir, deixar de:			
7.	Cumprir quaisquer dos itens do Edital e seus anexos, mesmo que não previstos nesta tabela de multas, após reincidência formalmente notificada pela FISCALIZAÇÃO; por ocorrência.	03	0,8% sobre o valor contratado
8.	Cumprir determinação formal ou instrução complementar da FISCALIZAÇÃO, por ocorrência;	03	0,8% sobre o valor contratado
9.	Iniciar execução de serviço nos prazos estabelecidos, observados os limites mínimos estabelecidos por este Contrato; por serviço, por ocorrência.	02	0,4% sobre o valor contratado
10.	Ressarcir o órgão por eventuais danos causados por sua culpa, em qualquer bem/material.	02	0,4% sobre o valor contratado
11.	Manter a documentação de habilitação atualizada; por item, por ocorrência.	01	0,2% sobre o valor contratado

Nota: Incidente sobre o valor da parcela do contrato.

25.10. As sanções aqui previstas poderão ser aplicadas concomitantemente, facultada a defesa prévia do interessado, no respectivo processo, no prazo de 05 (cinco) dias úteis.

25.11. Após 30 (trinta) dias da falta de execução do objeto, será considerada inexecução total do contrato, o que ensejará a rescisão contratual.

25.12. As sanções de natureza pecuniária serão diretamente descontadas de créditos que eventualmente detenha a Contratada ou efetuada a sua cobrança na forma prevista em lei.

25.13. As sanções previstas não poderão ser relevadas, salvo ficar comprovada a ocorrência de situações que se enquadrem no conceito jurídico de força maior ou casos fortuitos, devidos e formalmente justificados e comprovados, e sempre a critério da autoridade competente, conforme prejuízo auferido.

25.14. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

25.15. A sanção será obrigatoriamente registrada no Sistema de Cadastramento Unificado de Fornecedores - SICAF, bem como em sistemas Estaduais.

25.16. Também ficam sujeitas às penalidades de suspensão de licitar e impedimento de contratar com o órgão licitante e de declaração de inidoneidade, previstas no subitem anterior, as empresas ou profissionais que, em razão do contrato decorrente desta licitação:

a) Tenham sofrido condenações definitivas por praticarem, por meio dolosos, fraude fiscal no recolhimento de tributos;

b) Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

c) Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

25.17. Sem prejuízo das sanções cominadas no Decreto nº 28874, de 25 de janeiro de 2024, conforme se segue:

> [...]
>
> Art. 185. A apuração de infração administrativa que enseja a imposição de advertência ou multa, isoladas ou cumulativamente, se dará mediante rito simplificado, observadas as garantias do administrado.
>
> Parágrafo único. A sanção de advertência e a imposição de multa até o limite de 5% (cinco por cento) do valor contratado poderá ser aplicada diretamente pelo servidor ou comissão responsável pela fiscalização, assim como a constituição em mora do contratado em caso de inexecução do contrato.
>
> [...]

26. DIREITOS AUTORAIS

26.1. A forma de contratação do objeto não exige a previsão de direitos autorais, propriedade intelectual, nem tampouco sigilo e segurança de dados, conforme Art. 42, inciso XXVII, do Decreto Estadual No. 28.874/2024.

27. REQUISITOS PARA SERVIÇOS QUE ENVOLVAM SOLUÇÃO DE TIC

27.1. **Necessidades Tecnológicas Identificadas:**

27.1.1. Firewall: Necessidade de uma solução de firewall robusta e abrangente que ofereça proteção completa para toda a rede da secretaria, substituindo a cobertura limitada do Fortinet e o sistema obsoleto do Blockbit.

27.1.2. Switches: Aquisição de switches modernos com suporte a Power over Ethernet (PoE), capazes de fornecer energia e conectividade para dispositivos como telefones IP e pontos de acesso, reduzindo a necessidade de fontes de alimentação separadas e simplificando a infraestrutura de TI. É crucial substituir os switches desatualizados e hubs para reduzir o cascateamento e melhorar a eficiência da rede.

27.1.3. Access Points: Implementação de access points empresariais de alto desempenho para substituir os equipamentos de uso doméstico, garantindo uma conectividade estável e de alta qualidade, capaz de suportar o volume de dados e o número de acessos simultâneos exigidos.

27.1.4. Suporte e Instalação: Necessidade de um contrato que inclua a instalação completa da solução integrada e suporte técnico por 36 meses, para garantir a manutenção contínua e o funcionamento eficiente dos novos equipamentos.

27.1.5. **Solução Proposta:**

27.1.6. A aquisição de uma solução integrada composta por switches modernos, firewall robusto e access points empresariais é essencial para atender às necessidades tecnológicas da SESAU-RO. A contratação de um único fornecedor para fornecer, instalar e suportar toda a solução garantirá:

27.1.7. Integração Eficiente: Garantia de que todos os componentes funcionarão de maneira integrada e sem problemas de compatibilidade.

27.1.8. Redução de Custos: Economia de escala e menor custo total ao evitar múltiplas contratações e processos de integração complexos.

27.1.9. Melhoria na Qualidade do Serviço: Suporte contínuo e eficiente, assegurando a continuidade e a qualidade dos serviços de TI.

27.1.10. Eficiência e Produtividade: Solução que elimina falhas, lentidão e problemas de conectividade, aumentando a eficiência e a produtividade dos usuários da rede.

27.1.11. A aquisição de uma solução integrada e a contratação de um fornecedor único são estratégias fundamentais para assegurar que a SESAU-RO possa atender de maneira eficaz às suas necessidades tecnológicas e melhorar a infraestrutura de TI da secretaria.

27.2. O critério utilizado para definir os bens e serviços que compõem esta categoria fundamentou-se no potencial de impacto que esses recursos podem gerar à infraestrutura de TIC da organização e no grau de especialidade exigido para a especificação técnica desses bens e serviços, sendo inerentes ao domínio de conhecimento de TIC. Além disso, há amparo na Lei nº 8.248, de 23 de outubro de 1991, que atrai para o seu escopo as máquinas, equipamentos e dispositivos baseados em técnica digital, com funções de coleta, tratamento, estruturação, armazenamento, comutação, transmissão, recuperação ou apresentação da informação, seus respectivos insumos eletrônicos, partes, peças e suporte físico para operação.

27.3. A métrica utilizada para a arquitetura tecnológica foi definida com base na distribuição quantitativa dos equipamentos essenciais para a infraestrutura de TI, conforme detalhado no **QUADRO DE DISTRIBUIÇÃO**. A alocação dos itens, como pontos de acesso (246 unidades) e switches de acesso de 24 e 48 portas PoE (96 e 124 unidades, respectivamente), foi realizada considerando a demanda operacional de cada unidade, garantindo cobertura adequada da rede e segurança no tráfego de dados. O cálculo foi elaborado a partir da infraestrutura existente, levando em conta a quantidade de racks disponíveis em cada unidade de saúde e o número de máquinas conectadas a esses racks. Os firewalls foram dimensionados de acordo com a necessidade total de cada unidade, considerando a quantidade de equipamentos e o volume de tráfego gerado em cada local. Já os pontos de acesso foram planejados conforme a extensão física das unidades de saúde e a necessidade específica de conectividade em áreas estratégicas para o funcionamento dos sistemas

27.4. Portanto os objetos da presente demanda se enquadram nos requisitos para solução TIC.

28. CONDIÇÕES GERAIS

28.1. A contratada será obrigada a aceitar, nas mesmas condições contratuais, acréscimos ou supressões de até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato que se fizerem nas obras, nos serviços, conforme art. 125 da Lei Federal nº 14.133 de 1° de Abril de 2021.

28.2. Rege-se este instrumento pelas normas e diretrizes estabelecidas na Lei nº 14.133, de 1º abril de 2021, e outros preceitos de direito público, aplicando-se supletivamente os princípios da Teoria Geral dos Contratos e disposições de direito privado.

28.3. As omissões, dúvidas e casos não previstos neste instrumento, serão resolvidos e decididos aplicando as regras contratuais e a Lei Federal nº 14.133 de 1° de Abril de 2021 e suas alterações.

28.4. Nenhuma reivindicação adicional de pagamento ou reajustamento de preços será considerada.

28.5. Cumprir e fazer cumprir, todas as diretrizes, normas, regulamentos impostas por este Termo de Referência.

28.6. Será eleito o foro da Comarca de Porto Velho/RO, com expressa renúncia de qualquer outro, para dirimir os possíveis litígios que decorram do presente procedimento.

28.7. A Administração utilizar-se-á da aplicação de juízo arbitral para dirimir conflitos relativos a direitos patrimoniais disponíveis, conforme disposto na Lei Estadual 407 e Lei n. 9.307, de 1996, alterada pela Lei Federal n. 13.129, de 2015. Tal medida visa o cumprimento ao Art. 11, do referido diploma legal.

28.8. Fica vedado a contratação de cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do órgão ou entidade contratante ou de agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, conforme Art. 48, Parágrafo Único, da Lei 14133/2021.

28.9. Fica vedado a intervenção indevida da Administração na gestão interna do contratado, conforme art. 48, VI, da Lei 14133/21.

28.10. Certifica-se que esta Secretária de Estado da Saúde atende ao princípio da segregação de funções, conforme art. 7º, §1º, da Lei 14133/21 e art. 12 do Decreto 11246/22.

28.11. Certifica-se para os fins previstos no inciso II, do Art. 16 da Lei Complementar n°101, de 04 de maio de 2000, que a despesa pública acima especificada tem adequação financeira com a lei orçamentária anual (LOA) e compatibilidade com o Plano Plurianual (PPA) e com a Lei de Diretrizes Orçamentária (LDO).

28.12. Certifica-se que esta Secretaria de Estado da Saúde fica comprometida a emitir a devida Nota de Empenho assim que liberado o crédito orçamentário pela Secretária de Estado de Planejamento Orçamento e Gestão (SEPOG), no presente exercício e próximo de acordo com a LOA 2024 e 2025.

28.13. Certifica-se que está Secretaria de Estado da Saude cumpre o princípio compatibilidade da despesa estimada com a prevista nas leis orçamentárias. Art. 40, V, “c”, da Lei 14.133/21.

28.14. Certifica-se que está Secretaria de Estado da Saude atesta o cumprimento das disposições contidas no Plano de Contratações Anual (Decreto nº 10947/22), no Plano Diretor de Logística Sustentável e demais instrumentos de planejamento estabelecidos pela Instrução Normativa nº 81/2022 (Art. 7º), garantindo assim a otimização dos processos e a observância dos princípios da administração pública.

28.15. **CASOS OMISSOS**

28.15.1. Fica estabelecido, caso venha ocorrer algum fato não previsto neste termo de referência e seus anexos, os chamados casos omissos, estes serão dirimidos respeitado o objeto dessa licitação, por meio de aplicação da legislação e demais normas reguladoras da matéria, em especial a lei nº 14.133/21, aplicando-se paralelamente, quando for o caso, supletivamente, os princípios da teoria geral dos contratos estabelecidos na legislação civil brasileira e as disposições de direito privado.

29. PLANILHA DE COMPOSIÇÃO DE CUSTOS E FORMAÇÃO DE PREÇOS

29.1. O objeto da presente licitação e sua forma de contratação não exigem a confecção de planilha de composição de custos e formação de preços, conforme Art. 42, inciso XXX, do Decreto Estadual No. 28.874/2024.

30. SISTEMA DE REGISTRO DE PREÇOS

30.1. **JUSTIFICATIVA PARA ESCOLHA DO SISTEMA DE REGISTRO DE PREÇO:**

30.1.1. Sabe-se que o registro de preço é uma das modalidades de escolha para as aquisições públicas pelas características que se impõem através do Art. 40 da Lei 14.133/21.

30.1.2. O registro de preços é um sistema que visa a uma racionalização nos processos de contratação de compras públicas e de prestação de serviços. Sua finalidade precípua é maximizar o princípio da economicidade, permitindo à Administração Pública celebrar o contrato administrativo na exata medida e no momento de sua necessidade, sempre precedido de licitação, qualquer que seja o valor efetivo a ser praticado em cada situação específica.

30.1.3. A quantidade mínima a ser solicitada de cada item será de 10% do valor previsto para cada item.

30.1.4. No registro de preços não há obrigatoriedade de aquisição de todo o quantitativo licitado. Os valores registrados não são exclusivos para determinadas secretarias ou entidades e podem ser compartilhados por toda a administração, dentro dos limites esculpidos pela legislação.

30.1.5. Faz-se necessário o Registro de Preços, a fim de evitar a falta de estoque, proporcionando maior agilidade e qualidade nos serviços prestados a população.

30.1.6. Levando em conta as prerrogativas acima descritas JUSTIFICA-SE a necessidade do registro de preços para pretensa aquisição constante neste termo de referência conforme discriminação e quantitativos estabelecidos.

30.1.7. O órgão gerenciador da Ata de Registro de Preço será a Coordenadoria do Sistema de Registro de Preço-CRP/SUPEL/RO.

30.2. **REGISTRO DE PREÇOS**

30.2.1. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente motivada.

30.2.2. Fica a Detentora ciente que a publicidade da ata de registro de preços na imprensa oficial terá efeito de compromisso nas condições ofertadas e pactuadas na proposta apresentada à licitação.

30.2.3. A Ata de Registro de Preços, os ajustes dela decorrentes, suas alterações e rescisões obedecerão a Lei Federal nº 14.133/21 demais normas complementares e disposições desta Ata e do Edital que a precedeu, aplicáveis à execução e especialmente aos casos omissos.

30.3. **GERENCIAMENTO DA ATA DE REGISTRO DE PREÇOS**

30.3.1. A Superintendência Estadual de Compras e Licitações – SUPEL, será o órgão responsável pelos atos de administração, controle e gerenciamento da Ata de Registro de Preços, conforme Art. 122 do Decreto Estadual nº. 28.874, de 25 de janeiro de 2024, conforme versa abaixo:

> Art. 122.Caberá ao órgão gerenciador, órgão competente para operacionalizar os procedimentos licitatórios no âmbito da Administração Pública, a prática de todos os atos de controle e administração do SRP, e ainda o seguinte:
>
> II - consolidar todas as informações relativas a estimativa individual e total de consumo encaminhadas pelos órgãos participantes para atender aos requisitos de padronização e racionalização;
>
> III - elaborar o projeto básico ou termo de referência do registro de preços fruto da intenção;
>
> IV - promover todos os atos necessários à instrução processual para a realização do procedimento licitatório de intenção de registro de preços;
>
> V - realizar levantamento de mercado e pesquisa de preço ampla e diversificada para elaboração da estimativa orçamentária, devendo zelar pela maior amplitude possível das fontes pesquisadas;
>
> VI - confirmar junto aos órgãos participantes a sua concordância com o objeto a ser licitado, inclusive quanto aos quantitativos e projeto básico;
>
> VII - realizar todo procedimento licitatório, bem como os atos dele decorrentes;
>
> VIII - gerenciar a ata de registro de preços, providenciando a indicação, sempre que solicitado, dos fornecedores, para atendimento às necessidades da Administração, obedecendo a ordem de classificação e os quantitativos de contratação definidos pelos órgãos participantes;
>
> IX - conduzir os procedimentos relativos a eventuais renegociações dos preços registrados e a aplicação de penalidades por descumprimento do pactuado na ata de registro de preços;
>
> X - analisar as solicitações de adesão formuladas pelos órgãos não participantes;
>
> XI - zelar pela observância dos limites individual e global para adesão;
>
> XII - divulgar o conteúdo do edital, da ata de registro de preços, os eventuais contratos e termos aditivos, na Imprensa Oficial, no sítio eletrônico do Estado e no Portal Nacional de Contratações Públicas, conforme as diretrizes da Lei Federal n° 14.133, de 2021.
>
> § 1°A análise das solicitações de adesão deverá ser precedida de levantamento de mercado e pesquisa de preço para aferição do valor do objeto registrado com base no quantitativo resultante da adesão, apresentado por ato próprio da unidade aderente.
>
> § 2°A constatação de preço mais vantajoso em decorrência da pesquisa referida no parágrafo anterior, identificada e informada pela unidade de origem, acarretará a necessidade de repactuação do preço registrado.
>
> § 3°Não havendo êxito nas negociações, o órgão gerenciador não autorizará a adesão.

30.4. **DA INTENÇÃO DE REGISTRO DE PREÇOS - IRP**

30.4.1. A Superintendência Estadual de Compras e Licitações – SUPEL ficará responsável pela intenção de registro de preços, conforme preconiza o Art. 122 do Decreto Estadual 28.874/2024:

> Art. 122. Caberá ao órgão gerenciador, órgão competente para operacionalizar os procedimentos licitatórios no âmbito da Administração Pública, a prática de todos os atos de controle e administração do SRP, e ainda o seguinte:
>
> **I - realizar o procedimento de intenção de registro na forma do art. 124;**

30.5. **UTILIZAÇÃO DA ATA E DO FORNECIMENTO ADICIONAL "CARONAS"**

30.5.1. De acordo com o Artigo 124 do Decreto Estadual n° 28.874/24, durante a sua vigência, a utilização de ata de registro de preço por órgão não participante está sujeita à prévia autorização do órgão gerenciador.

30.5.2. **Conforme disposto no art. 121 do decreto estadual 28.874/2024, o limite individual da cada órgão ou entidade não participante será de um aumento de 50% do quantitativo registrado, ressalvado o disposto no ressalvado o disposto no art. 86, § 7°, da Lei Federal n° 14.133, de 2021.**

30.5.3. **O conjunto de solicitações de adesão, independente do órgão ou entidade solicitante, não poderá exceder ao limite global de duas vezes o quantitativo registrado, conforme art. 121 do Decreto Estadual n° 28.874/24.**

30.5.4. **A quantidade mínima para cada ordem de fornecimento, será de 10% do quantitativo registrado, conforme art. 121 do Decreto Estadual n° 28.874/24.**

30.5.5. É facultada aos órgãos ou entidades municipais, distritais ou estaduais a adesão à ata de registro de preços dos órgãos e entidades da União, dos Estados- Membros e do Distrito Federal, desde que os preços sejam compatíveis com os praticados no mercado e seja demonstrada a vantagem da adesão.

30.5.6. Por se tratar de pregão de menor preço por lote, a adesão à ata só pode ocorrer globalmente no lote registrado.

30.5.7. Caso haja adesão de itens individualizados, estes devem corresponder à proposta de menor valor, sob pena de inviabilidade da adesão

30.5.8. A utilização da ata de registro de preço por órgão não participante está sujeita a prévia autorização do órgão gerenciador.

30.6. **VIGÊNCIA DA ATA DE REGISTRO DE PREÇO**

30.6.1. Os contratos decorrentes da Ata de Registro de Preços terão sua vigência conforme as disposições contidas no art. 84 da Lei 14.133/21.

30.6.2. Conforme art. 125 do Decreto Estadual n° 28.874/2024, o prazo de vigência da ata de registro de preços será de 12 (doze) meses e poderá ser prorrogado, por igual período, desde que comprovada a vantajosidade do preço registrado, mediante pesquisa de mercado que leve em consideração os parâmetros fixados no art. 51, do mesmo decreto.

30.7. **ALTERAÇÃO DA ATA DE REGISTRO DE PREÇOS**

30.7.1. Os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos serviços ou bens registrados, cabendo ao órgão gerenciador promover as negociações junto aos fornecedores, observadas as disposições contidas na alínea "d" do inciso II do caput do artigo 124 da Lei 14.133/21.

30.7.2. Quando o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, o órgão gerenciador convocará os fornecedores para negociarem a redução dos preços aos valores praticados pelo mercado.

30.7.3. Os fornecedores que não aceitarem reduzir seus preços aos valores praticados pelo mercado serão liberados do compromisso assumido, sem aplicação de penalidade.

30.7.4. A ordem de classificação dos fornecedores que aceitarem reduzir seus preços aos valores de mercado observará a classificação original.

30.7.5. Quando o preço de mercado tornar-se superior aos preços registrados, e o fornecedor não puder cumprir o compromisso, o órgão gerenciador poderá:

30.7.6. Liberar o fornecedor do compromisso assumido, caso a comunicação ocorra antes do pedido de fornecimento, sem aplicação de penalidade se confirmada à veracidade dos motivos e comprovantes.

30.7.7. Convocar os demais fornecedores para assegurar igual oportunidade de negociação.

30.7.8. Não havendo êxito nas negociações, o órgão gerenciador deverá proceder à revogação do item da ata de registro de preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

30.7.9. Art. 132 do Decreto Estadual n. 28.874/2024 , as eventuais alterações da ata de registro de preços não poderão acarretar aumento dos quantitativos registrados, inclusive, nas hipóteses previstas no art. 124 da Lei Federal n° 14.133, de 2021. (Redação do parágrafo dada pelo Decreto Nº 28.874 de 25/01/2024).

30.7.10. Com relação às supressões, conforme previsto no § 1°, do Art. 124, da Lei Federal nº. 14.133/21, o objeto da presente licitação poderá sofrer supressões.

30.8. **DO CANCELAMENTO DO REGISTRO**

30.8.1. Os preços registrados poderão ser revisto em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução tal como pactuado, observada a instrução processual respectiva, cabendo ao órgão gerenciador promover as negociações junto aos fornecedores, conforme disposto no art. 133 do Decreto Estadual n° 28.874 de 25 de janeiro de 2024.

30.8.2. Os preços registrados serão mantidos inalterados por todo o período de vigência da Ata de Registro de Preços - ARP, admitida sua revisão para majorar ou minorar os preços registrados em casos excepcionais, nas hipóteses legais e considerando os preços vigentes de mercado.

30.8.3. A revisão de preços precederá de requerimento: I - do detentor da ata, que deverá fazê-la antes do pedido de fornecimento e, instruindo seu pedido com documentação probatória de majoração de preço do mercado e a oneração de custos; ou II - pelo órgão participante ou órgão interessado, comprovando por meio de pesquisas de preços que há minoração do valor originalmente registrado.

30.8.4. Quando o preço inicialmente registrado, por motivo superveniente, tornar-se superior ao preço praticado no

mercado o órgão gerenciador convocará o fornecedor visando a negociação para redução de preços e sua adequação ao praticado pelo mercado e, caso este não aceite a redução dos seus preços aos valores praticados pelo mercado será liberado dos compromissos assumidos, sem aplicação de penalidades administrativas, nos termo do art. 134, § 1º do Decreto Estadual n° 28.874/2024.

30.8.5. Se não houver prova efetiva da desatualização dos preços registrados e da existência de fato superveniente, o fornecedor continuará obrigado a cumprir os compromissos pelo valor registrado na ata, sob pena de cancelamento do registro de preços e de aplicação das penalidades administrativas previstas em lei e no edital, nos termos do art. 135, § 2º do Decreto Estadual n° 28.874/2024.

30.8.6. Na hipótese do cancelamento do registro de preços prevista no art. 135, § 2º do Decreto Estadual n° 28.874/2024, o órgão gerenciador poderá convocar os demais fornecedores integrantes do cadastro de reserva para que manifestem interesse em assumir o fornecimento dos bens, a execução das obras ou dos serviços, pelo preço registrado na ata.

30.8.7. Caso comprovada a desatualização dos preços registrados decorrente de fato superveniente que prejudique o cumprimento da ata, poderá ser efetuada a atualização do preço registrado, adequando-o aos valores praticados no mercado.

30.8.8. O órgão gerenciador, em alternativa à atualização prevista no item 5.6 desta Ata de Registro de Preços, poderá liberar o fornecedor do compromisso sem aplicação de penalidades, convocando, posteriormente, os licitantes remanescentes, na ordem de classificação, para negociação e assinatura da ata no máximo nas condições ofertadas por estes, desde que o valor seja igual ou inferior ao orçamento estimado para a contratação, inclusive quanto aos preços atualizados, nos termos do instrumento convocatório.

30.8.9. A redução do preço registrado será comunicada pelo órgão gerenciador aos órgãos que tiverem formalizado contratos com fundamento no respectivo registro, para que avaliem a necessidade de efetuar a revisão dos preços contratados.

30.8.10. O cancelamento do preço registrado, em conformidade com o artigo 136 do Decreto Estadual n° 28.874/2024, poderá ocorrer por fato superveniente decorrente de caso fortuito ou força maior que prejudique o cumprimento da ata, devidamente comprovados e justificados, por razão de interesse público ou a pedido do fornecedor.

30.8.11. O preço registrado, em atenção ao estabelecido pelo art. 136, inc. I a V do Decreto Estadual n° 28.874/2024, também poderá ser cancelado quando o fornecedor descumprir total ou parcialmente as condições previstas na Ata de Registro de Preços, não retirar a nota de empenho ou instrumento equivalente no prazo estabelecido pela Administração, não aceitar reduzir o seu preço registrado na hipótese deste se tornar superior aqueles praticados no mercado ou sofrer sanção prevista na forma do Decreto Estadual n° 28.874/2024 em seu Capítulo VIII.

30.9. **OBRIGAÇÕES DA DETENTORA DA ATA**

30.9.1. Em conformidade com o disposto no art. 42, §1º, VII, do Decreto Estadual nº 28.874, de 2024, a detentora da ata de registro de preços deverá:

> Art. 42.O termo de referência é documento obrigatório para todos os processos licitatórios e contratações diretas destinados a aquisições de bens e contratação de serviços, inclusive serviços comuns de engenharia, quando possível, devendo os demais casos observar a obrigatoriedade de elaboração de projeto básico, excetuando-se a hipótese prevista no § 1º do artigo anterior devendo conter, no que couber, os seguintes parâmetros e elementos descritivos, dentre outros que se fizerem necessários:
>
> VII - modelo de execução do objeto, que consiste na definição de como o contrato deverá produzir os resultados pretendidos desde o seu início até o seu encerramento, incluindo as informações de prazo de início da prestação, local, regras para o recebimento provisório e definitivo, quando for o caso, incluindo regras para a inspeção, se aplicável, e demais condições necessárias para a execução dos serviços ou o fornecimento de bens;

30.9.2. Cumprir os prazos de entrega dos itens contratados, conforme estabelecido na ata e no Termo de Referência.

30.9.3. Manter a qualidade e as especificações dos produtos/serviços, conforme previamente acordado e detalhado no edital e na ata.

30.9.4. Apresentar relatórios de fornecimento e desempenho sempre que solicitado pelos órgãos/entidades participantes.

30.9.5. Notificar imediatamente os órgãos/entidades participantes sobre quaisquer dificuldades que possam comprometer o cumprimento das obrigações assumidas.

30.9.6. Atender às demandas dos órgãos/entidades participantes, conforme a necessidade de aquisição, respeitando as condições e limites estabelecidos.

30.9.7. O não cumprimento das obrigações aqui estabelecidas poderá acarretar penalidades, conforme a legislação vigente e as disposições do Termo de Referência.

30.9.8. Órgão ou entidade participante participa dos procedimentos iniciais da contratação para registro de preços e integra a ata de registro de preços;

30.10. **REGISTRO DE MAIS DE UM FORNECEDOR**

30.10.1. A possibilidade de registro de mais de um fornecedor ou prestador de serviço, desde que aceitem cotar o objeto em preço igual ao do licitante vencedor, assegurada a preferência de contratação de acordo com a ordem de

classificação

30.10.2. Para atender ao disposto no art. 82, VII, da Lei Federal nº 14.133, de 2021, fica estabelecida a possibilidade de registro de mais de um fornecedor na ata de registro de preços, conforme as seguintes condições:

30.10.3. Diversidade de Fornecedores: O registro poderá contemplar diferentes fornecedores que apresentem propostas dentro das especificações técnicas e condições de preço estabelecidas neste Termo de Referência.

30.10.4. Critérios de Seleção: A seleção dos fornecedores será realizada com base em critérios de habilitação e classificação, levando em consideração a melhor proposta apresentada em termos de preço e qualidade.

30.10.5. Acesso aos Fornecedores: Todos os fornecedores registrados poderão ser convocados para atender às demandas dos órgãos/entidades participantes, conforme a necessidade de aquisição e o cumprimento das condições da ata.

30.10.6. Os detalhes sobre o número máximo de fornecedores a serem registrados e as condições para convocação serão especificados na fase de execução da ata.

30.11. **DOS ÓRGÃOS E ENTIDADES PARTICIPANTES**

30.11.1. Faz parte desta Ata de Registro de Preços a Secretaria de Estado da Saúde - SESAU.

31. **ANEXOS**

*** ANEXO I - MINUTA DE CONTRATO**

*** ANEXO II - MANUAL DE GESTÃO E FISCALIZAÇÃO (0051378718)**

*** ANEXO III - MAPA DE RISCO (0050881188)**

*** ANEXO IV - MATRIZ DE RISCO (0050880812)**

Porto Velho, 24 de março de 2025.

Elaborado por:
JOELMA DA SILVA TELES
Assessor - GECOMP/SESAU

Revisado por:
LUCAS MATHEUS TELES
Responsável Núcleo de Serviços Continuados - GECOMP/SESAU

MARCOS ALESSANDRO FERNANDES SALES
Gerente de Compras em substituição - GECOMP/SESAU
Portaria 1457 (0058061956)

Revisado por:
COORDENADORIA DE INOVAÇÃO E TECNOLOGIA DA INFORMAÇÃO - CITI

Declaro e dou fé no presente Termo de Referência e Anexos:

(Assinado Eletronicamente)

ADRIANO FLORES MESSIAS DA SILVA
Secretário Executivo de Estado da Saúde em Substituição
Portaria Nº 1768 de 20 de Março de 2025 (0058448160)

ANEXO I

MINUTA DO CONTRATO

CONTRATANTE: O ESTADO DE RONDÔNIA, por intermédio da (ÓRGÃO CONTRATANTE), inscrita no CNPJ/MF sob o n° (00.000.000/0001-00), com sede na Rua Farquar, n° 2986, Complexo Rio Madeira, Bairro Pedrinhas, nesta cidade de Porto Velho-RO, representada pelo (CARGO DO REPRESENTANTE), o Sr. ou Sr(a) (REPRESENTANTE DO ÓRGÃO), portador(a) do CPF/MF nº (000.000.000-00).

CONTRATADA: (NOME DA EMPRESA), inscrita no CNPJ/MF sob n° (00.000.000/0001-00), com endereço na Rua (ENDEREÇO EMPRESARIAL), aqui representada por seu (CARGO), o Sr. ou Sr(a) (REPRESENTANTE EMPRESARIAL), portador(a) do CPF/MF n° (000.000.000-00), de acordo com a representação legal que lhe é outorgada.

Os Contratantes celebram, por força do presente instrumento, CONTRATO DE (DESCRIÇÃO DO SERVIÇO), o qual se regerá pelas disposições da Lei nº 14.133/21 e demais normas pertinentes, licitado através da (MODALIDADE DE LICITAÇÃO), vinculando-se aos termos do Processo Administrativo n° (NÚMERO DO PROCESSO), e à proposta da CONTRATADA, mediante as seguintes cláusulas:

1. CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O objeto do presente instrumento é a (DESCRIÇÃO DO OBJETO), nas condições estabelecidas no Termo de Referência, Edital e seus anexos.

1.2. **Da Vinculação**:

1.2.1. Integram este Contrato além do Termo de Referência, as normas do Edital de Licitação (MODALIDADE DE LICITAÇÃO), e a proposta da CONTRATADA, independentemente de transcrição.

2. CLÁUSULA SEGUNDA – DO DETALHAMENTO DO OBJETO

2.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

3. CLÁUSULA TERCEIRA – DA EXECUÇÃO DO SERVIÇO

3.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

4. CLÁUSULA QUARTA – DAS CONDIÇÕES DE RECEBIMENTO DO OBJETO

4.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

5. CLÁUSULA QUINTA – DA GARANTIA

5.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

6. CLÁUSULA SEXTA – DA VIGÊNCIA

6.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

7. CLÁUSULA SÉTIMA – DO VALOR E DOTAÇÃO ORÇAMENTÁRIA

7.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

8. CLÁUSULA OITAVA – DAS CONDIÇÕES DE PAGAMENTO

8.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

9. CLÁUSULA NONA – DA FISCALIZAÇÃO

9.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

10. CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DA CONTRATADA

10.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

11. CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DA CONTRATANTE

11.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

12. CLÁUSULA DÉCIMA SEGUNDA – DAS SANÇÕES E PENALIDADES

12.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

13. CLÁUSULA DÉCIMA TERCEIRA – DO REAJUSTE, ACRÉSCIMO E SUPRESSÃO (SE HOUVER)

13.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

14. CLÁUSULA DÉCIMA QUARTA – DA RESCISÃO CONTRATUAL

14.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

15. CLÁUSULA DÉCIMA QUINTA – MATRIZ DE RISCOS

15.1 - Na hipótese de ocorrência de um dos eventos listados no Anexo - Matriz de Riscos deste Contrato, a CONTRATADA deverá, no prazo de 01 (um) dia útil, informar a SESAU/RO sobre o ocorrido, contendo as seguintes informações mínimas:
a) Detalhamento do evento ocorrido, incluindo sua natureza, a data da ocorrência e sua duração estimada;

b) As medidas que estavam em vigor para mitigar o risco de materialização do evento, quando houver;
c) As medidas que irá tomar para fazer cessar os efeitos do evento e o prazo estimado para que esses efeitos cessem;
d) As obrigações contratuais que não foram cumpridas ou que não irão ser cumpridas em razão do evento; e,
e) Outras informações relevantes.
15.1.1 - Após a notificação, a SESAU/RO decidirá quanto ao ocorrido ou poderá solicitar esclarecimentos adicionais a CONTRATADA. Em sua decisão a SESAU/RO poderá isentar temporariamente a CONTRATADA do cumprimento das obrigações contratuais afetadas pelo Evento.
15.1.2 - A concessão de qualquer isenção não exclui a possibilidade de aplicação das sanções previstas na Cláusula contratual respectiva.
15.1.3 - O reconhecimento pela SESAU/RO dos eventos descritos na Matriz de Riscos deste Contrato que afetem o cumprimento das obrigações contratuais, com responsabilidade indicada exclusivamente a CONTRATADA, não dará ensejo a recomposição do equilíbrio econômico financeiro do Contrato, devendo o risco ser suportado exclusivamente pela CONTRATADA.
15.2 - As obrigações contratuais afetadas por caso fortuito, fato do príncipe ou força maior deverão ser comunicadas pelas partes em até 01 (um) dia útil, contados da data da ocorrência do evento.
15.2.1 - As partes deverão acordar a forma e o prazo para resolução do ocorrido.
15.2.2 - As partes não serão consideradas inadimplentes em razão do descumprimento contratual decorrente de caso fortuito, fato do príncipe ou força maior.
15.2.3 - Avaliada a gravidade do evento, as partes, mediante acordo, decidirão quanto a recomposição do equilíbrio econômico financeiro do Contrato, salvo se as consequências do evento sejam cobertas por Seguro, se houver.
15.2.3.1 - O Contrato poderá ser rescindido, quando demonstrado que todas as medidas para sanar os efeitos foram tomadas e mesmo assim a manutenção do contrato se tornar impossível ou inviável nas condições existentes ou é excessivamente onerosa.
15.2.4 - As partes se comprometem a empregar todas as medidas e ações necessárias a fim de minimizar os efeitos advindos dos eventos de caso fortuito, fato do príncipe ou força maior.
15.3 - Os fatos imprevisíveis, ou previsíveis, porém de consequências incalculáveis, retardadores ou impeditivos da execução do contrato, não previstos na Matriz de Riscos, serão decididos mediante acordo entre as partes, no que diz respeito à recomposição do equilíbrio econômico financeiro do contrato.

16. CLÁUSULA DÉCIMA SEXTA - DA FRAUDE E CORRUPÇÃO

16.1. A CONTRATADA deverá observar os mais altos padrões éticos durante a execução do Contrato, estando sujeitas às sanções previstas na legislação em caso de inobservância.

17. CLÁUSULA DÉCIMA SÉTIMA – DOS CASOS OMISSOS

17.1. As omissões, dúvidas e casos não previstos neste instrumento, serão resolvidos e decididos aplicando-se as regras da Lei nº 14.133/21 e suas alterações, bem como demais ordenamentos jurídicos correlatos, levando-se sempre em consideração os princípios que regem a administração pública.

18. CLÁUSULA DÉCIMA OITAVA – DA PUBLICAÇÃO

18.1. Incumbirá à CONTRATANTE, através da Procuradoria Geral do Estado, providenciar a publicação deste instrumento, por extrato, no Diário Oficial do Estado de Rondônia, no prazo previsto na Lei nº 14.133/21.

19. CLÁUSULA DÉCIMA NONA – DO FORO

19.1. Fica eleito pelas partes o Foro da Comarca de Porto Velho, Capital do Estado de Rondônia, para dirimir todas e quaisquer questões oriundas do presente ajuste, inclusive às questões entre a CONTRATADA e a CONTRATANTE, decorrentes da execução deste CONTRATO, com renúncia expressa de qualquer outro, por mais privilegiado que seja.

20. CLÁUSULA VIGÉSIMA - DAS DISPOSIÇÕES GERAIS

20.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

Para firmeza e como prova do acordado, é lavrado o presente Contrato, o qual, depois de lido e achado conforme, vai assinado pelas partes, dele sendo extraídas as cópias que se fizerem necessárias para sua publicação e execução, devidamente certificadas pela Procuradoria Geral do Estado.

Porto Velho/RO, _____de_____ de 2024.

_____
Titular da Contratante

_____
Titular da contratada

_____
Procurador do Estado de Rondônia

ANEXO II

MANUAL DE GESTÃO E FISCALIZAÇÃO DE CONTRATOS ADMINISTRATIVOS (0051378718)

	Documento assinado eletronicamente por **Lucas Matheus Teles da Conceição**, **Chefe de Núcleo**, em 24/03/2025, às 13:08, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.
	Documento assinado eletronicamente por **Patrick Hebert da Silva**, **Coordenador(a)**, em 24/03/2025, às 17:04, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.
	Documento assinado eletronicamente por **Joelma Da Silva Teles**, **Assessor(a)**, em 25/03/2025, às 09:14, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.
	Documento assinado eletronicamente por **Marcos Alessandro Fernandes Sales**, **Subgerente**, em 25/03/2025, às 11:12, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.
	Documento assinado eletronicamente por **Adriano Flores Messias da Silva**, **Secretário(a) Executivo(a)**, em 27/03/2025, às 17:10, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.
	A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **0058196040** e o código CRC **235091EB**.

Referência: Caso responda este Termo de Referência, indicar expressamente o Processo nº 0036.014359/2024-32 SEI nº 0058196040