CONTRATO N.º463/2023

CONTRATO QUE ENTRE SI CELEBRAM O MUNICÍPIO DE BELÉM, POR INTERMÉDIO DA SECRETARIA MUNICIPAL DE SAÚDE – SESMA, E A EMPRESA OI S.A., EM RECUPERAÇÃO JUDICIAL, SOCIEDADE ANÔNIMA PARA OS FINS ABAIXO DECLARADOS.

O **MUNICÍPIO DE BELÉM**, por intermédio da **SECRETARIA MUNICIPAL DE SAÚDE – SESMA**, com sede na Av. Governador José Malcher, 2821 (entre Av. Almirante Barroso e Av. José Bonifácio), bairro: São Brás, CEP: 66.090-100, Belém/PA, inscrita no CNPJ/MF sob o nº 07.917.818/0001-12, neste ato representado por seu titular, **Sr. PEDRO RIBEIRO ANAISSE**, brasileiro, casado, economista, portador do RG nº 2377948 SEGUP/PA, e inscrito no CPF nº 184.227.302-78, residente e domiciliado nesta capital, doravante denominado **CONTRATANTE** e de outro lado, a empresa **OI S.A.**, **EM RECUPERAÇÃO JUDICIAL, SOCIEDADE ANÔNIMA**, , inscrita no **CNPJ (MF) nº 76.535.764/0001-43**, com sede na Cidade do Rio de Janeiro, Estado do Rio de Janeiro, na Rua do Lavradio, 71, 2º andar, Bairro Centro, CEP 20230-070, inscrita no, neste ato representada pelo Executivo de Negócios **SR. BRUCY MARTINS COSTA, CPF Nº 400.897.972-72, Identidade nº 2760282-SSP-PA e pelo** Gerente de Vendas **o Sr. GUSTAVO GIRALDES BETTONI, CPF Nº 003.773.439-35, RG 39471558 SSP-PR**, doravante denominada **CONTRATADA**, resolvem de comum acordo e na melhor forma de direito celebrar o presente **CONTRATO** em regime de execução indireta, **Adesão a ATA de registro de preços da Procuradoria Geral do Estado do Amapá nº 169/2022 – CLC/PGE**, **Gdoc 13347/2023**, mediante as cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA – DO FUNDAMENTO LEGAL

1.1. Este Contrato é firmado em observância as disposições contidas no art. 37, inciso XXI da Constituição Federal do Brasil de 1988; Lei nº 10.520/2002; Lei Complementar n.º 123/2006; Lei Complementar Estadual n.º 108/2018; Decreto Federal n.º 8.538/2015; Decreto Estadual n.º 2.648/2007 e, subsidiariamente, no que couber pela Lei n.º 8.666/1993 e Lei nº 8.078/1990 (CDC), bem como, pelas legislações correlatas e demais exigências estabelecidas no Edital do Pregão Eletrônico nº 082/2022-CLC/PGE e seus anexos, **Gdoc 13347/2023**.

CLÁUSULA SEGUNDA – DO OBJETO

2.1. O presente contrato tem por objeto a **PRESTAÇÃO DE SERVIÇOS DE COMUNICAÇÃO CORPORATIVA DE LINK DE INTERNET, SERVIÇO SDWAN, GERENCIA DE REDE PROATIVA, SOLUÇÃO DE CONECTIVIDADE WIFI LANE SERVIÇO DE NOC (NETWORK OPERATION CENTER), VISANDO ATENDER ÀS NECESSIDADES DOS ESTABELECIMENTOS E ENTIDADES DA SECRETARIA MUNICIPAL DE SAÚDE DE BELÉM, ADESÃO A ATA DE REGISTRO DE PREÇOS DA PROCURADORIA GERAL DO ESTADO DE REGISTRO DE PREÇO DE N º 169/2022 – CLC/PGE.**

2.2. O presente contrato será executado em regime de empreitada por preço unitário.

CLÁUSULA TERCEIRA – DOCUMENTOS INTEGRANTES

3.1. Fazem parte integrante deste CONTRATO, independentemente de sua transcrição, os documentos constantes no **Gdoc 13347/2023**, os abaixo relacionados:

a) Termo de Referência e apêndices;
b) Edital de Pregão Eletrônico nº 082/2022-CLC/PGE;
c) Pareceres Jurídicos da fase interna e externa;
d) Proposta da Contradada, adjudicada e homologada;
e) Resultado da Licitação.
f) Ata de registro de preços

CLÁUSULA QUARTA – DA DOTAÇÃO ORÇAMENTÁRIA E DO PREÇO

4.1. As despesas decorrentes deste Contrato correrão por conta da seguinte Dotação Orçamentária:

Função Programática:2.09.22.10.302.0001
Atividade: 2217
Fonte: 1500100200
Elemento de despesa: 33.90.39

Função Programática:2.09.22.10.122.0007
Atividade: 2311
Fonte: 1500100200
Elemento de despesa: 33.90.39

Função Programática:2.09.22.10.302.0001
Atividade: 2217
Fonte: 1600020000
Elemento de despesa: 33.90.39

Função Programática:2.09.22.10.302.0001
Atividade: 2217
Fonte: 1621020000
Elemento de despesa: 33.90.39

Função Programática:2.09.22.10.301.0001
Atividade: 1169
Fonte: 1600010000
Elemento de despesa: 33.90.39

4.2. O valor da presente contratação **é de R$106.424,19 (Cento e seis mil quatrocentos e vinte e quatro reais e dezenove centavos),** que será pago de acordo com a certificação do serviço.

CLÁUSULA QUINTA – DO PAGAMENTO

5.1. O pagamento será efetuado em até 30 (trinta) dias, após o regular fornecimento do objeto, mediante o processamento normal de liquidação e liberação dos recursos financeiros pela Secretaria Municipal de Saúde de Belém.

5.2. Deverá ser fornecida nota fiscal fatura de serviços, discriminando de forma detalhada, todo e qualquer registro relacionado com a prestação do serviço do período, em meio físico e/ou meio eletrônico, totalizada e discriminada individualmente de forma não contínua, por acesso, de acordo com a quantidade especificada em cada item;

5.3. A nota fiscal fatura de serviços deverá ser entregue, com antecedência mínima de 5 (cinco) dias da data do vencimento;

5.4. A Empresa apresentará a Nota Fiscal (is)/Fatura(s) referente(s) ao(s) objeto(s) regularmente fornecido(s), acompanhada(s) dos documentos de habilitação perante a Fazenda Federal, Estadual e Municipal, INSS, FGTS e Ministério do Trabalho (CNDT) junto a Administração Contratante, para sua devida certificação, conforme disposto o art. 29 da Lei n.º 8.666, de 1993, e no Art. 7º do Decreto Estadual nº 1.278, de 17 de fevereiro de 2011;

5.5. O pagamento será creditado em favor da contratada, através de ordem bancária, na entidade bancária indicada na proposta, cabendo ao interessado informar com clareza o nome do banco, assim como os números da respectiva agência e da conta corrente em que deverá ser efetivado o crédito;

5.6. A Administração reserva-se ao direito de descontar da(s) Nota(s) Fiscal(is)/Fatura(s) a serem pagas, qualquer débito existente da empresa em consequência de penalidade aplicada durante o fornecimento do objeto;

5.7. Nenhum pagamento será efetuado à contratada, enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência, sem que isto gere direito ao pleito de reajustamento ou correção monetária do valor inicial;

5.8. A Contratada poderá realizar o bloqueio da prestação dos serviços, em caso de inadimplemento por parte da Contratante, depois de decorridos 90 (noventa) dias da data de vencimento, condicionando o desbloqueio ao pagamento do valor da fatura em atraso.

5.9. Quando ocorrerem 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:

EM = I x N x VP, onde:
I = Índice de atualização financeira;
I = (TX/100)360
I= (6/100)/360 = 0,00016438
TX = Percentual da taxa de juros de mora anual (= 6%);
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.

5.10. Eventuais discussões sobre condições de pagamento devem seguir as regras estabelecidas no Termo de Referência anexo a este Edital.

CLÁUSULA SEXTA – DA PRESTAÇÃO DOS SERVIÇOS

6.1. ESPECIFICAÇÕES TÉCNICAS MÍNIMAS E QUANTIDADES

6.1.1. O serviço a ser prestado deverá atender as especificações técnicas mínimas e quantidades constantes no Anexo I do Termo de Referência, conforme abaixo:

LOTE 1				
ITEM	**VELOCIDADE**	**QUANT.**	**VALOR UNIT**	**VALOR MENSAL**
1	IP 20Mbps	8	R$ 1.495,74	R$ 11.965,92
15	BANDA LARGA	77	R$ 840,00	R$ 64.680,00
VALOR TOTAL MENSAL				**R$ 76.645,92**

LOTE 2				
ITEM	**VELOCIDADE**	**QUANT.**	**VALOR UNIT**	**VALOR MENSAL**
3	IP 500Mbps	1	R$ 8.778,27	R$ 8.778,27
12	BANDA LARGA	25	R$ 840,00	R$ 21.000,00
VALOR TOTAL MENSAL				**R$ 29.778,27**

VALOR TOTAL MENSAL LOTE 1 E 2	**R$ 106.424,19**

6.2. DO SERVIÇO DE COMUNICAÇÃO DE DADOS MULTIMÍDIA

6.2.1. As modalidades de serviços de comunicação foram caracterizadas em função de parâmetros técnicos, forma de interligação de cada unidade remota, das características dos serviços (aplicações) que
poderão ser utilizados pela Contratante, e ainda, em função da tecnologia de transmissão adotada. Cada unidade poderá contratar mais de uma tecnologia, modalidade de serviços, classes de acordo de nível de serviço (SLA) e itens ofertados neste documento;

6.2.2. Os serviços de ativação, mudança de endereço, alteração de velocidade e outros estará sujeito à viabilidade técnica para atendimento, onde a Contratada deverá arcar com os respectivos custos, desde que não seja necessário o desenvolvimento de projetos especiais para atendimento.

6.2.3. As modalidades de serviço de comunicação são:

6.2.3.1. SERVIÇO DE COMUNICAÇÃO PARA INTERLIGAÇÃO AO BACKBONE DE INTERNET MUNDIAL (INTERNET)

I. Serviço de comunicação de dados, em unidade de banda discriminada a seguir, interligando cada uma das Unidades da Contratada com a rede mundial de computadores – Internet, através de uma ou mais das seguintes tecnologias: IP/MPLS, ou Metroethernet, ou banda larga ou outras tecnologias de acesso terrestre, com acessos de última milha terrestre, sendo aceito também múltiplos acessos para composição do serviço ao site;

II. Em caso de excepcionalidade em locais onde não haja viabilidade de conexão através de tecnologia acesse terrestre, poderá ser aceito mediante autorização previa do órgão contratante a solução de conexão via satélite sendo aceito as características técnicas de velocidade, latência e atendimento inerentes da solução;

III. Será admitida a utilização de atendimento em last mile e redes neutras na composição da solução de conectividade tendo a contratada total responsabilidade no cumprimento dos índices de qualidade técnica e atendimento aos SLA's definidos neste Contrato e seus anexos.

6.2.3.2. ACORDOS DE NÍVEL DE SERVIÇO (SLA)

6.2.3.2.1. SERVIÇO DE INTERNET TERRESTRE

I. Os acessos devem, obrigatoriamente, utilizar no acesso à Internet, uma ou mais das seguintes tecnologias: Frame-Relay, ATM, MetroEthernet, Banda larga ou outras tecnologias terrestres, suportando o protocolo TCP/IP, com acessos de última milha terrestre, sendo aceito também múltiplos acessos para composição do serviço ao site.

REQUISITOS OBRIGATÓRIOS REFERÊNCIA	
Tipo de acesso – Especifica o tipo da conexão da unidade remota do órgão Internet com acesso terrestre	Internet com acesso terrestre
Disponibilidade de Serviço – Relação entre o tempo de operação plena e prejudicada no período de 30 dias.	99,35%
Tempo Máximo de Retardo Admissível – Consiste no tempo médio de trânsito (ida e volta – roundtrip) de um pacote de 32 bytes entre a porta WAN do roteador da Contratante e o primeiro roteador de borda da Contratada integrada ao Backbone, cujo acesso se dá por meios de transmissão terrestre	Deverá ser igual ou inferior a 100 ms
Taxa de Erro de Bit (TEB) - A Taxa de Erro de Bit (TEB) é definida como a	10^{-6}

relação entre a quantidade de bits corretamente transmitidos para cada bit transmitido com erro no enlace.	
Descarte de Pacotes (DP) - Trata-se da relação entre a quantidade de pacotes enviados pela origem e a quantidade de pacotes recebidos pelo destino para um dado enlace. Em suma, medem quantos pacotes são descartados na transmissão	≤ 2%
Banda mínima garantida – banda mínima disponível para acesso a Internet para cada um dos pontos contemplados	100% da largura de banda contratada
Ativação – Período entre a solicitação e ativação do Serviço. (Sujeito a disponibilidade técnica no local)	90 (noventa) dias, prorrogável por igual período desde que devidamente justificado.
Prazo de Manutenção – Período máximo para o restabelecimento do serviço, contado a partir do momento da abertura do chamado até a finalização do atendimento.	(oito) horas para Capital e 12 (doze) horas para Interior
Prazo Mínimo de notificação de manutenção preventiva ou atualização de recursos técnicos – Período mínimo entre a notificação do cliente pela operadora até o início da interrupção programada.	7 (sete) dias
Abertura de Chamado – Disponibilidade de atendimento para solicitações de reparos, Help Desk da Operadora Contratada e discagem sem cobrança (0800) em língua portuguesa.	24 x 7 (00:00 ás 24:00 de Segunda a Domingo)
Horário de Reparo – Disponibilidade de atendimento técnico a partir da abertura da chamada.	24 x 7 (00:00 ás 24:00 de Segunda a Domingo)
Sistema Web de Monitoramento do link – Disponibilização de acesso ao sistema web de monitoramento de disponibilidade, utilização e falha do link (sujeito a disponibilidade).	Sim
Quantidade de IPs fixos válidos – Disponibilização de endereços IPs fixos válidos	5

6.2.3.3. PRESTAÇÃO DE SERVIÇOS DE INTERNET

I. O serviço de INTERNET refere-se à comunicação de dados sem a utilização de

qualidade de serviço, ou seja, limita-se ao uso de tecnologias que permitam a transferência de dados entre cada uma das unidades;

II. O serviço INTERNET deverá ser ofertado utilizando endereçamento fixo para o

protocolo da Internet (IP Fixo), não sendo admitida a atribuição de endereçamento de forma dinâmica;

- A Contratada, sempre que solicitado, deverá prever utilização do serviço de

tradução de endereço (NAT) no equipamento de acesso disponibilizado em cada unidade remota

III. Tempo máximo de latência do equipamento na localidade, Unidade remota, e o roteador de borda de saída da Contratada para a Internet instalada na rede da Contratada, conforme discriminado nas Classes do Acordo de Nível de Serviço (SLA) contempladas;

IV. Especificamente para o serviço de INTERNET, considerando as características o Tempo Máximo de Retardo Admissível será a mensurado através da média aritmética entre 03 (três) pontos préestabelecidos: 1) Site oficial do órgão. 2) Site da instituição federal a qual o órgão é vinculado ou site oficial do governo federal. 3) Site de grandes players do mercado (www.google.com, www.terra.com.br, www.uol.com.br, www.globo.com, www.msn.com) ou outro a ser definido pela Contratante.

V. Todas as instalações lógicas necessárias entre a rede da Contratada até o(s) equipamento(s) de conectividade (modem, roteador, etc.) na sede da Contratante, deverão ser de responsabilidade da Contratada, exceto a Rede Interna da unidade e o Distribuidor Geral (DG). Tais instalações devem seguir os padrões internacionais de cabeamento estruturado;

VI. Caberá a Contratante a responsabilidade pela indicação do local físico de instalação do equipamento de conectividade fornecido pela Contratada.

6.2.3.4. ESPECIFICAÇÕES DO SERVIÇO DE SEGURANÇA PARA PREVENÇÃO DE ATAQUES DDOS NO BACKBONE

I. A Contratada deverá disponibilizar a solução para Serviços dedicados de acesso à Internet com velocidade igual ou superior a 200Mbps, quando solicitado;

II. A Contratada deverá disponibilizar em seu backbone, proteção contra ataques de negação de serviço, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DOS (Denial of Service) e DDOS (Distributed Denial of Service);

III. A solução ANTI-DDOS deverá prover o serviço de mitigação de ataques de negação de serviço (DoS – Denial of Service) para o circuito de conectividade IP dedicada à Internet, sejam eles distribuídos (DDoS – DistributedDenialof Service) ou não;

IV. A Contratada deve possuir e disponibilizar no mínimo 2 (dois) centros de limpeza nacional cada um com capacidade de mitigação de no mínimo 40Gbps e no mínimo 1 (um) centro de limpeza internacional com capacidade de mitigação de no mínimo 80Gbps;

V. Não haverá taxa adicional para a por volume de mitigação de ataques (DDoS– DistributedDenialof Service) nos IP's monitorados;

VI. O ataque deve ser mitigado separando o tráfego legítimo do malicioso, de modo que os serviços de Internet providos pelo cliente continuem disponíveis;

VII. A limpeza do tráfego deverá ser seletiva e atuar somente sobre os pacotes destinados ao IP atacado, todo tráfego restante não deverá sofrer nenhuma forma de limpeza ou desvio;

VIII. A solução deve possuir mecanismos para filtragem de pacotes anômalos, garantindo a validade das conexões, sem efetuar qualquer limitação com base no número de sessões ou de pacotes por endereço, de modo a evitar o bloqueio de usuários legítimos;

IX. A Contratada deve tomar todas as providências necessárias para recompor a disponibilidade do link em caso de incidentes de ataques de DDoS, recuperando o pleno funcionamento do mesmo;

X. Para a mitigação dos ataques o tráfego só deverá ser encaminhado para limpeza fora do território brasileiro nos casos em que os centros nacionais não suportarem a capacidade de mitigação e a demanda de ataques, no restante os ataques de origem nacional deverão ser tratados nos centros nacionais e os de origem internacional nos centros internacionais;

XI. O envio de tráfego para mitigação em centros internacionais deverá ser justificado em relatório;

XII. Nos períodos de ataque a latência do circuito deverá ser de no máximo 100 ms (milissegundos) quando a mitigação se originar dos centros de limpeza nacionais e de no máximo 250 ms (milissegundos) quando se originar do(s) centro(s) internacionais;

XIII. A solução deverá possuir funcionalidades de monitoramento, detecção e mitigação de ataques, mantidas em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

XIV. A análise realizada para fins da solução deverá ser passiva sem utilização de elementos da rede da contratante para coleta dos dados a serem analisados;

XV. A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento;

XVI. A solução deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro por um determinado cliente;

XVII. A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White Lists, Black Lists, limitação de taxa, técnicas desafio-resposta, descarte de pacotes malformados, técnicas de mitigação de ataques aos protocolos HTTP/HTTPS, DNS, VPN, FTP, NTP, UDP, ICMP, correio eletrônico, bloqueio por localização geográfica de endereços IP, dentre outras;

XVIII. A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, para protocolo IPv4, incluindo, mas não se restringindo aos seguintes:

a) Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;

b) Ataques à pilha TCP, incluindo mal-uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;

c) Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;

d) Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing);

e) Em nenhum caso será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas da contratada

XIX. Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS, devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole;

XX. Realizar a comunicação da ocorrência do ataque à Contratante imediatamente após a detecção;

XXI. A solução deve permitir a proteção, no mínimo, do tráfego dos serviços web (HTTP/HTTPS), DNS, VPN, FTP e correio eletrônico;

XXII. Outras configurações deverão ser possíveis, como exemplo monitoração de um cliente por sub-interface no PE;

XXIII. A Contratada deverá disponibilizar relatórios mensais de mitigação de ataques, contendo no mínimo horário de início do ataque, horário de início de ação de mitigação, horário de sucesso da mitigação e horário de fim do ataque. Em conjunto com o relatório mensal relatórios dinâmicos deverão ser disponibilizados em até 48 horas após um ataque por solicitação da Contratante.

XXIV. A Contratada deverá apresentar relatório analítico, enviado mensalmente ao cliente;

XXV. A Contratada deverá disponibilizar 02 (dois) Centro Operacional de Segurança no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

XXVI. A Contratada terá no máximo 15 minutos para iniciar a mitigação de ataques de DOS e DDOS;

XXVII. Os serviços ofertados deverão operar no regime 24x7 (vinte e quatro horas por dia, sete dias por semana);

XXVIII. O backbone IP do provedor deve ter saída com destino direto a outros provedores de backbone IP Nacionais de nível Tier 1, 2 e 3, com banda de 100 Gbps no mínimo.

6.2.3.5. SERVIÇO DE COMUNICAÇÃO PARA INTERLIGAÇÃO AO BACKBONE DE INTERNET MUNDIAL, NA MODALIDADE BANDA LARGA (INTERNET)

- Serviço de acesso à Internet em Banda Larga assimétrico em acesso terrestre com fornecimento de IP dinâmico.

6.2.3.5.1. Característica do Link Banda Larga:

I. Downstream: 100Mbps;

II. Upstream: 20Mbps;

III. As velocidades indicadas são as máximas nominais;

IV. No período de maior tráfego, deverá ser garantida em 95% dos casos, uma velocidade média de no mínimo, 80% do valor nominal máximo, e uma velocidade instantânea de conexão de pelo menos 40% do valor nominal máximo, conforme regulamentação vigente;

V. Obrigatório a entrega através de acesso via última milha terrestre;

VI. Entrega mediante existência de viabilidade técnica dentro da área urbana;

VII. Será permitida subcontratação de links de terceiros.

6.2.3.5.2. Requisitos obrigatórios:

REQUISITOS OBRIGATÓRIOS	REFERÊNCIA
Ativação – Período entre a solicitação e ativação do Serviço. (Sujeito a disponibilidade técnica no local)	45 (quarenta e cinco) dias, prorrogável por igual período desde que devidamente justificado.
Prazo de Manutenção – Período máximo para o restabelecimento do serviço, contado a partir do momento da abertura do chamado até a finalização do atendimento.	48 (quarenta e oito) horas para Capital e 72 (setenta e duas) horas para Interior
Prazo Mínimo de notificação de manutenção preventiva ou atualização de recursos técnicos – Período mínimo entre a notificação do cliente pela operadora até o início da interrupção programada	7 (sete) dias **Abertura de**
Abertura de Chamado – Disponibilidade de atendimento para solicitações de reparos, Help Desk da Operadora Contratada e discagem sem cobrança (0800) em língua portuguesa.	24 x 7 (00:00 ás 24:00 de Segunda a Domingo)
Horário de Reparo – Disponibilidade de atendimento técnico a partir da abertura da chamada.	8 x 5 (8:00 às 12:00 e das 14:00 às 18:00 de Segunda a Sexta)

- O serviço de acesso à Internet em Banda Larga não terá qualquer tipo de gerenciamento ou monitoramento de rede.

6.2.3.6. SERVIÇO DE GERÊNCIA DE REDES E SERVIÇOS

6.2.3.6.1. Requisitos mínimos e obrigatórios do serviço de gerência de rede e serviços:

I. A Contratada deverá prover Solução de Gerência da Rede que contemple os módulos de gerência de falhas, desempenho, disponibilidade, capacity planning, relatórios, tickets e de nível de serviço:

a) A Solução de Gerência da Rede deverá disponibilizar a visualização de informações on-line (de forma gráfica) da rede para o acompanhamento e monitoração do estado global e detalhado do ambiente;

b) Em caso de formação de consórcio deverá ser provida uma única solução de Gerência de Rede.

II. A Solução de Gerência da Rede da Contratada deverá atuar de forma próativa, antecipando-se aos problemas na rede e garantindo o cumprimento do Acordo de Nível de Serviço (ANS),
realizando abertura, acompanhamento e fechamento de chamados de falhas relacionados com indisponibilidade, operando em regime 24 horas por dia, 7 dias por semana, todos os dias do ano.

6.2.3.6.2. Requisitos da Solução de Gerência de Rede:

I. A solução fornecida deve permitir acesso a todos os recursos e módulos através de única autenticação, sem a necessidade de realizar outros logins para acessar qualquer outro recurso de gerenciamento;

II. A Solução de Gerência da Rede deverá ser operada e administrada através de uma console única, portanto, não serão aceitas soluções que possuem acessos segmentados aos módulos;

III. Deverá ser escalável, permitindo futuras ampliações no número de elementos de rede a serem gerenciados.

IV. Deverá permitir acessos de usuários com perfis diferenciados com limitação de acesso a consoles, dispositivos, menus, alarmes, indicadores, etc;

V. Deverá permitir acesso de até 5 (cinco) usuários logados simultaneamente;

VI. A Solução de Gerência da Rede deverá permitir a criação de grupos de perfis de acesso, que serão associados a tipos de usuários;

VII. Os perfis deverão prever configurações em níveis de alertas, equipamentos, interfaces, aplicações, funcionalidades de monitoração, capacityplanning, inventário, etc;

VIII. A Solução de Gerência da Rede deverá ser 100% web sem necessidade de instalação de clients específicos, portanto, não serão aceitas soluções que não sejam

nativas em WEB ou que requeiram a instalação de agentes ou plugins nos desktops dos colaboradores da Contratante;

IX. O acesso deverá ser via web padrão HTTP e suportar a HTTPS, e em português, portanto não serão aceitas soluções que não possuam toda a sua estrutura em português;

X. A Solução de Gerência da Rede deverá ser compatível para acesso através de smartphones e tablets;

XI. A Solução de Gerência da Rede deverá ser escalável, mas transparente para a CONTRATANTE em termos de console única;

XII. A Solução de Gerência da Rede deverá ser acessível através dos principais browsers do mercado, tais como, Internet Explorer, Firefox, Google Chrome e Safari;

XIII. Deverá permitir a exportação das informações para relatórios em formatos comerciais;

XIV. A Solução de Gerência da Rede deverá gerar alertas quando os thresholds “limites” configurados para um componente monitorado são excedidos (ex., utilização de CPU, memória, interfaces, volume de erros, tempo de resposta de serviços);

XV. A Solução de Gerência da Rede deverá fornecer, através do portal, visualização de informações on-line (em intervalos de 5 minutos e de forma gráfica) da rede que deverá apresentar, no mínimo, os seguintes itens para cada um dos elementos monitorados:

a) Topologia da rede, incluindo os roteadores CPE e seus enlaces, com visualização do estado operacional de todos os elementos da rede (enlaces e equipamentos). O estado operacional dos elementos da rede deverá ser atualizado automaticamente na Solução de Gerência da Rede, sempre que os mesmos sofrerem alterações;

b) Alarmes e eventos ocorridos na rede com informações de data, hora e duração de ocorrência e identificação dos recursos gerenciados;

c) Consumo de banda dos enlaces (entrada e saída) separados por dia e mês;

d) Consumo de banda por classe de serviço separados por dia e mês;

e) Ocupação de memória e CPU dos roteadores CPE;

f) Retardo dos enlaces separados por dia e mês;

g) Perda de pacotes (descarte) no sentido IN e OUT em %;

h) Taxa de erros em erros por segundo;

i) Latência em milissegundos;

j) A Solução de Gerência de Rede de possuir gráficos de Capacity Planning que permita criar uma série de cenários para projeções de tendências de um determinado recurso;

k) A Solução de Gerência da Rede deverá permitir a apresentação de indicadores que reflitam o nível de SLA (Service LevelAgreement) e SLM (Service Level Management) dos
serviços contratados;

l) Backup de configuração dos elementos gerenciados, alarmes para alterações realizadas, relatório de mudanças;

m) Inventário dos equipamentos e enlaces da rede contendo, no mínimo,
as seguintes informações:

I. Enlace: designação, tecnologia e nível de serviço;
II. Roteador CPE: fabricante e modelo e configuração física (interfaces, memória, slots, dentre outros);
III. Endereçamento lógico: endereços IPs e máscaras.

n) A Solução de Gerência da Rede deverá permitir adicionar a nomenclatura conhecida pelo Contratante para os recursos gerenciados.

6.2.3.6.3. A Solução de Gerência da Rede deverá permitir a criação de Relatórios:

a) Permitir ser exportados conforme os principais métodos como: pdf, csv, pacote office;
b) Relatórios de desempenho sumarizado por período especifico;

c) Relatórios de desempenho classificados em uma visão TOP N. Ex.:

I. Top Roteadores % de utilização de CPU
II. Top N Interfaces % de utilização
III. Top N Interfaces com descartes
IV. Top N Interfaces com eventos de Latência.

d) Relatórios de disponibilidade com períodos específicos;

e) Dashboards relacionando falhas, desempenho, capacity e disponibilidade;

f) Dashboards executivos com visão sumarizadas de indicadores operacionais (Pro atividade, Taxa de Reincidência, Reparos no Prazo e Taxa de Falha).

6.2.3.6.4. A Solução de Gerência da Rede deverá realizar registro de todas as ocorrências de alarmes/eventos em log de históricos e/ou em base de dados contendo informações de data e hora de ocorrência, identificando os recursos gerenciados;

I. A Solução de Gerência da Rede deverá armazenar os dados por um período de 6 (seis) meses.

6.2.3.7. SERVIÇO DE SEGURANÇA DE PERÍMETRO FIREWALL UTM

6.2.3.7.1. Item A: Appliance UTM de 750 Mbps de capacidade de firewall.

a) Características do hardware:

I. O equipamento deve se instalar em mesa ocupando no máximo 1U (44,45mm) da referida mesa;

II. Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

III. Deverão ser fornecidos todos os cabos de energia, serial (RS- 232/RJ45) ou outra tecnologia disponível para acesso console, para instalação e funcionamento do dispositivo;

IV. Possuir led indicador on/off, disco e devices de rede;

V. Possuir throughput mínimo de 750 Mbps para tráfego UDP;

VI. Suportar no mínimo 82.000 (oitenta e duas mil) conexões simultâneas;

VII. Suportar no mínimo 11.000 (onze mil) novas conexões por segundo;

VIII. Possuir throughput mínimo de 435 Mbps para tráfego IPS/IDS;

IX. Possuir throughput mínimo de 225 Mbps para tráfego VPN IPSEC com criptografia (AES-128);

X. Possuir throughput mínimo de 60 Mbps para tráfego VPN SSL com criptografia (AES-128);

XI. Possuir throughput mínimo de 92 Mbps/28 Mbps para tráfego Proxy Web filter/SSL Inspection;

XII. Possuir throughput mínimo de 64 Mbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

XIII. Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

XIV. Possuir dispositivo de armazenamento interno de no mínimo 32 GB padrão SSD;

XV. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

XVI. Possuir pelo menos 1 (uma) portas USB para conexão de dispositivos externos;

XVII. A interface USB deve suportar o uso de modem 3G/4G/LTE para conexão de link de Internet.

6.2.3.7.2. Item B: Appliance UTM de 2.4 GBPS de capacidade de firewall

a) Características do hardware:

I. O equipamento deve se instalar em mesa ocupando no máximo 1U (44,45mm) da referida mesa;

II. Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

III. Deverão ser fornecidos todos os cabos de energia, serial 232/RJ45) ou outra tecnologia disponível para acesso console, para instalação e funcionamento do dispositivo;

IV. Possuir led indicador on/off, disco e devices de rede;

V. Possuir throughput mínimo de 2.4 Gbps para tráfego UDP;

VI. Suportar no mínimo 220.000 (duzentos e vinte mil) conexões simultâneas;

VII. Suportar no mínimo 15.000 (quinze mil) novas conexões por segundo;

VIII. Possuir throughput mínimo de 900 Mbps para tráfego IPS/IDS;

IX. Possuir throughput mínimo de 290 Mbps para tráfego VPN IPSEC com criptografia (AES-128);

X. Possuir throughput mínimo de 195 Mbps para tráfego VPN SSL com criptografia (AES-128);

XI. Possuir throughput mínimo de 410 Mbps/180 Mbps para tráfego Proxy Web filter/SSL Inspection;

XII. Possuir throughput mínimo de 191 Mbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

XIII. Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

XIV. Possuir dispositivo de armazenamento interno de no mínimo 32 GB padrão SSD;

XV. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

XVI. Possuir pelo menos 1 (uma) portas USB para conexão de dispositivos externos;

XVII. A interface USB deve suportar o uso de modem 3G/4G/LTE para conexão de link de Internet

6.2.3.7.3. Item C: Appliance UTM de 7 GBPS de capacidade de firewall

a) Características do hardware:

I. O equipamento deve se instalar em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 1U (44,45mm) do referido rack;

II. Dispor de fonte de alimentação interna com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

III. Deverão ser fornecidos todos os cabos de energia, serial (RS- 232/RJ45) ou outra tecnologia disponível para acesso console, para instalação e funcionamento do dispositivo;

IV. Possuir painel/led indicador on/off, disco e devices de rede;

V. Possuir throughput de no mínimo 7Gbps para tráfego UDP;

VI. Suportar no mínimo 900.000 (novecentas mil) conexões simultâneas;

VII. Suportar no mínimo 50.000 (cinquenta mil) novas conexões por segundo;

VIII. Possuir throughput mínimo de 1.4 Gbps para tráfego IPS/IDS;

IX. Possuir throughput mínimo de 900 Mbps para tráfego VPN IPSEC com criptografia (AES-128);

X. Possuir throughput mínimo de 800 Mbps para tráfego VPN SSL com criptografia (AES-128);

XI. Possuir throughput mínimo de 1.4 Gbps/400 Mbps para tráfego Proxy Web filter/SSL Inspection;

XII. Possuir throughput mínimo de 760 Mbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

XIII. Possuir pelo menos 6 (seis) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

XIV. Possuir dispositivo de armazenamento interno de no mínimo 120 GB padrão SSD;

XV. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

XVI. Possuir no mínimo 2 (duas) portas USB para conexão de dispositivos externos;

XVII. A interface USB deve suportar o uso de modem 3G/4G/LTE para conexão de link de Internet.

6.2.3.7.4. Item D: Appliance UTM de 11 GBPS de capacidade de firewall

a) Características do hardware:

I. O equipamento deve se instalar em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 1U (44,45 mm) do referido rack;

II. Dispor de fonte de alimentação interna com tensão de entrada de 110V / 220V ACautomática e frequência de 50-60 Hz;

III. Deverão ser fornecidos todos os cabos de energia, serial (RS-232/RJ45) ou outra tecnologia disponível para acesso console, para instalação e funcionamento do dispositivo;

IV. Possuir painel/led indicador on/off, disco e devices de rede;

V. Possuir throughput de no mínimo 11 Gbps para tráfego UDP;

VI. Suportar no mínimo 1.300.000 (hum milhão e trezentas mil) conexões simultâneas;

VII. Suportar no mínimo 75.000 (setenta e cinco mil) novas conexões por segundo;

VIII. Possuir throughput mínimo de 3.9 Gbps para tráfego IPS/IDS;

IX. Possuir throughput mínimo de 1.3 Gbps para tráfego VPN IPSECcom criptografia (AES-128);

X. Possuir throughput mínimo de 600 Mbps para tráfego VPN SSL com criptografia (AES-128);

XI. Possuir throughput mínimo de 1.9 Gbps/900 Mbps para tráfego Proxy Web filter/SSL Inspection;

XII. Possuir throughput mínimo de 900 Mbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

XIII. Possuir pelo menos 8 (oito) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

XIV. Possuir 4 interfaces SFP+ 10GBASE-SR Multimodo;

XV. Possuir dispositivo de armazenamento interno de no mínimo 240 GB padrão SSD;

XVI. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

XVII. Possuir pelo menos 2 (duas) portas USB para conexão de dispositivos externos.

6.2.3.7.5. Item E: Appliance UTM de 18 GBPS de capacidade de firewall

a) Características do hardware:

I. O equipamento deve se instalar em rack com largura padrão de polegadas, padrão EIA-310, ocupando no máximo 1U (44,45 mm) do referido rack;

II. Dispor de fonte de alimentação interna com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

III. Possuir painel/led indicador on/off, disco e devices de rede;

IV. Deverão ser fornecidos todos os cabos de energia, serial (RS- 232/RJ45) ou outra tecnologia disponível para acesso console, para instalação e funcionamento do dispositivo;

V. Possuir throughput de no mínimo 18.000 Mbps para tráfego UDP;

VI. Suportar no mínimo 1.800.000 (um milhões e oitocentas mil) conexões simultâneas;

VII. Suportar no mínimo 100.000 (cem mil) novas conexões por segundo;

VIII. Possuir throughput mínimo de 5.8 Gbps para tráfego IPS/IDS;

IX. Possuir throughput mínimo de 3Gbps para tráfego VPN IPSEC com criptografia (AES-128);

X. Possuir throughput mínimo de 1.2 Gbps para tráfego VPN SSL com criptografia (AES-128);

XI. Possuir throughput mínimo de 3Gbps/1 Gbps para tráfego Proxy Web filter/SSL Inspection;

XII. Possuir throughput mínimo de 1.2 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

XIII. Possuir pelo menos 8 (oito) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

XIV. Possuir 4 interfaces SFP+ 10GBASE-SR Multimodo;

XV. Possuir dispositivo de armazenamento interno de no mínimo 240 GB padrão SSD;

XVI. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

XVII. Possuir pelo menos 2 (duas) portas USB para conexão de dispositivos externos;

XVIII. A interface USB deve suportar o uso de modem 3G/4G/LTE para conexão de link de Internet.

6.2.3.7.6. Item F: Appliance UTM de 38 GBPS de capacidade de firewall

a) Características do hardware:

I. O equipamento deve se instalar em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 2U (88,90 mm) do referido rack;

II. IDispor de fonte de alimentação redundante interna com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz, Hot swapping;

III. Deverão ser fornecidos todos os cabos de energia, serial (RS- 232/RJ45) ou outra tecnologia disponível para acesso console, para instalação e funcionamento do dispositivo;

IV. Possuir painel/led indicador on/off, disco e devices de rede;

V. Possuir throughput de no mínimo 38.000 Mbps para tráfego UDP;

VI. Suportar no mínimo 6.000.000 (seis milhões) conexões simultâneas;

VII. Suportar no mínimo 195.000 (cento e noventa e cinco mil) novas conexões por segundo;

VIII. Possuir throughput mínimo de 9Gbps para tráfego IPS/IDS;

IX. Possuir throughput mínimo de 7.5 Gbps para tráfego VPN IPSEC com criptografia (AES-128);

X. Possuir throughput mínimo de 6.4 Gbps para tráfego VPN SSL com criptografia (AES-128);

XI. Possuir throughput mínimo de 9Gbps/2.9 Gbps para tráfego Proxy Web filter/SSL Inspection;

XII. Possuir throughput mínimo de 4Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

XIII. Possuir pelo menos 08 (oito) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

XIV. Possuir 4 interfaces SFP+ 10GBASE-SR Multimodo;

XV. Possuir dispositivo de armazenamento interno de no mínimo 480 GB padrão SSD;

XVI. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

XVII. Possuir pelo menos 2 (duas) portas USB para conexão de dispositivos externos;

XVIII. A interface USB deve suportar o uso de modem 3G/4G/LTE para conexão de link de Internet.

6.2.3.7.7. Item G: Appliance UTM de 57 Gbps de capacidade de firewall

a) Características do hardware:

I. O equipamento deve se instalar em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 2U (88,90 mm) do referido rack;

II. Dispor de fonte de alimentação redundante interna com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz, Hot swapping;

III. Deverão ser fornecidos todos os cabos de energia, serial (RS- 232/RJ45) ou outra tecnologia disponível para acesso console, para instalação e funcionamento do dispositivo;

IV. Possuir painel/led indicador on/off, disco e devices de rede;

V. Possuir throughput de no mínimo 57.000 Mbps para tráfego UDP;

VI. Suportar no mínimo 8.000.000 (oito milhões) conexões simultâneas;

VII. Suportar no mínimo 255.000 (duzentos e cinquenta e cinco mil) novas conexões por segundo;

VIII. Possuir throughput mínimo de 11 Gbps para tráfego IPS/IDS;

IX. Possuir throughput mínimo de 10 Gbps para tráfego VPN IPSEC com criptografia (AES-128);

X. Possuir throughput mínimo de 7Gbps para tráfego VPN SSL com criptografia (AES-128);

XI. Possuir throughput mínimo de 10 Gbps/3.8 Gbps para tráfego Proxy Web filter/SSL Inspection;

XII. Possuir throughput mínimo de 5Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

XIII. Possuir pelo menos 08 (oito) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

XIV. Possuir 8 interfaces SFP+ 10GBASE-SR Multimodo;

XV. Possuir dispositivo de armazenamento interno de no mínimo 480 GB padrão SSD;

XVI. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

XVII. Possuir pelo menos 2 (duas) portas USB para conexão de dispositivos externos.

6.2.3.7.8. Especificações gerais de software NGFW para os itens A, B, C, D, E, F,G.

a) Funções básicas:

I. Hardware (Appliances) que atuam na segurança e performance do ambiente de rede;
II. VPN SSL, VPN IPSec (Client-to-site e Site-to-site);
III. Controle de Aplicações;
IV. Proxy Web e Filtro de Conteúdo Web (URL Filtering);

V. Detecção e prevenção de intrusos – IPS;
VI. Qualidade de serviço – QOS;
VII. Anti-Malware;
VIII. SD-WAN;
IX. Cluster.

b) Características gerais:

I. O desempenho e as interfaces solicitados deverão ser comprovados através de datasheet público na internet. Caso haja divergência entre métricas do mesmo datasheet, será aceitoo valor de maior capacidade.

II. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

III. Interface em português e inglês;

IV. Qualquer interface de rede do equipamento deverá ser utilizada como gerenciamento, ou seja, não deve haver nenhuma interface exclusiva para a função de gerenciamento;

V. O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;

VI. O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.

VII. Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.

VIII. Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3.

IX. Deverá possuir uma janela para monitoramento do tráfego de rede com informações do throughput e da quantidade de conexões simultâneas;

X. A Solução deverá prover inspeção SSL;

XI. A solução deverá ser em hardware dedicado tipo appliance com sistema operacional customizado para garantir segurança e melhor desempenho.

XII. Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo;

XIII. Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado;

XIV. Suportar a utilização de um proxy para atualização do software e licenciamento e deverá permitir as seguintes opções de configuração:

- Endereço do servidor;
- Porta do servidor;
- Usuário;
- Senha;

XV. Deverá permitir o monitoramento SNMP, no mínimo, dos seguintes itens:

- Desempenho total (throughput);
- Conexões simultâneas;
- Usuários autenticados;
- Serviços habilitados ou desabilitados;
- Quantidade de endereços distribuídos pelo DHCP;

XVI. Deverá implementar a funcionalidade de "zero-touch" para sua primeira implementação ou substituição. Dessa forma, deverá ser possível provisionar a configuração

do equipamento via sistema de gerenciamento centralizado, mesmo antes do equipamento ser conectado à rede,
transformando a atividade em uma simples conexão física de equipamento, sem a necessidade de configurações individuais nos equipamentos;

XVII. A Solução deve permitir ao administrador associar na solução de gerenciamento centralizado o número de série dos equipamentos ao site aonde ele será instalado, de maneira que ao se ativar um equipamento no site remoto, esse equipamento se conecte com o Sistema Central e receba a configuração;

XVIII. Ao instalar um equipamento no site remoto, cabeá-lo e energizá-lo, ele deverá tentar localizar Sistema Central para receber a sua configuração, sem que seja necessária qualquer configuração via console local do equipamento;

XIX. A solução ofertada deverá permitir a criação de perfis de proteção, tais como e não limitado a perfil de IPS, perfil de controle WEB/aplicações e perfil de SD-WAN e dever ser
possível utilizá-los nas políticas de segurança;

XX. Deverá possuir um painel centralizado para exportação e agendamento de relatórios e deverá permitir exportá-los nos formatos: HTML, PDF, CSV;

XXI. Implementar protocolo de coleta de informações de fluxos que circulam pelo equipamento, como Netflow v5, v9 e v10 (IPFIX):
XXII. A solução deverá possuir uma única janela para a criação, configuração e edição dos recursos de segurança;

XXIII. Os módulos de IPS, SD-WAN, Controle de aplicativos, Proxy WEB e Antimalware devem ser disponibilizados em perfis e estes devem ser inseridos em uma única policy.

b) Das funcionalidades do firewall:

I. Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;
II. Possuir um sistema de armazenamento remoto para salvar backups da solução com suporte a conexões utilizando os protocolos Network File System (NFS), SSH e que permita
salvar em PenDrive local;
III. Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.
IV. Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deve permitir o agendamento diário ou semanal;
V. O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.
VI. As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;
VII. O sistema ainda deve contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;

VIII. Deve possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;

IX. Deve permitir habilitar ou desabilitar o registro de log por política de firewall.

X. Possuir controle de acesso à internet por endereço IP de origem e destino;

XI. Possuir controle de acesso à internet por sub-rede;

XII. Possuir suporte a tags de VLAN (802.1q);

XIII. Suportar agregação de links, segundo padrão IEEE 802.3ad;

XIV. Possuir ferramenta de diagnóstico do tipo tcpdump;

XV. Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;

XVI. Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

XVII. Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network AddressTranslation), um para um, N-para-um e vários para um.

XVIII. Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

XIX. Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;

XX. Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT.

XXI. Possuir suporte a roteamento dinâmico RIP V1, V2, OSPF, BGP;

XXII. Possuir funcionalidades de DHCP Cliente, Servidor e Relay;

XXIII. Deverá suportar aplicações multimídia como: H.323, SIP;

XXIV. Possuir tecnologia de firewall do tipo Stateful;

XXV. Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo;

XXVI. Permitir o funcionamento em modo transparente tipo “bridge”;

XXVII. Permitir a criação de pelo menos 20 VLANS no padrão IEEE 802.1q;

XXVIII. Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);

XXIX. Deverá suportar forwarding de multicast;

XXX. Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;

XXXI. Permitir o agrupamento de serviços;

XXXII. Permitir o filtro de pacotes sem a utilização de NAT;

XXXIII. Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

XXXIV. Possuir mecanismo de anti-spoofing;

XXXV. Permitir criação de regras definidas pelo usuário;

XXXVI. Permitir o serviço de autenticação para HTTP e FTP;

XXXVII. Possuir a funcionalidade de balanceamento e contingência de links;

XXXVIII. Deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: WhatsApp, Telegram, Messenger (Facebook), Direct (Instagram), Yahoo! Messenger, BitTorrent, eDonkey, GNUTella, KaZaa, Skype e WinNY

d) Identificação de usuário:

I. Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integrada ao repositório de usuários sendo: Active Directory, LDAP,

TACAC´S e Radius;

II. 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;

III. Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (CaptivePortal), sem a necessidade de agente;

IV. Deve possuir Captive Portal com suporte a Autenticação Social (Facebook, Twitter, Google);

V. A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;

VI. Na integração com o AD, todos os domain controllers em operação na rede do cliente devem ser cadastrados de maneira simples e sem utilização de scritps de comando;

VII. A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante;

VIII. A solução deve suportar a opção de instalação de softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais de IP/nome de usuário do

domínio/nome da máquina para o gateway diretamente, sem que o Gateway tenha que fazer Queries no AD;

IX. O UTM deve permitir gerenciar múltiplas políticas de controles no serviço de autenticação. As políticas devem permitir criar controles para autenticação, e deve permitir ou

bloqueia o acesso ao serviço de autenticação baseado em condições e para sessão, ou seja, uma vez que o usuário esteja permitido se autenticar no serviço, a política deve definir os parâmetros de sessão do usuário;

X. Para o sistema de controles no serviço de autenticação o produto deve possuir, no mínimo, as seguintes condições para o Controle de Autenticação:

- Usuários e Grupos de Usuários;

- Datas (Objetos de Datas)
- Horários (Objetos de Horário)
- Plataformas (Objetos de Dicionários)
- Endereços Remotos (Objetos de IPv4 e IPv6)
- Zona de Rede (Múltiplas Zonas).

e) Das funcionalidades da VPN:

I. VPN baseada em appliance;
II. Suporte a certificados PKI X.509 para construção de VPNs;
III. Possuir suporte a VPNs IPSec site-to-site:
a) Criptografia, 3DES, AES128, AES256, AES-GCM-128
b) Integridade MD5, SHA-1, SHA-256, SHA384, AES-CMAC e AES-XCBC;
c) Algoritmo Internet Key Exchange (IKE) versões I e II;
d) AES 128 e 256 (AdvancedEncryption Standard);

e) Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30;

IV. Possuir suporte a VPN SSL;

V. Possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

VI. Suportar VPN SSL Client less, sem a necessidade de utilização de Java, no mínimo, para os serviços abaixo:

VII. RDP;

VIII. VVNC;

IX. SSH;

X. WEB;

XI. SMB.

XII. Deve permitir a arquitetura de vpnhub and spoke;

XIII. Suporte a VPNs IPSecclient-to-site:

a) Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site.

XIV. Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);

XV. Possuir funcionalidades de Auto-Dicovery VPN capaz de permitir criar tuneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub);

XVI. A funcionalidade de AD-VPN deve suportar criar os seguintes tipos de túneis:

a) Site-to-Site;

b) Full-Mesh;

c) Star.

f) Das funcionalidades da detecção de intrusão:

I. A Detecção de Intrusão deverá ser baseada em appliance;

II. Possuir no mínimo 30.000 assinaturas ou regras de IPS/IDS;

III. O Sistema de detecção e proteção de intrusão deverá estarorientado à proteção de redes;

IV. Possuir tecnologia de detecção baseada em assinatura;

V. Deverá suportar a implantação em modo Gateway, inline e em modo sniffer;

VI. Suportar implementação de cluster do IPS em linha se o equipamento possuir interface do tipo by-pass;

VII. O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança;

VIII. Possuir opção para administrador as listas de Blacklist, Whitelist e Quarentena com suporte a endereços IPv6.

IX. Possuir capacidade de remontagem de pacotes para identificação de ataques;

X. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque; Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;

XI. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denialof Service (DoS) do tipo Flood, Scan, Session e Sweep;

XII. Mecanismos de detecção/proteção de ataques;
XIII. Reconhecimento de padrões;
XIV. Análise de protocolos;
XV. Detecção de anomalias;
XVI. Detecção de ataques de RPC (Remote procedure call);
XVII. Proteção contra ataques de Windows ou NetBios;
XVIII. Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);
XIX. Proteção contra ataques DNS (Domain Name System);
XX. Proteção contra ataques a FTP, SSH, Telnet e rlogin;
XXI. Proteção contra ataques de ICMP (Internet ControlMessageProtocol);
XXII. Alarmes na console de administração;
XXIII. Alertas via correio eletrônico;
XXIV. Monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;
XXV. Capacidade de resposta/logs ativa a ataques;
XXVI. Terminação de sessões via TCP resets;
XXVII. Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
XXVIII. O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;
XXIX. Possuir filtros de ataques por anomalias;
XXX. Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destinationsessionlimit;
XXXI. Permitir filtros de anomalias de protocolos;
XXXII. Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;
XXXIII. Suportar verificação de ataque nas camadas de aplicação

g) Das funcionalidades de QoS:

I. Adotar solução de Qualidade de Serviço baseada em appliance;
II. Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;
III. Permitir modificação de valores DSCP;
IV. Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;
V. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
VI. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;
VII. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
VIII. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;
IX. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino

h) Das funcionalidades do antivírus:

I. Possuir funções de Antivírus, Anti-spyware;

II. Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP;

III. Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.)

IV. Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;

V. Permitir o bloqueio de download de arquivos por tamanho

i) Das funcionalidades do Proxy e filtro de conteúdo web:

ii)

I. Possuir solução de filtro de conteúdo web integrado a solução de segurança

II. Possuir pelo menos 75 categorias para classificação de sites web

III. Possuir base mínima contendo, 40 milhões de sites internet web já registrados e classificados;

IV. Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:

a) Webmail;
b) Instituições de Saúde;
c) Notícias;
d) Pornografia;
e) Restaurante;
f) Mídias Sociais;
g) Esporte;
h) Educação;
i) Games;
j) Compras

V. Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

VI. Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;

VII. Deve permitir a definição do tamanho mínimo dos objetos salvos em cache no disco;

VIII. Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;

IX. Possibilitar a integração com servidores de cache WEB externos;

X. Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update®, Youtube®, MSN Vídeos®, Facebook®, Google Maps®;

XI. Deve possuir a capacidade de excluir URL's específicas do cache web, configurável por lista de palavras chaves com suporte inclusive a expressões regulares;

XII. Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

XIII. Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

XIV. Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;

XV. Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de: base de URL própria atualizável;

XVI. Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;

XVII. Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;

XVIII. Deverá permitir o bloqueio de URLs inválidas cujo campo CN do certificado SSL não contém um domínio válido;

XIX. Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;

XX. Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

XXI. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

XXII. Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem;

XXIII. Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;

XXIV. Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Audio, Video e URLs originadas de Spam;

XXV. Deverá permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;

XXVI. Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, e FTP e em Proxy Transparente;

XXVII. Deverá permitir configurar a porta do Proxy Explícito.

j) Das funcionalidades do controle de aplicações:

I. As funcionalidades abaixo devem ser baseadas em appliance:

II. Deverá reconhecer no mínimo 3.000 aplicações;

III. Deverá possuir pelo menos 10 categorias para classificação de aplicações;

IV. Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:

a) P2P;
b) Web;
c) Transferência de arquivos;
d) Chat;
e) Social;

V. Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

VI. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

VII. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

VIII. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

IX. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

X. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

XI. Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;

XII. Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

k) Do sistema de proteção contra ameaças:

I. Possuir sistema de proteção contra ameaças nativo;

II. Possuir no mínimo 30.000 (trinta mil) assinaturas;

III. O sistema de deve monitorar e analisar o tráfego da rede, identificar aplicativos e ameaças de ataques direcionados e persistentes e efetuar os respectivos bloqueios.

IV. Deve ser baseado em uma lista de assinaturas eletrônicas que atue em tempo real analisando a camada de aplicação, capaz de identificar o conteúdo dos pacotes, fazer log (registros) das assinaturas trafegadas, inspecionar os pacotes e efetuar o descarte automático do pacote quando identificado assinaturas de pacotes maliciosos, inapropriados para o uso no ambiente corporativo;

V. A base de assinaturas do sistema ativo deverá ser fornecida pelo período do contrato;

VI. Dever permitir a identificação de aplicativos e ameaças independente das portas e protocolos;

VII. Possuir mecanismo de bloqueio para listas de reputação de endereço IP catalogadas no mínimo para 6 (seis) categorias, capaz de permitir seleção por categorização, elas devem atender as seguintes classificações: spam, reputation, malware, attacks, anonymous e abuse;

VIII. Deve permitir a atualização automática das assinaturas por meio de agendamento diário;

IX. Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, malware-backdoors, ataques P2P, trojans, worms, user_agents, pua

(adware, p2p, toolbars) malwares para mobile, blacklist, botcc, exploits-kits, file-executable, file flash, file-identify, file-image, file-java, file-multimedia, file-office, file-other, file-pdf, games, inappropriate e vulnerabilidades conhecidas;

X. Possuir uma ferramenta de bloqueio de execução de aplicativos, integrado a base de Antivírus e Antimalware;

XI. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos do tipo: ads, cloud, colaboração, download, e-mail, games, mobile, p2p, proxy, remote, redes sociais; storage, streaming, update, voip e web.

XII. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de VoIP tais como: Hotline, Asterisk, Linphone, SIP, Skype, Xlite SIP, X-Pro SIP, Cisco SIP, OpenSIP, Bria, ClearSea e Nero SIP;

XIII. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de Redes Sociais tais como: AolInstant Messenger, Badoo, BaiduHi, Airtime, Blogger,BoldChat, ChatON, China.com, Facebook, Flickr, FC2, Fring, Google Analytics, Google App, ICQ, Linkdin, Meetup, MSM Messenger,Netlog, Skype, Tinder, Tuenti, Twitter, WhatssApp, WeChat e Zoho Chat;

XIV. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos e transferências de arquivos do tipo P2P (peertopeer) tais como: BitTorrent, Gnutella, FastTrack,

IceShare, Napster, Shareman e de Storages, tais como: Dropbox, Easy-share, Google Drive, Megashare, MegaUpload, Rapidshare, OneDrive, Yahoo Box, SoundCloud e Filemail,DivShare;

XV. Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;

XVI. Suportar exceção de aplicativos por assinatura; IP de origem ou IP de destino;

XVII. Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre as “ameaças detectadas” e as “ameaças bloqueadas”;

XVIII. Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os “aplicativos detectados” e os “aplicativos bloqueados”;

XIX. Deve possuir mecanismos para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: “baixo; médio e alto”;

XX. Gerar registro do tipo Top Level, dos 10(dez) mais, inclusive da relação de eventos entre usuários e ameaças, usuário e aplicativos, aplicativos e ameaças identificados e bloqueados.

l) SD-WAN:

I. Entende-se como tecnologia SD-WAN (Software-Defined WAN) a rede de área ampla definida por software que centraliza a gerência da rede WAN em uma console única,

eliminando a necessidade de intervenções manuais em roteadores em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou performance e utilização de túneis VPN para comunicação entre os sites remotos;

II. Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas;

III. Permitir utilizar VPN IPsec para interligar unidades remotas;

IV. Possuir recurso de “persistência de link” para impedir a queda de conexões em aplicações que não suportam o load balance de link;

V. O balanceamento deverá ser baseado em critérios de desempenho, devendo no mínimo, permitir verificar o monitoramento do consumo de banda, perda de pacotes, jitter e latência;

VI. Deve possuir uma janela web ou dashboard capaz de fornecer informações dos eventos e com informações do monitoramento de desempenho relacionado ao recurso SDWAN;

VII. O recurso de SD-WAN deverá suportar o roteamento de tráfego por política baseado em aplicação;

VIII. O appliance SD-WAN deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link monitorado recuperado veja avaliado. Deve

suportar especificar um valor variando de 1 a 100.

IX. O recurso de SD-WAN deverá permitir o monitoramento de, no mínimo 03 (três) endereços alvos para verificar a disponibilidade e desempenho do link;

X. A solução de SD-WAN UTM deve permitir a configuração da funcionalidade de SD-WAN em qualquer interface WAN de forma agnóstica, independente se é internet, 3G/4G/LTE, entre outras;

XI. Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações em uma única janela:

a) Consumo de banda;
b) Perda de pacotes;
c) Jitter;

d) Latência.

m) Alta disponibilidade:

I. Permitir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby, com as implementações de Fail Over.

II. Não serão permitidas soluções de cluster (HA) que façam com que o equipamento (s) reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador.

III. O Sincronismo dos servidores deve ser por interface exclusiva permitindo utilizar mais de uma interface de Heartbeat.

6.2.3.7.9. Item G: Serviço de instalação:

I. Para as soluções ofertadas, a contratada deverá cotar um valor total para a instalação e customização inicial dos dispositivos adquiridos;

II. Este serviço deverá ser utilizado para a operacionalização inicial dos produtos adquiridos, customização, funcionalidades e políticas;

III. Toda a despesa de deslocamento e hospedagem deve ser de responsabilidade da contratada

6.2.3.7.10. Item H: Serviços de prestação de suporte técnico remoto 8X5:

I. Serviço de suporte REMOTO para os equipamentos de segurança de borda contratados, no horário 8x5 (Segunda a sexta-feira das 08:00 às 18:00, exceto feriados), pelo tempo de contrato.

II. A contratada deve possuir serviço de abertura de chamados remoto capaz de abrir chamados de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede relativos aos equipamentos e/ou produtos fornecidos;

III. A contratada deverá iniciar o atendimento de suporte em no máximo 8 horas úteis após a abertura do chamado;

IV. A Contratada será eximida da aplicação das sanções administrativas para os respectivos chamados em que sejam descumpridos os tempos de solução, desde que comprovadas as seguintes situações:

a) Quando constatado que o problema está relacionado a “bug” no produto e que o fabricante não possui uma correção imediata para tal, sendo este fato declarado pelo próprio;
b) A Contratada tomou todas as medidas possíveis visando providenciar solução de contorno.

6.2.4. SOLUÇÃO DE WI-FI

6.2.4.1. Solução de mobilidade – acesso WiFi indoor:

a) Características gerais:

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

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

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

IV. 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.

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

VI. Possuir suporte a pelo menos 16 (dezesseis) SSIDs por ponto de acesso.

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

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

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

X. Deverá possuir 2 (duas) interfaces ethernet 10/100/1000 Mbps, utilizando conector RJ-45, para conexão à rede local.

XI. Deve suportar LACP viabilizando agregação de portas ethernet.

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

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

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

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

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

b) Características dos rádios:

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

II. Implementar as seguintes taxas de transmissão com fallback automático: IEEE 802.11b: 1 Mbps a 11 Mbps, IEEE 802.11a e IEEE 802.11g: 6 Mbps a 54 Mbps, IEEE 802.11n: 6.5 Mbps a

300 Mbps, IEEE 802.11ac: 6.5 Mbps a 867 Mbps e IEEE 802.11ax: 4 Mbps a 1200 Mbps.

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

IV. Deverá suportar potência agregada de saída, considerando todas as cadeias

MIMO, de, no mínimo, 25 dBm na frequência de 5 GHz e 26 dBm na frequência de 2.4 GHz.

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

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

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

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

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

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

b) Serviços, segurança e gerenciamento:

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

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

pela rede local.

III. Deve suportar auto cura por meio de Mesh em caso de falha da conexão cabeada de dados, bem como permitir que os pontos de acesso gerenciados estabeleçam automaticamente

uma rede mesh sem fio.

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

V. Deve suportar, somente por meio do ponto de acesso em conjunto com o controlador de rede sem fio, a identificação e controle de aplicações dos dispositivos clientes conectados ao

ponto de acesso, levando em consideração a camada 7 do modelo OSI.

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

VII. Deve oferecer suporte a mecanismo de localização e rastreamento de usuários (LocationBased Services).

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

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

X. Deve suportar atribuição dinâmica de VLAN por usuário.

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

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

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

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

XV. Implementar, pelo menos, os seguintes padrões de segurança wireless: (WPA) Wi-Fi Protected Access, (WPA2) Wi-Fi Protected Access 2, (WPA3) Wi-Fi Protected Access 3, (AES) AdvancedEncryption Standard, (TKIP) Temporal Key IntegrityProtocol, chave única por usuário, IEEE 802.1X e IEEE 802.11i.

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

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

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

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

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

XXI. Deverá suportar funções para análise de espectro.

XXII. Deve suportar conversão de tráfego multicast para unicast.

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

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

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

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

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

6.2.4.2. Solução de mobilidade – acesso WiFi outdoor:

a) Características gerais:

I. Deverá ser do mesmo fabricante do controlador WLAN para fins de compatibilidade.

II. Deverá possuir estrutura que permita a utilização do equipamento em locais internos e externos, com fixação em teto, parede e também em poste e fornecer acessórios para que possa ser feita a fixação

III. 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.

IV. Deverá possuir certificação IP-67.

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

VI. Possuir suporte a pelo menos 16 (dezesseis) SSIDs por ponto de acesso.

VII. Possibilitar alimentação elétrica via padrão PoE (IEEE 802.3af), visando não onerar o total de PoE disponível no switch e consumir, no máximo, 15.4 watts com todas as funcionalidades habilitadas.

VIII. Deve suportar temperatura de operação entre -20°C a 65°C.

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

X. Deverá possuir 1 (uma) interface 1 GbE, utilizando conector RJ-45, para conexão à rede local.

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

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

XIII. Deverá ser fornecido com a versão mais recente de software.

XIV. Deve ser compatível com IPv4 e IPv6.

XV. Deverá ser novo, de primeiro uso e estar na linha de produção atual do fabricante.

b) Características dos rádios:

I. O ponto de acesso deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n e IEEE 802.11ac Wave1 e Wave2, com operação nas frequências de 2.4 GHz e 5 GHz de forma simultânea.

II. Implementar as seguintes taxas de transmissão com fallback automático: IEEE 802.11b: 11, 5.5, 2 e 1 Mbps, IEEE 802.11a e IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps, IEEE 802.11n: 6.5 Mbps a 300 Mbps e IEEE 802.11ac: 6.5 Mbps a 867 Mbps.

III. Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n e IEEE 802.11ac, com ganhos de, no mínimo, 3dBi para 5GHz.

IV. Deverá suportar potência agregada de saída, considerando todas as cadeias MIMO, de, no mínimo, 24dBm na frequência de 5GHz e 23dBm na frequência de 2.4GHz.

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

VI. Deverá possuir mecanismo de rádio com suporte a SU-MIMO e MU-MIMO 2x2 com 2 fluxos espaciais.

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

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

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

c) Serviços, segurança e gerenciamento:

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

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

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

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

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

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

VII. Deve oferecer suporte a mecanismo de localização e rastreamento de usuários (LocationBased Services).

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

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

X. Deve suportar atribuição dinâmica de VLAN por usuário.

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

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

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

XIV. Implementar, pelo menos, os seguintes padrões de segurança wireless: (WPA) Wi-Fi Protected Access, (WPA2) Wi-Fi Protected Access 2, (WPA3) Wi-Fi Protected Access 3, (AES) AdvancedEncryption Standard, (TKIP) Temporal Key IntegrityProtocol, chave única por usuário, IEEE 802.1X e IEEE 802.11i.

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

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

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

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

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

XX. Deve implementar autenticação de usuários usando WISPr e Hotspot 2.0;

XXI. Deverá suportar funções para análise de espectro.

XXII. Deve suportar conversão de tráfego multicast para unicast.

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

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

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

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

6.2.4.3. Da Infraestrutura:

I. A responsabilidade pela instalação e manutenção da solução de Rede Wireless (Wi-Fi) será única exclusivamente da CONTRATADA. Deverão estar inclusos os serviços de instalação, manutenção preventiva e corretiva e atualização de licenças. A solução deverá ser configurada através de solução centralizada de gerenciamento.

II. A CONTRATADA deverá prover infraestrutura envolvida e realizar atividades de instalação e configurações para disponibilização dos itens necessários para o pleno funcionamento do serviço, buscando sempre atender aos mais atuais padrões de qualidade para instalações físicas e lógicas para este tipo de serviço.

III. Os itens que a CONTRATADA deverá fornecer são: Access Points (AP's) do tipo outdoor e indoor, antenas, injetores PoE ou switches PoE, modens, roteadores, caixas herméticas, dutos, racks, conectores e todos os demais acessórios para sua instalação.

IV. Será de responsabilidade da CONTRATANTE disponibilizar postes para instalação dos AP's outdoor e do fornecimento de energia elétrica para a operação contínua da Solução de Internet sem fio.

6.2.4.4. Solução de captive portal:

I. Deverá ser oferecido uma solução de Captive Portal que será totalmente compatível com a controladora wireless ofertada.

II. Deverá oferecer fácil customização para personalização do portal seguindo padrões da empresa (logo, cores e imagem);

III. Deverá suportar autenticação por meio de redes sociais (Pelo menos, Google, Facebook, Twitter);

IV. Permitir a autenticação (através de endereço MAC, Portal Captivo ou IEEE 802.1X) de usuários conectados à rede WLAN (wireless).

V. Oferecer recurso de Portal Captivo (Captive Portal), integrado a plataforma de gestão, permitindo a flexibilidade na implementação.

VI. O Captive Portal, interno ou integrado na plataforma de gestão, deverá disponibilizar recurso de auto cadastro do visitante ("self-register"), de forma que o visitante consiga acesso a rede sem necessitar que alguém criar sua conta de acesso.

VII. Deve suportar autenticação com Social Login.

VIII. Deve suportar também a utilização de Portal Captivo externo a solução;

IX. Deve permitir a customização do Portal, possibilitando a importação de imagens e logo;

X. Deve permitir a customização do Portal, possibilitando a importação de imagens e logo;

XI. Permitir a inclusão de anúncios no Captive Portal, para uso em campanhas de marketing ou institucionais.

XII. Possuir base de dados de usuários interna para autenticação de usuários convidados / temporários (acesso guest);

XIII. Realizar o controle de autorização baseado em perfis de acesso ou atributo;

XIV. Permitir que seja configurado um perfil de acesso, com regras aplicadas de firewall, para o qual será direcionado o usuário após sua autenticação

6.2.5. FORNECIMENTO DE SERVIÇO DE NOC (NETWORK OPERATION CENTER) NÍVEL 1,

INCLUINDO EQUIPE

6.2.5.1. Especificações Técnicas e Quantitativas:

a) A Contratada deverá prestar os serviços conforme as informações a seguir:

ITEM	DESCRIÇÃO	QTD	UND	CONSUMO
1	Fornecimento de mão de obra para compor a Central de Suporte remote e presencial do CONTRATANTE - jornada de trabalho em horário comercial (8:00 –18:00hrs)	**6**	Serviço	Mensal
	Software para registro de atendimentos e chamados		Licença	Anual

2	para a central de suporte do CONTRATANTE	**1**	anual	
3	Software para suporte e acesso remote	**8**	Licença anual	Anual
4	Treinamento de operações básicas para as unidades de informática do GEA (turma de 20 pessoas) – 24 horas	**1**	Serviço	Único

b) O **ITEM 01** descreve o serviço onde a Contratada deverá alocar 6 profissionais nas dependências da Contratante para atendimento e resolução de solução de problemas em forma de suporte em procedimentos operacionais (nível 1) de forma remota por meio de ferramentas computacionais e em caso de necessidade de intervenção física, se deslocar fisicamente aos endereços dos clientes da contratante. O deslocamento será fornecido pela Contratante;

c) O **ITEM 02** descreve a ferramenta para o Sistema de registro de chamados para o Contratante como todo, tanto o N1 e demais Níveis existentes nos órgãos como N2 para suporte especializado por meio de colaboradores do Contratante e N3 para suporte especializado por meio de terceirizados do Contratante, além disso, o sistema deverá fornecer usuários para todos os usuários internos, usuários clientes e usuários para fornecedores do Contratante. A estimativa é de em torno de 150 usuários com perfil de solicitante de chamados e em torno de 30 usuários que farão atendimentos. A ferramenta deverá possuir as seguintes funcionalidades:

- Sistema focado em Help desk e atendimento ao cliente (Interno e/ou externo);
- Centralização de ticket sem uma única plataforma (E-mail, central do cliente, chat, telefonia);
- Integração com ferramentas de comunicação como mídias sociais.
- Rastreabilidade de tickets;
- Melhor categorização de tickets através de campos personalizados: Serviços, Categorias, Urgências, etc;
- PushNotification para os solicitantes;
- Regras de SLA's personalizáveis;
- Regras de aprovações e agrupamento de tickets (Pai e Filho);
- Automações para atendimento de tickets;
- Base de conhecimento;
- Painel de indicadores completo com diversas métricas e visualizações;
- Relatórios de produtividade por atendentes;
- Filtros de consulta de atendimentos por órgãos, setor do governo, por usuário solicitante;
- Medição produtividade por SLA.

d) O **ITEM 03** descreve a ferramenta para fornecer ferramenta para acesso remoto às máquinas dos clientes do Contratante para realizar o atendimento remoto. A ferramenta deverá possuir as seguintes características mínimas:

- Acesso remoto por meio de comunicação de Intranet e Internet;
- Acesso remoto de forma segura, utilizando tecnologia de tunelamento de dados;
- Acesso controlado e registro de acesso;

- Realizar chamada vídeo chamada entre o atendente e o usuário;
- Realizar acesso a tela do usuário e realizar procedimentos de teste e resolução de problemas.

e) O **ITEM 04** será a realização de treinamento de operações básicas de serviços prestados pela Contratante para os clientes, e a Contratada poderá ministrar os treinamentos sob demanda.

6.2.5.2. Perfil dos Profissionais a Serem Fornecidos Pela Contratada:

6.2.5.2.1. Na equipe de profissionais que irá prestar serviços para a Contratante, cada um deverá possuir as seguintes formações e habilidades:

a) Possuir ensino médio completo com curso técnico em informática ou técnico em redes de computadores ou possuir curso superior em cursos superiores da área de Tecnologia da Informação;

b) Possuir os seguintes conhecimentos:

I. Atendimento ao cliente;

II. Manutenção e Redes de Computadores;

III. Possuir conhecimento de manutenção de hardware em nível básico - detecção de problemas em componentes tais como: placas, cabos, conectores, drivers, fontes e monitores;

IV. Conhecimentos em atividade de configuração de hardwares, softwares básicos e aplicativos de automação de escritório;

V. Conhecimento técnico de ambiente Windows, Linux, Microsoft Office e Open Office, Softwares de correio eletrônico MS-Outlook e Mozilla Thunderbird, Softwares de navegação na

internet: Internet Explorer, Google Chrome e Mozila Firefox para estações de trabalho (instalação, customização e manutenção);

VI. Possuir dinamismo para atuar com atendimento a usuários e utilização de Scripts de Atendimento;

VII. Conhecimento técnico do ambiente Internet, Intranet e Rede Corporativa;

VIII. Ter conhecimento em Instalação e Customização de sistemas corporativos em ambientes de duas camadas (cliente- servidor);

IX. Conhecimentos em Redes de Computadores, resolver problemas associadas a redes de computadores, dominar comandos e protocolos TCP/IP: ping, Traceroute, Ipconfig, NetStat, Route, ARP, conhecimentos de linha de comando dos roteadores como exemplo Mikrotik;

X. Conhecimento em antivírus e internet security, além de realizar diagnósticos e configurações;

XI. Conhecimento técnico sobre roteamento de redes;

XII. Conhecimento sobre testes de conectividade e identificação de comunicação com serviços de redes em servidores de plataforma Windows e GNU/Linux;

XIII. Domínio das atividades de instalação e customização de softwares e/ou produtos em estações de trabalho;

XIV. Domínio de técnicas de telessuporte ou telemarketing receptivo e ativo;

XV. Capacidade de expressar-se com clareza e objetividade, tanto na linguagem escrita como na falada;

XVI. Conhecimento na utilização de ferramentas de acesso remoto;

XVII. Conhecimento sobre serviços de redes como e-mail, servidor web, dns, firewall, proxy, domínio;

XVIII. Conhecimentos sobre configuração de serviços de redes tanto para ambientes Windows, GNU/Linux e/ou FreeBSD;

XIX. Conhecimentos sobre configuração de roteadores sem fio;

XX. Conhecimentos básicos sobre banco de dados e SGDB;

XXI. Conhecimentos em Resolução de problemas de funcionalidades de sites e portais, identificar mensagens de erros de conexão

XXII. Conhecimentos sobre sistemas de informação e aplicativos;

XXIII. Conhecimento sobre ferramenta de helpdesk;

XXIV. Conhecimento sobre testes de identificação de problemas seja na camada de rede, banco ou aplicação em sistemas de informação;

XXV. Conhecimento sobre ferramentas de acesso remoto.

6.2.5.3. Serviços a serem prestados pela Contratada:

I. Os profissionais da Contratada deverão prestar os serviços designados pela Contratante previamente, e toda nova atividade que os profissionais prestarem na central de suporte o

Contratante realizará o treinamento e repasse das atividades;

II. Os serviços a serem repassados para os profissionais será conforme o perfil técnico descrito neste Contrato;

III. Os profissionais da Contratada além de prestar os serviços, devem registrar todas as atividades no sistema de chamados, documentar todas as tarefas e ser responsável pela manutenção e atualização da base de conhecimento da central de suporte dos serviços de N1;

IV. Os profissionais da Contratada deverão ser distribuídos durante a jornada de atendimento do Contratante aos clientes que é de 8:00 horas até as 18:00 horas (de forma ininterrupta), sendo pelo período da manhã o período de maior demanda de suporte.

6.2.5.4. Operacionalização dos serviços:

a) Deverão ser disponibilizados os seguintes serviços:

I. Posições de Atendimento;
II. Comunicação;
III. Qualidade de Atendimento;
IV. Gestão do Atendimento;
V. Infraestrutura/Sistemas;
VI. Segurança da Informação.

6.2.5.5. Forma de prestação dos serviços – Níveis de atendimento:

a) Os atendimentos da Central de Relacionamento do Contratante atenderão em 2 (dois) níveis. A tramitação das demandas entre os canais e níveis, deve ocorrer através da mesma ferramenta de ITSM, disponibilizada pela Contratada, acompanhada de solução de integração entre os canais.

6.2.5.6. Nível de atendimento – N1 – 6 Técnicos:

6.2.5.6.1. Serviços Prestados: Deverão ser prestados os seguintes serviços:

I. Service Desk: Atendimento presencial/remoto, responsável pelo registro, análise, tratativa e direcionamento de chamados, atuando através dos seguintes critérios:

II. Ponto único de contato para a entrada de demandas relacionadas a TI;

III. Atendimento humano realizado de segunda a sexta-feira, das 8h às 18h, contemplando:

1. Atendimentos de Chamados abertos pelos diferentes canais;
2. Atendimento de Ligações;
3. Registro de Incidentes e solicitações no sistema de ITSM;
4. Monitoramento da Caixa de correio do Service Desk;
5. FCR (Correção de problemas simples como redefinições de Senhas e problemas previamente mapeados);
6. Atribuição de tickets para as Equipes de suporte (sempre que estiverem fora do seu skill de tratativa).

IV. Viabilizar meios para a captura de chamados, realizada em regime 24x7;

V. Serviço contemplando o atendimento remoto:

1. Suporte a Microinformática para usuários internos;

- Suporte a computadores e periféricos;
- Suporte a tablets e smartphones corporativos;
- Solicitação e liberação de licenças de softwares;

2. Suporte a impressão;

- Suporte geral ao usuário;
- Orientação na utilização dos equipamentos;
- Ponte de contato com os fornecedores das impressoras para suporte ao hardware;

3. Suporte a redes;

- Acesso remoto aos ativos internos de redes (roteadores, wifi etc.);
- Conhecimento sobre testes de identificação de problemas na camada de rede, banco ou aplicação;
- Suporte a telefonia;
- Atendimento remoto a incidentes;
- Registro e atendimento a solicitações;
- Posicionamento do status de chamados;

5. Acompanhamento / execução de Gmuds;

- Gestão de incidentes;

VI. Field Services;

VII. Atendimento presencial realizado de segunda a sexta-feira, das 8h às 18h;

VIII. Atendimentos em horários distintos poderão ser previamente agendados;

IX. Mesmo escopo de atuação da equipe de Service Desk, com atuação presencial na sede localizada na R. São José, 290 - Central, Macapá - AP, 68900-110 ;

X. Demandas de campo serão abertas e direcionadas pela equipe de Service Desk, sendo tratadas através do sequenciamento de tarefas.

XI. Serviço contemplando o atendimento presencial, realizando as seguintes atividades:

1. Suporte a Microinformática para usuários internos;

- Suporte a computadores e periféricos;
- Suporte a tablets e smartphones corporativos;
- Apoio na instalação de software;

2. Suporte a impressão;

- Suporte presencial ao usuário;
- Avaliação de problemas funcionais com os equipamentos de impressão;
- Revisão de insumos e itens de consumo;

3. Suporte a redes;

- Gestão presencial dos ativos internos de redes (roteadores, wifi etc.)
- Instalação, suporte e configuração;

4. Suporte telefonia;

- Atuação presencial;

5. Atividades de IMAC;

- Instalação;
- Movimentação;
- Adição;
- Mudanças.

XII. Governança:

1. O Catálogo de Serviços deve ser construído pela Contratada durante o período de assessment;

- Realizar a análise das responsabilidades das equipes de serviço, a fim de mapear os tipos de atendimento realizados atualmente;
- Documentar os parâmetros que serão utilizados para aconstrução do catálogo de serviços implementar o catálogo na ferramenta de ITSM
- Capacitar todos os recursos que irão interagir com o catálogo
- Mapear e cadastrar os níveis de serviço para cada item
- Acompanhar a utilização do catálogo de serviços, realizando as alterações necessárias durante todo o período de prestação dos serviços Elaborar os scripts de atendimento que deverão ser utilizados pelos analistas durante a tratativa de Incidentes e Solicitações
- Desenhar o fluxo de escalonamento com nomes, números detelefone e e-mails de contato dos interlocutores responsáveis por atuarem na resolução dos incidentes;

2. O processo de Gestão de relatórios, métricas, indicadores e apresentações dos serviços prestados será realizado pela empresa Contratada, sendo parte do escopo as seguintes atividades;

- Validar os indicadores que serão utilizados para medir a entrega dos serviços da Contratada
- Desenvolver mecanismo para acompanhamento e controle dos indicadores
- Implementar rotinas de apresentação periódica dos indicadores para a Contratante (book mensal de serviços e reports periódicos)

- Propor constantemente novos meios de acompanhamento para garantir a melhoria contínua no processo
- Todos os números apresentados pela equipe de Governança,bem como os processos e procedimentos implementados, poderão ser auditados a qualquer momento pela Contratante;

3. A implementação dos Processos ITIL será parte do escopo dos serviços da contratada, sendo esta realizada através das seguintes macro tarefas;

- Análise do ambiente atual que será sustentado por este contrato;
- Avaliação da aderência dos processos ITIL na rotina de execução dos serviços.
- Avaliação da aderência dos serviços prestados pela Contratada com o processo de Gestão de Mudanças;
- Avaliação da aderência dos serviços prestados pela Contratada com o processo de Gestão de Incidentes;
- Avaliação da aderência dos serviços prestados pela Contratada com o processo de Gestão de Problemas;
- Avaliação da aderência dos serviços prestados pela Contratada com as demais disciplinas ITIL pertinentes ao serviço.
- Desenho e implementação das rotinas pertinentes
- Acompanhamento da evolução dos processos durante toda a duração do contrato;

XIII. Melhoria Contínua de serviços, realizando, mas não se restringindo a:

1. Acompanhamento da performance dos recursos que prestam os serviços;
2. Treinamento, Capacitação e Reciclagem;
3. Identificação de oportunidades de melhoria;
4. Detecção de oportunidades de redução do esforço ou agilidade no atendimento, seja através de procedimentos, automações ou demais artifícios que possam ser implementados na operação;
5. Elaborar e implementar procedimentos para a Pesquisa de Satisfação dos usuários do serviço;

XIV. Responsável pela Base de Conhecimento, realizando, mas não se restringindo a:

1. Desenho de processos e procedimentos utilizados pelas equipes de serviços da Contratante;
2. Acompanhamento da efetividade dos procedimentos elaborados;
3. Revisão e manutenção dos processos e procedimentos conforme demanda;
4. Alinhamento com áreas externas para viabilizar a criação de novos conteúdos;

5. 5. Controle do versionamento de documentação, distribuição de versões e capacitação das equipes envolvidas;

XV. Serviços especializados:

1. Gestão de ativos, responsável por:

- Mapeamento dos ativos utilizados pelas equipes da Contratante;
- Tabulação e registro dos ativos;
- Construção e administração dos controles de ativos;
- Sinalização de eventuais demandas de ativos de TI, identificadas durante o processo de gestão;

2. Banco de dados, responsável por:

- Ser o ponto focal da Contratante referente a temas relacionadas à utilização dos bancos de dados;
- Ser responsável pela elaboração de consultas para atender a demandas pontuais de extração de informações;

3. Aplicações, responsável por:

- Gestão dos sistemas internos utilizados pela Contratante
- Criação e revogação de usuários nos sistemas
- Análise e avaliação de novos sistemas que possam ser implementados na operação
- Ser o ponto focal da Contratante referente a temas relacionados a aplicações;

XVI. Sistemas e ferramentas:

1. ITSM: Disponibilização de um sistema de ITSM para controle de todos os processos realizados pela Contratada, incluindo, mas não se resumindo a:
2. Chat: Principal canal de contato para abertura de chamado:
3. Telefonia, utilizada como meio de contato adicional com a central de serviços:
4. E-mail, utilizado como canal de apoio para a tratativa dos chamados;
5. Base de conhecimento;
6. Acesso Remoto: Disponibilizar solução que permita o acesso remoto aos equipamentos, viabilizando assim o suporte sem a demanda de atuação presencial;

6.2.5.6.2. Fornecimento de serviço de mão de obra especializada para NOC (Network Operation Center) nível 2:

I. 2º Nível de Atendimento – Suporte Técnico Presencial – N2

1. O serviço de Atendimento e Suporte Técnico de 2º Nível atuará naresolução de incidentes e requisições de serviços escalados pelo Serviço de Atendimento e Suporte Técnico de 1º Nível, além de elaborar e gerir procedimentos, scripts e itens da base de conhecimento sobre erros conhecidos, atuando em incidentes ou solicitações de maior complexidade e aqueles que envolvem usuários especiais;
2. A equipe alocada neste serviço buscará prevenir a ocorrência de problemas e seus incidentes resultantes, eliminar incidentes recorrentes correlacionando-os e identificando a causa raiz e sua solução, além de minimizar o impacto dos incidentes que não podem ser prevenidos;

3. O Serviço de Atendimento e Suporte Técnico de 2º Nível será responsável por prestar as seguintes atividades básicas;

- Prestar suporte presencial, de segundo nível, aos usuários de TIC da CONTRATANTE, no atendimento de requisições de serviço e resolução de incidentes ou problemas não resolvidos pelo Serviço de Atendimento e suporte Técnico de 1º Nível, respeitando os Indicadores de Medição de Resultados acordados;
- Executar e restaurar cópias de segurança de dados (backup) localizados nas estações de trabalho dos servidores da CONTRATANTE;
- Contatar o usuário demandante para obter maiores informações, se necessário, e prestar a devida orientação;
- Contatar as equipes internas da área de TIC da CONTRATANTE para auxílio no diagnóstico ou solução do chamado do usuário, se necessário;
- Contatar outras equipes ou prestadores de serviço da CONTRATANTE que porventura possuam correlação com o incidente, problema ou requisição a ser tratada, se necessário;
- Registrar, diagnosticar e solucionar problemas referentes aos serviços de TIC da CONTRATANTE;
- Correlacionar incidentes a fim de identificar sua causa raiz, solucioná-la e prevenir novas ocorrências;
- Repassar conhecimentos a respeito de questões relativas à Central de Serviços para as equipes internas da CONTRATANTE;
- Escalar os chamados não resolvidos neste nível para o 3º (terceiro) nível de suporte ou fornecedores de serviços e produtos de TIC contratados pela CONTRATANTE, quando for o caso;
- Esclarecer dúvidas de usuários quanto ao uso de softwares básicos, aplicativos, sistemas de informações, equipamentos e aparelhos de TIC em geral;
- Oferecer orientações técnicas e dicas quanto ao uso de
- funcionalidades e facilidades disponíveis nos softwares básicos, aplicativos, sistemas de informações e equipamentos de TIC em geral;
- Orientar os usuários quanto aos produtos e serviços de TIC fornecidos pela CONTRATANTE;
- Apoiar e orientar tecnicamente o suporte de 1º (primeiro) nível, quando necessário; e
- Executar outros serviços correlatos ao atendimento de usuários;

6.2.5.6.3. Analista de Suporte Técnico Especializado – Nível 2 – 1 técnico:

1. Requisitos de qualificação técnica do Analista – N2:

a. Entendimento de sistemas operacionais (Windows, Linux e FreeBsd);
b. Configuração física e lógica de redes (TCP/IP, ranges de IP, subnets/máscaras, gateways, roteamento, topologia de rede, etc.);
c. Segurança de redes e banco de dados;
d. Varredura e análise de vulnerabilidades, detecção de intrusos, correção de falhas de segurança da informação, tratativas de incidentes, propostas de melhorias, assim como outras relacionadas à atividade de Pentester;
e. Conhecimento em DNS(BIND);
f. Conhecimento de Firewall;
g. Conhecimento de virtualização (Vmware e Nutanix);
h. Conhecimento em conteinerização (Docker Cubernet, openshift);

6.2.5.6.4. Fornecimento de serviço de mão de obra especializada para NOC (Network Operation Center) sustentação e retaguarda:

1. 3º Nível de Atendimento – Sustentação e Retaguarda – 1 técnico: a. As seguintes atividades compõem os processos do serviço de Sustentação e Retaguarda:

- Atuar nas demandas de instalação, configuração, gerenciamento, atualização e monitoramento de Banco de Dados, visando assegurar a continuidade e suporte das aplicações, em conformidade com a complexidade e volumetria estimada;
- **DBA – SQL SERVER;**

b. Requisitos de qualificação técnica do perfil de Analista de Banco de Dados – DBA:

- Conhecimentos da linguagem estruturada SQL;
- Conhecimentos em estrutura de banco de dados (Postgres, Oracle, Mysql, etc.);
- Conhecimentos em estrutura de banco de dados mais precisamente em diagrama entidade-relacionamento;
- Entendimento básico de Arquitetura de computadores;
- Um bom entendimento do funcionamento dos sistemas operacionais (Linux/Unix e rotinas em shell script);
- Realização de backup/recovery (RMAN quando o BD é Oracle);
- Realização de backup/recovery Postgres e Mysql;
- Criação e testes de backup para garantir a recuperabilidade dos dados em caso de falha de hardware ou outros problemas severos;
- Instalar e atualizar as ferramentas do banco de dados;
- Alocar o espaço do sistema reservado ao banco e garantir uma alocação futura no sistema;
- Saber modificar a estrutura do banco de dados;
- Saber os comandos básicos e exclusivos de cada SGBD;
- Verificar e zelar pela integridade do banco de dados;
- Ter um controle de acesso, ou privilégios, aos dados como quem pode acessar e o que pode acessar e talvez quando possa acessar;
- Garantir o acesso ao banco de dados no maior tempo possível;
- Garantir o máximo de desempenho para as consultas ao banco de dados;
- Auxiliar a equipe de desenvolvimento e a equipe de testes a maximizar o uso e desempenho do banco de dados;
- Contatar suporte técnico em caso de certos problemas com o banco de dados

6.2.5.7. Fornecimento dos equipamentos de conectividade:

I. A prestação do serviço deverá incluir a previsão de instalação dos equipamentos de conectividade (roteadores, switch, modem, conversores, antenas, etc) necessários, contemplando os serviços de implantação, configuração, manutenção e gerenciamento dos mesmos;

II. Caberá à Contratada o serviço de instalação, configuração e manutenção de qualquer equipamento por ela fornecido, que venha a ser substituído durante a vigência do contrato;

III. Caberá a Contratante a responsabilidade por toda infraestrutura elétrica (aterramento, DG, etc) interna às unidades dos órgãos necessária para o funcionamento adequado do serviço;

IV. Caberá a Contratante a responsabilidade por toda infraestrutura lógica entre o

equipamento de conectividade fornecido pela Contratada e a rede interna às unidades dos órgãos necessária para o funcionamento adequado do serviço.

V. Todos os equipamentos fornecidos pela Contratada deverão estar configurados com os devidos materiais e acessórios para montagem;

6.2.5.8. Equipamento CPES:

I. Deverá ser disponibilizado pela Contratada, quando necessário, juntamente com os serviços de comunicação de dados, os equipamentos CPE's (Customer premises equipament) ou Modens que se referem aos equipamentos terminais de rede situados dentro dos limites de propriedade do Contratante.

6.3. REQUISITOS COMPLEMENTARES

6.3.1. REUNIÕES:

6.3.1.1. A Contratada junto com a Contratante deverá promover reuniões semanais, quinzenais ou mensais de acordo com as demandas em andamento no intuito de avaliar e zelar pela qualidade de atendimento e serviços;

6.3.2. ESTRUTURA DE ATENDIMENTO:

6.3.2.1. A Contratada deverá manter um canal de atendimento gratuito, por meio de serviço

0800, para suporte técnico e solicitações de baixa complexidade disponível 24h X 7d (Call Center). O ambiente da estrutura de atendimento da Contratada poderá ser operacionalizado em qualquer município do país, desde que atenda todos os requisitos de qualificação técnica e de segurança de TIC, bem como das melhores práticas de mercado.

6.3.2.2. A Contratada deverá manter em seu quadro próprio uma equipe dedicada à atender as demandas da Contratante;

6.3.2.3. Esta equipe deverá ser formada por:

a) Um gerente de contas responsável pelo relacionamento direto com a Contratada e demanda comerciais;

b) Um engenheiro especializado em telecomunicações com, no mínimo, 2 anos de experiência, responsável por dar atendimento consultivo à equipe de TI da Contratante;

c) Um analista responsável por gerir a planta de serviços da Contratante e o seu correto faturamento, bem como dirimir dúvidas sobre este tema quando for necessário;

d) Um gestor de projetos e serviços responsável por garantir a entrega dos serviços

bem como os índices de qualidade exigidos;

e) Um gestor técnico responsável por administrar as ocorrências de defeitos/falhas dos serviços de comunicação de dados.

6.3.3. DO PORTAL DE GESTÃO DE CONTAS:

6.3.3.1. A Contratada deverá disponibilizar um sistema de gestão de contas online, sem ônus, que ofereça, no mínimo, as funcionalidades a seguir:

1. Ser acessado via WEB e compatível com navegadores padrão de mercado tais como: Internet Explorer, Microsoft Edge, Google Chrome e Mozilla Firefox;

2. Deverá utilizar o protocolo HTTPS para acesso ao portal;

3. Deverá ser em idioma português do Brasil;

4. Deverá possuir, no próprio portal, manual de utilização para auxílio dos usuários;

5. Deverá possuir alerta para acesso a área exclusiva de notificações para o usuário;

6. Deverá possuir recurso de enviar notificações de novas contas para o e-mail aos usuários;

7. Deverá armazenar os dados históricos de contas pelo período mínimo de 60 meses;

8. Permitir visualizar as contas de todos os serviços contratados;

9. Deverá possuir, no mínimo, três níveis de usuários com as seguintes permissões:

a) Nível 1 – É o administrador principal da Contratante, possui maior hierarquia e pode executar as funções de criação/exclusão de usuários, visualização/alteração relatórios, visualização de faturas e associação usuários de a contratos/serviços;

b) Nível 2 – É o administrador de contas, possuindo as mesmas atribuições de Nível 1 com exceção de alteração de relatórios, ou seja, pode apenas visualizar;

c) Nível 3 – É o usuário cliente, possuindo a permissão de visualização de faturas e relatórios;

10. A plataforma deverá possibilitar a criação de usuários via o perfil Nível 1, sendo que o novo usuário deverá receber uma notificação por e-mail para completar seu cadastro e ser ativado na plataforma;

11. A plataforma deverá prever um limite de, no máximo, 7 (sete) dias para que o novo usuário possa completar seu cadastro e ativar o usuário. Caso o prazo seja expirado, o convite deve ser reenviado;

12. Deverá prever que os usuários possam visualizar Contas/Contratos de mais de um CNPJ/Razão Social podendo ter perfis diferentes por CNPJ/Razão Social;

13. Deverá permitir a criação de usuários em massa;

14. Deverá permitir, via portal, a redefinição da senha de acesso dos usuários;

15. Deverá possuir Filtro para visualização de dados com pelo menos: Produto, Contrato e CNPJ;

16. Deverá possuir sinalização para controle de leitura de contas;

17. Deverá permitir a exportação de contas nos formatos PDF e FEBRABAN;

18. Deverá permitir a exportação de contas em massa;

19. Deverá oferecer visualização de, no mínimo, os seguintes campos:

a) Tipo do Documento;
b) CNPJ;
c) Razão Social do Cliente;
d) Data de Vencimento;
e) Data Disponibilização da Conta;
f) Valor Total;
g) Mês de Referência da conta;

20. Deverá apresentar, sempre, a conta atual válida. Caso haja mudança na

conta/fatura em virtude de contestações, o portal deve apresentar a conta ajustada com um flag para diferenciação;

21. A Contratada deverá promover treinamento à Contratante para no mínimo 10 pessoas com instrutores devidamente capacitados e todo o material necessário;

22. O treinamento deverá ocorrer nas dependências da Contratante, em prédio situado na cidade de Macapá, estado do Amapá;

23. O portal ofertado deverá substituir as contas físicas, que não precisarão ser enviadas para a Contratante;

24. A Contratada deverá enviar as contas detalhas por meio digital, via e-mail ou aplicativo instalado no computador da Contratante.

CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DO CONTRATANTE E DA CONTRATADA

7.1. São obrigações da Contratante:

7.1.1. Permitir acesso dos empregados da Contratada às suas dependências para execução dos serviços referentes ao objeto, quando necessário;

7.1.2. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos empregados da Contratada;

7.1.3. Assegurar-se da boa prestação dos serviços, verificando sempre o seu bom desempenho;

7.1.4. Assegurar-se de que os preços contratados estão compatíveis com aqueles praticados no mercado palas demais prestadoras dos serviços objeto desta contratação, de forma a garantir que continuem a ser os mais vantajosos para a Administração;

7.1.5. Solicitar, sempre que julgar necessário, a comprovação do valor vigente dos preços na data da emissão da nota fiscal fatura de serviços;

7.1.6. Controlar as ligações realizadas e documentar as ocorrências havidas;

7.1.7. Fiscalizar o cumprimento das obrigações assumidas pela Contratada, inclusive quanto à continuidade da prestação dos serviços que, ressalvados os casos de força maior justificados e aceitos pelo Contratante, não deve ser interrompida;

7.1.8. Acompanhar e fiscalizar o andamento dos serviços, por intermédio do Gestor de TI;

7.1.9. Notificar a Contratada, por escrito, acerca de eventuais falhas ou irregularidades constatadas na execução dos serviços para que sejam adotadas as medidas corretivas necessárias;

7.1.10. Efetuar o pagamento nas condições e preços pactuados;

7.1.11. Exigir o fiel cumprimento de todos os requisitos acordados e da proposta apresentada,

podendo rejeitar os serviços no todo ou em parte, caso não estejam sendo prestados com qualidade.

7.2. São obrigações da Contratada:

7.2.1. Designar consultor para acompanhamento do objeto contratado e atendimento das reclamações feitas pelo Contratante; **7.2.2.** Fornecer número telefônico para registro das reclamações sobre o funcionamento do serviço contratado, com funcionamento 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana;

7.2.3. Prestar as informações e os esclarecimentos solicitados, em até 48 (quarenta e oito) horas, a contar da solicitação do Contratante;

7.2.4. Responder, em relação aos seus empregados, por todas as despesas decorrentes da execução dos serviços, tais como: salários, seguros de acidente, taxas,

impostos,contribuições, indenizações, vales-refeição, vales-transporte, e outras que porventura venham a ser criadas e exigidas pelo Governo;

7.2.5. Responder pelo cumprimento dos postulados legais vigentes de âmbito federal, estadual ou municipal, bem, ainda, assegurar os direitos e cumprimento de todas as obrigações estabelecidas por regulamentação da ANATEL, inclusive quanto aos preços praticados;

7.2.6. Zelar pela perfeita execução dos serviços contratados, devendo as falhas que porventura venham a ocorrer, degradando a qualidade do serviço, serem sanadas em até 12 (doze) horas para os serviços de comunicação de dados, em conformidade com o item 6.2.3.2 (Acordo de Nível de Serviço);

7.2.7. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis e às recomendações aceitas pela boa técnica;

7.2.8. Atender prontamente quaisquer exigências do representante do Contratante, inerentes ao objeto do contrato;

7.2.9. Fornecer ao Contratante, mensalmente, nota fiscal fatura de serviços;

7.2.10. Comunicar à Coordenação Administrativa, por escrito, qualquer anormalidade de caráter urgente e prestar os esclarecimentos julgados necessários;

7.2.11. Assumir a responsabilidade pelos encargos fiscais e comerciais resultantes da contratação;

7.2.12. Em nenhuma hipótese, veicular publicidade ou qualquer outra informação acerca da prestação

dos serviços sem prévia autorização do Contratante;

7.2.13. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações a serem assumidas, todas as condições de habilitação e qualificação exigidas.

CLÁUSULA OITAVA – DA SUBCONTRATAÇÃO

8.1. Para atendimento às necessidades técnicas será admitida a constituição de consórcios, observada a legislação brasileira que regula a matéria e a subcontratação de empresas fornecedoras de produtos e/ou serviços necessários à composição da solução, de acordo com as exigências previstas neste Contrato e seus anexos.

CLÁUSULA NONA – DA PRESTAÇÃO, PRAZO, LOCAL E CONDIÇÕES DE EXECUÇÃO DOS SERVIÇOS

9.1. Por tratar-se de prestação de serviço continuado o prazo de vigência contratual será de **12 (doze) meses**;

9.2. Contratada fica obrigada a executar os serviços em até 45 (quarenta e cinco) dias corridos após a assinatura do contrato e/ou ordem de serviço da Contratante;

9.3. O prazo de que trata o subitem anterior poderá ser prorrogado uma única vez por igual período, em casos devidamente justificados e autorizados pela Contratante;

9.4. Toda ativação/mudança de serviços está condicionada a viabilidade técnica no endereço de instalação;

9.5. Os objetos deverão ser entregues em até **15 (quinze) dias úteis** após o recebimento da nota de empenho e de acordo com a solicitação formal do órgão **no seguinte endereço**: PREDIO DA NATI/SESMA – AVENIDA JOSÉ MALCHER 2821 – SÃO BRÁS **- Horário de 08h às 17h, de 2ª a 6ª-feira – terceiro andar**, para efetivar a entrega respectiva, quando então apresentará a nota fiscal correspondente. A empresa vencedora deverá comunicar a data e o

horário previsto para a entrega de cada um dos links ao **NATI/SESMA/PMB**, no horário de expediente, com no mínimo 48 (quarenta e oito) horas de antecedência.

9.6. A critério da **CONTRATANTE** poderá ser modificado o local de instalação, para outro endereço no Município de Belém, sem qualquer tipo de ônus adicionais, desde que verificada a viabilidade;

9.7. O recebimento e a aceitação dos objetos estarão condicionados após avaliação pelo responsável técnico do NATI/**SESMA/PMB**, sendo atestados, mediante avaliação técnica favorável.

9.8. A aceitação do objeto está condicionada ao atendimento das especificações mínimas constantes deste termo de referência.

9.9 Apresentar os equipamentos para a prestação do serviço de internet novos e em embalagem em perfeito estado;

9.10 No **ATO DA ENTREGA DOS EQUIPAMENTOS DE REDE para a ativação do serviço, os equipamentos** não poderão conter prazo de validade inferior a 75% (setenta e cinco por cento) de sua validade total.;

9.11 Não serão aceitos objetos diferentes dos especificados neste Termo de Referência, fora dos prazos mínimos estipulados, em mau funcionamento, de qualidade inferior, ou com os equipamentos de rede danificados ou com os lacres de segurança rompidos;

9.12 Caso, durante o prazo de instalação, seja constatado quaisquer defeitos ou divergências nas características dos objetos, o Contratante, comunicará o fato, por escrito, ao Fornecedor, **sendo de até 5 (cinco) dias úteis o prazo para correção dos defeitos e/ou troca dos equipamentos em comodato**, contadas a partir da solicitação efetuada, sem qualquer ônus à Administração Pública;

9.13 Locais e endereços para as instalações consta no Termo de Referência e seus anexos.

CLÁUSULA DÉCIMA – DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

10.1. Nos termos do art. 67 da Lei nº 8.666, de 1993, tão logo o Contrato seja firmado, será designado representante para acompanhar e fiscalizar a conformidade da prestação dos serviços anotando em registro próprio todas as ocorrências relacionadas ao fornecimento e determinando o que for necessário à regularização de falhas ou defeitos constatados;

10.2. As decisões e providências que ultrapassarem a competência do representante da Administração deverão ser solicitadas aos seus superiores em tempo hábil para a adoção das medidas convenientes;

10.3. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em co responsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993;

10.4. Durante o período de fornecimento do objeto, a Empresa poderá manter preposto, aceito pela Administração contratante, para representá-la sempre que for necessário;

CLÁUSULA DÉCIMA PRIMEIRA – DO REAJUSTE

11.1. Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

11.1.1. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o de acordo com o Índice de Serviço de Telecomunicações (IST) da Agência Nacional de Telecomunicações (ANATEL), exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

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

11.3. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

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

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

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

11.7. O reajuste será realizado por apostilamento.

CLÁUSULA DÉCIMA SEGUNDA – DAS ALTERAÇÕES

12.1. O objeto contratado poderá sofrer **ACRÉSCIMOS OU SUPRESSÕES no limite percentual de 25%**,mediante celebração de Termo Aditivo, de acordo com o disposto no Art. 65, caput e § 1º, da Lei nº 8.666/1993, ficando a CONTRATADA obrigada a aceitar, nas mesmas condições contratuais.

CLÁUSULA DÉCIMA TERCEIRA – DAS PENALIDADES

13.1. Com fundamento no Art. 7º da Lei n.º 10.520/2002 e Art. 29 do Decreto Estadual n.° 2.648/2007, ficará impedida de licitar e contratar com o Estado do Amapá e será descredenciada do cadastro de fornecedores, pelo prazo de até 5 (cinco) anos, sem prejuízo demais cominações legais, a CONTRATADA que:

a) Não mantiver a proposta;
b) Deixar de entregar a documentação exigida no certame ou apresentar documentação falsa;
c) Ensejar o retardamento da execução do objeto;
d) Fornecer material que não atenda à especificação exigida no edital;
e) Falhar ou fraudar na execução do contrato;
f) Comportar-se de modo inidôneo;
g) Fizer declaração falsa;
h) Cometer fraude fiscal.

13.2. Para os fins da alínea "f", reputar-se-ão inidôneos atos como os descritos no Art. 178 da Lei n.° 14.133/2021.

13.3. Com fundamento nos artigos 86 e 87 da Lei nº 8.666/1993 e suas alterações, a CONTRATADA ficará sujeita, no caso de atraso injustificado, assim considerado pela Administração, inexecução parcial ou inexecução total das obrigações, sem prejuízo das responsabilidades civil e criminal, às seguintes penalidades:

a) Advertência, por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a CONTRATANTE;
b) Multa moratória de 0,5% (cinco décimos por cento) por dia de atraso injustificado e por ocorrência de fato em desacordo com o proposto e o estabelecido neste edital, até o máximo de 15% (quinze por cento) sobre o valor da parcela inadimplida, recolhida no prazo máximo de 15 (quinze) dias corridos, uma vez comunicados oficialmente;
c) Multa compensatória de até 15% (quinze por cento) sobre o valor total do Contrato, no caso de inexecução total do objeto e pela recusa em retirar a Nota de Empenho, recolhida no prazo máximo de 15 (quinze) dias corridos, uma vez comunicada oficialmente, e sem prejuízo da aplicação de outras sanções legalmente previstas;
d) Em caso de inexecução parcial, a multa compensatória, no mesmo percentual da alínea anterior,
será aplicada de forma proporcional à obrigação inadimplida;
e) Suspensão temporária de participar em licitação, pelo prazo de até 02 (dois) anos, em relação ao órgão da administração ou entidade Contratante que a aplicou;
f) Impedimento de licitar e contratar com o Estado do Amapá com o consequente descredenciamento do Cadastro Central de Fornecedores do Estado do Amapá, pelo prazo de até 05 (cinco) anos;
g) 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 a CONTRATADA ressarcir a CONTRATANTE pelos prejuízos causados.

13.4. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei n.º 8.666, de 1993, a CONTRATADA que:
a) tenha sofrido condenação definitiva por praticar, por meio doloso, fraude fiscal no recolhimento de quaisquer tributos;
b) tenha praticado atos ilícitos visando a frustrar os objetivos da licitação;

c) demonstre não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados;

13.5. As sanções previstas nas alíneas “a”, “e” e “f” do item 13.3 desta Seção poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados, sem prejuízo de perdas e danos cabíveis.

13.5.1. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do infrator, o Estado do Amapá ou a Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

13.6. A aplicação de qualquer das penalidades previstas neste instrumento realizar-se-á mediante processo administrativo que assegure o contraditório e a ampla defesa, observando-se o rito previsto na Lei nº 12.846/2013 (Lei Anticorrupção), e, subsidiariamente, o procedimento previsto na Lei nº 8.666/1993 e na Lei nº 9.784/1999.

13.7. A competência para processamento das penalidades, antes da homologação da Licitação, é da Central de Licitações e Contratos. Após, a responsabilidade será do respectivo órgão Contratante.

13.8. Em atenção ao princípio da proporcionalidade, na estipulação das sanções, a autoridade competente deverá considerar a gravidade da conduta do infrator, o caráter educativo da pena, o grau de comprometimento do interesse público e o prejuízo pecuniário decorrente das irregularidades constatadas.

13.9. A CONTRATANTE poderá reter dos pagamentos devidos à CONTRATADA, como medida cautelar, independentemente de sua manifestação prévia, valor relativo à eventual multa a ser aplicada em razão de inadimplemento contratual, com base no Art. 45 da Lei nº 9.784/1999.

13.10. O valor da multa aplicada será descontado dos pagamentos eventualmente devidos à CONTRATADA ou da garantia prestada, quando houver, ou ainda, quando for o caso, cobrado judicialmente.

13.11. Aplicada à penalidade de multa, após regular processo administrativo, e observado o disposto nas condições deste Edital, a licitante será notificada para efetuar o recolhimento do seu valor, no prazo de 30 (trinta) dias, contados da notificação.

13.12. Se, durante o processo de aplicação de sanção, houver indícios de prática de ato ilícito tipificado pela Lei nº 12.846, de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

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

13.14. As situações dispostas no art. 78 da Lei 8.666/1993 poderão ensejar, a critério da Administração, a rescisão unilateral do contrato.

CLÁUSULA DÉCIMA QUARTA – DA RESCISÃO

14.1. Não cumprimento ou o cumprimento irregular das cláusulas e condições estabelecidas em instrumento contratual, por parte da empresa, assegurará ao órgão demandante, sem ônus de qualquer espécie para este e sem prejuízo do disposto na cláusula anterior, o direito de dá-lo por rescindido, mediante notificação através de ofício, com antecedência mínima de 30 (trinta) dias corridos, entregue diretamente ou via postal, com prova de recebimento, sem prejuízo dos demais motivos previstos no Art. 78 da Lei nº 8.666/93 e alterações posteriores;

14.2. A rescisão do contrato dar-se-á nas seguintes modalidades, consoante estabelece o Art. 79 da Lei nº 8.666/93 e alterações posteriores:

a) Unilateralmente, a critério exclusivo da Administração CONTRATANTE, assegurado o contraditório e a ampla defesa, mediante notificação por ofício, com antecedência mínima de 30 (trinta) dias corridos, entregue diretamente ou via postal, com prova de recebimento, sem ônus de qualquer espécie para este nos casos enumerados nos incisos I a XII e XVII e XVIII, do Art. 78 da mesma Lei, e sem prejuízo do disposto na Cláusula "Das Penalidades";

b) Amigavelmente, por acordo entre as partes, reduzido a termo, desde que haja conveniência para a Administração CONTRATANTE; e

c) Judicialmente, nos termos da legislação vigente.

14.3. A rescisão **administrativa** ou **amigável** deverá ser precedida de autorização escrita e fundamentada, devidamente ratificada pelo Gestor do órgão demandante;

14.4. No procedimento que visa à rescisão do contrato, será assegurado o contraditório e a ampla defesa, sendo que, depois de encerrada a instrução inicial, a empresa terá o prazo de 5 (cinco) dias úteis para se manifestar e produzir provas, sem prejuízo da possibilidade da Contratante adotar, motivadamente, providências acauteladoras, como a retenção dos créditos decorrentes do contrato até o limite dos prejuízos causados, dentre outras medidas, para que não haja a imediata interrupção dos serviços.

14.5. A CONTRATADA reconhece, desde já, os direitos da CONTRATANTE em caso de rescisão administrativa prevista na legislação referente a Licitações e Contratos Administrativos.

CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS

15.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 10.520/2002; na Lei nº 8.666/1993, subsidiariamente, ao contido na Lei nº 8.078/1990 (CDC); demais normas aplicáveis e princípios gerais dos contratos.

CLÁUSULA DÉCIMA SEXTA – DA PUBLICAÇÃO

16.1. O presente Contrato deverá ser publicado, em resumo, no Diário Oficial do Estado do Amapá, no prazo máximo de 20 (vinte) dias a contar do 5º (quinto) dia útil do mês seguinte a sua assinatura, conforme preceitua o art. 61, parágrafo único, da Lei n.º 8.666/93.

CLÁUSULA DÉCIMA SÉTIMA – DO PRAZO DE VIGÊNCIA

17.1. O prazo de vigência deste Contrato será de **12 (doze) meses**, com início na data de assinatura do contrato, sendo que a vigência inicialmente prevista poderá ser prorrogada por iguais e sucessivos períodos, mediante a celebração de Termos Aditivos, limitado a 48 (quarenta e oito) meses, já computados os iniciais, conforme disposto no Art. 57, IV, § 2º da Lei 8.666/93, caso sejam preenchidos os requisitos abaixo enumerados de forma simultânea, e autorizado formalmente pela autoridade competente:

a) Os serviços tenham sido prestados regularmente;
b) A contratada não tenha sofrido qualquer punição de natureza pecuniária;
c) O contrato permaneça economicamente vantajoso para a administração;
d) A administração ainda tenha interesse na realização do serviço.

CLÁUSULA DÉCIMA OITAVA – DO FORO

18.1. O Foro deste contrato é o da Comarca de Belém, com exclusão total de qualquer outro que seja invocável. E por estarem assim, justos e contratados, o presente instrumento será lavrado em 02 (duas) vias de igual teor e forma, que, depois de lido e achado em ordem, vai assinado pelas partes contraentes na presença de 02 (duas) testemunhas.

Belém, 28 de setembro de 2023.

BRUCY MARTINS COSTA:40089797272
Assinado de forma digital por BRUCY MARTINS COSTA:40089797272
Dados: 2023.09.28 15:48:42 -03'00'

SR. BRUCY MARTINS COSTA
OI S.A., EM RECUPERAÇÃO JUDICIAL, SOCIEDADE ANÔNIMA

Gustavo Giraldes Bettoni
GUSTAVO GIRALDES BETTONI:00377343935
Assinado de forma digital por GUSTAVO GIRALDES BETTONI:00377343935
Dados: 2023.09.28 14:25:38 -03'00'

GUSTAVO GIRALDES BETTONI
OI S.A., EM RECUPERAÇÃO JUDICIAL, SOCIEDADE ANÔNIMA

PEDRO RIBEIRO ANAISSE:18422730278
Assinado de forma digital por PEDRO RIBEIRO ANAISSE:18422730278
Dados: 2023.09.28 17:24:13 -03'00'

PEDRO RIBEIRO ANAISSE
SECRETARIA MUNICIPAL DE SAÚDE – SESMA