
**ASSOCIAÇÃO DOS MUNICÍPIOS DA MICRORREGIÃO DO VALE DO RIO
GRANDE – AMVALE - CNPJ Nº 18.495.218/0001-20.**

PROCEDIMENTO DE SELEÇÃO SIMPLIFICADA Nº 017/2026

TERMO DE REFERÊNCIA

1. DAS CONDIÇÕES GERAIS DA CONTRATAÇÃO

Contratação de empresa especializada, que possua outorga da Agência Nacional de Telecomunicações, para serviços de telefonia fixo comutada (STFC), na modalidade "Software as a Service-SaaS" (Software como serviço) de tráfego ilimitado para ligações locais e nacionais, fixo-fixo e fixo-móvel, incluindo os serviços PABX Virtual, com estrutura em nuvem, baseado em protocolo SIP e tecnologias VoIP (Voz sobre IP), com fornecimento de aparelhos IP, internet por meio de link de internet assimétrica, via fibra óptica com firewall e Anti DDoS, oferta mínima de 1 IPs externos fixos (públicos e válido), Serviço de Wifi seguro com plataforma de gestão e Serviço Móvel Pessoal (SMP) com tecnologia 4G ou superior pelo sistema pós-pago, além da prestação de serviços de implantação das soluções, fornecimento, configuração, manutenção preventiva e corretiva, suporte, sistema de gerenciamento e monitoramento do link de internet dedicado.

2. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

A execução das atividades inerentes à CONTRATANTE exige, invariavelmente, a percepção de serviços de telecomunicações dotados de alta disponibilidade e performance e adequados às pretensões de agregação de serviços tecnológicos aos munícipes e à Associação. Para isso, entende-se que a convergência de uma mesma rede para transmitir e receber dados, voz e imagens otimiza custos de implantação e permite uma gestão mais eficiente pela CONTRATANTE. A solução proporcionará segurança jurídica para a Associação sobre a utilização da internet pelos usuários, pois além das regras para utilização, será possível efetuar auditoria sobre os acessos, identificando o autor de alguma transgressão, se necessário.



3. REQUISITOS DA CONTRATAÇÃO

3.1 DAS ESPECIFICAÇÕES TÉCNICAS:

3.1.1 REQUISITOS GERAIS

3.1.2 Toda a infraestrutura de rede, acesso e CPE da CONTRATADA deverão ser dimensionadas e preparadas para suportar a totalidade do serviço.

3.1.3 A CONTRATADA deverá reservar os canais de comunicação e as portas de acesso à sua infraestrutura para uso exclusivo da CONTRATANTE, não sendo admitido o compartilhamento desses recursos com outro de seus clientes ou usuários

3.1.4 O acesso referido no item anterior deverá ser provido por meio de backbone próprio da prestadora de serviço.

3.1.5 Os equipamentos da CONTRATADA utilizados em toda a solução deverão ser novos e compatíveis com ambientes corporativos.

3.1.6 A CONTRATADA obriga-se e se responsabiliza a prestar o serviço objeto da seleção, por meio de mão de obra especializada e devidamente qualificada, necessária à completa e perfeita execução dos serviços, em conformidade com as especificações do Termo de Referência.

3.1.7 Será de responsabilidade da CONTRATANTE o fornecimento de energia elétrica para alimentação dos equipamentos nas dependências das unidades, o aterramento da rede elétrica e a climatização das dependências.

3.2 CARACTERÍSTICAS DO LINK INTERNET

3.2.1 Fornecer e instalar link de Internet Assimétrica nas velocidades de: 1000 Mbps.

3.2.2 A CONTRATADA deverá disponibilizar 01 endereços IPV4 fixo e válido para provimento da solução de Internet.

3.2.3 Contratação de empresa especializada para o fornecimento de acesso à Rede Mundial de Internet com 100% de garantia de banda downstream e upstream, full-duplex, com conectividade em protocolos IPv4 e IPv6.

3.2.4 Para os links de internet assimétrica de 1000 Mbps

3.2.5 A CONTRATADA deverá atender as seguintes exigências de conexões de Backbone IP para estar apta a prestar os serviços de Internet especificados neste Termo de Referência:

3.2.6 O provedor deve ter o seu backbone IP com saída internacional através de conexão direta para os Estados Unidos da América (EUA) com no mínimo 100 Gbps. Essa saída deve ser composta por uma ou mais conexões "ponto a ponto" entre o backbone IP do provedor do AS remoto, sem backbones intermediários.

3.2.7 O backbone IP do provedor deve ter saída com destino direto para pelo



menos outros 03 provedores de backbone IP Nacionais, com banda não inferior a 200 Gbps.

3.2.8 A conexão entre o CPE da CONTRATADA e o equipamento da CONTRATANTE deverá ser realizada através de interface Gigabit Ethernet 1000BASE-T.

3.2.9 A CONTRATADA poderá utilizar acessos de terceiros como última milha, sendo de inteira responsabilidade da CONTRATADA o cumprimento dos SLAs especificados no edital.

3.2.10 O acesso físico (conexão entre o ponto de presença da CONTRATADA e os equipamentos de comunicação de dados da CONTRATADA instalados nas dependências da CONTRATANTE) deverá ser realizado exclusivamente por meio de fibra óptica, sendo vedada a utilização de qualquer outra tecnologia de acesso.

3.2.10.1 Para os links de internet de 1000 Mbps, poderão ser entregues por meio de Satélite de baixa órbita, radio ou fibra.

3.2.11 O serviço de Internet deverá ser entregue em rede roteada, utilizando protocolos de camada 3, com SLA 99,5% de disponibilidade e MTTR de 4 horas.

3.2.12 Disponibilizar serviço de Domain Name Resolution (DNS) da CONTRATADA, capaz de resolver direta e reversamente endereços de Internet, para registro no servidor DNS primário.

3.2.13 Ser monitorado em regime 24x7 por centro de monitoração da CONTRATADA, sendo responsável pela administração e gerência de equipamentos e links de comunicação de dados, manutenção dos níveis mínimos de serviços exigidos e prevenção e recuperação de falhas de serviço.

3.2.14 Disponibilizar informações sobre os serviços de acesso à Internet por meio de um portal de monitoramento, com acesso restrito, utilizando protocolo seguro (HTTPS), contendo estatísticas de desempenho e de disponibilidade do acesso.

3.2.15 Possibilitar que a equipe técnica da CONTRATANTE realize consultas no portal de monitoramento, bem como visualize relatórios das informações de desempenho dos serviços contratados

3.2.16 A CONTRATADA não poderá:

3.2.16.1 Implementar nenhum tipo de filtro de pacotes que possa incidir sobre o tráfego originado ou destinado à CONTRATANTE, a menos que tenha expressa concordância com esta.

3.2.16.2 Implementar nenhum tipo de cache transparente, a menos que tenha expressa concordância da CONTRATANTE.

3.3 CARACTERÍSTICAS DO ROTEADOR

3.3.1 O roteador a ser instalado no ambiente da CONTRATANTE deverá ter no mínimo as seguintes características técnicas:

3.3.1.1 O equipamento e seus módulos e softwares não deverão constar em

nenhuma lista do fabricante com as situações de "End-of-Sale", "End-of-Order", "End-of-Life" ou "End-of-Support".

3.3.1.2 Deve possuir no mínimo 4 interfaces Gigabit Ethernet padrão 1000BASE-T.

3.3.1.3 Possuir protocolo SNMP habilitado com acesso de leitura.

3.3.1.4 Deve implementar os protocolos de roteamento RIP, OSPFv2, OSPFv3 e BGP-4.

3.3.1.5 Deve possuir suporte nativo ao protocolo IPv6.

3.3.1.6 Deve possuir suporte ao protocolo Netflow v9 ou superior.

3.3.1.7 Deve possuir suporte ao protocolo 802.1q.

3.3.1.8 Deve possuir suporte aos protocolos Telnet e SSHv2.

3.3.1.9 Deve possuir gerenciamento local através de uma porta console, sendo que todos os cabos e adaptadores necessários para o gerenciamento através da porta console deverão ser fornecidos pela CONTRATADA de forma a propiciar o gerenciamento do roteador a partir de uma porta USB.

3.3.1.10 Deverá ser disponibilizado para a CONTRATANTE com o último release de software estável disponibilizado pelo fabricante, capaz de atender a todos os requisitos acima, incluindo o suporte à atualização do referido software durante o período de vigência do contrato.

3.3.1.11 Deve ser montável em rack padrão EIA-310 com largura padrão 19" ocupando no máximo 1U de altura.

3.4 CARACTERÍSTICAS DO SERVIÇO DE BANDA LARGA

3.4.1 Contratação de empresa especializada na prestação continuada de Serviço de Comunicação Multimídia (SCM), na modalidade link compartilhado de internet, para acesso à Internet Banda Larga, nas velocidades necessárias para atendimento da demanda interna da AMVALE, incluindo instalação e manutenção dos serviços pelo período a ser contratado. Os equipamentos devem ser fornecidos, incluindo todos os insumos necessários para o correto funcionamento das conexões, quando for o caso.

3.4.2 A solução escolhida foi Internet Banda Larga por meio de Cabo/Fibra Ótica que oferece maior velocidade de conexão e é amplamente utilizada pelas empresas de Telecomunicações.

3.4.3 A contratada deverá disponibilizar os acessos à Internet Banda Larga, com todos os materiais, insumos e equipamentos necessários à efetiva prestação dos serviços nos endereços e bandas de comunicação deste mesmo documento;

3.4.4 Fornecer e instalar link de Internet Banda Larga, na modalidade link compartilhado de internet, na velocidade contratada para uso nas unidades do TRE-PR;



- 3.4.5** Instalar a conectividade IP (Internet Protocol) – que suporte aplicações TCP/IP – a uma velocidade de transmissão de, no mínimo, especificada para cada item com a Rede Internet nas dependências da CONTRATANTE;
- 3.4.6** A CONTRATADA deverá se encarregar de prover o serviço observando os locais de instalação, meio físico e taxa de transmissão para cada unidade, conforme indicado pela CONTRATANTE.
- 3.4.7** O modem/roteador e demais equipamentos devem ser instalados no rack de comunicação já disponível nos endereços da CONTRATANTE;
- 3.4.8** A CONTRATADA deverá disponibilizar toda a infraestrutura de telecomunicações (equipamentos e insumos) necessária ao pleno funcionamento dos serviços contratados, sem custo adicional ao CONTRATANTE;
- 3.4.9** Para velocidades superiores a 100MB, a CONTRATADA deverá disponibilizar modem/roteador com interface LAN, Gigabit Ethernet 100/1000, com no mínimo um conector RJ-45 para interconexão aos equipamentos da CONTRATANTE;
- 3.4.10** A CONTRATADA deverá fornecer as informações de login/senha para que a CONTRATANTE possa configurar a rede wi-fi e rede LAN do roteador/modem.
- 3.4.11** Após a implantação não deve haver nenhuma rede sem fio (wifi) publicada nos equipamentos instalados, somente a conexão via cabo deve estar disponível, eventual publicação de rede sem fios será efetuada pela equipe técnica do TRE-PR;
- 3.4.12** A conexão da porta LAN do roteador/modem com a rede interna será executada pela CONTRATANTE.
- 3.4.13** Mudanças de endereço deverão ser realizadas sempre que solicitado mediante viabilidade técnica. Neste caso será devido o pagamento de novo instalação, de acordo com o valor de instalação apurado no presente processo;
- 3.4.14** Garantia de banda com média mensal mínima de 80% da velocidade contratada;
- 3.4.15** Taxa mínima de upload de 50% (cinquenta por cento) do download contratado.
- 3.4.16** Não deverá haver limite de tráfego (filtros) no circuito contratado, todos os protocolos e portas devem estar disponíveis para utilização.
- 3.4.17** Disponibilidade mínima mensal do serviço de 95%, considerando-se 24 (vinte e quatro) horas por dia, nos 7 (sete) dias da semana;
- 3.4.18** Tempo de reparo no local em até 24 (vinte e quatro) horas corridas contadas a partir do registro do chamado de indisponibilidade na CONTRATADA.
- 3.4.19** Latência máxima de 50 (cinquenta) ms (milissegundos) e perda de pacotes máxima de 5% (cinco por cento);
- 3.4.20** Cumprir as obrigações impostas pelas Resoluções ANATEL nº 632/2014 (Regulamento Geral de Direitos do Consumidor de Serviços de

Telecomunicações), nº 426/2005 (Regulamento do STFC) e/ou nº 477/2007 (Regulamento do SMP), no que cabível;

3.4.21 Os serviços a serem contratados são de natureza contínua, com duração inicial de 30 (trinta) meses, prorrogável até o limite máximo da legislação vigente, e não envolvem dedicação exclusiva de mão de obra.

3.4.22 Declaração do licitante de que tem pleno conhecimento das condições necessárias para a prestação do serviço.

3.5 CARACTERÍSTICAS DO SDWAN

3.5.1 Fornecer Entende-se como tecnologia SD-WAN (Software-Defined WAN):

3.5.1.1 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;

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

3.5.1.3 A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo;

3.5.1.4 Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;

3.5.1.5 A solução deve permitir a definição do roteamento para cada aplicação;

3.5.1.6 Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;

3.5.1.7 Deve possibilitar a definição do link de saída para uma aplicação específica;

3.5.1.8 Deve implementar balanceamento de link por hash do IP de origem;

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

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

3.5.1.11 Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

3.5.1.12 A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding;



- 3.5.1.13 Deve suportar roteamento estático e dinâmico (OSPF, BGP);
- 3.5.1.14 Deve possibilitar a agregação de túneis IPsec;;
- 3.5.1.15 Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões;
- 3.5.1.16 Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;
- 3.5.1.17 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve contemplar:
- 3.5.1.18 Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:
 - 3.5.1.18.1 por endereço de origem;
 - 3.5.1.18.2 por endereço de destino;
 - 3.5.1.18.3 por usuário e grupo;
 - 3.5.1.18.4 por aplicações;
 - 3.5.1.18.5 por porta;
- 3.5.1.19 O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
- 3.5.1.20 O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc;
- 3.5.1.21 Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;
- 3.5.1.22 O QoS deve possibilitar a definição de fila de prioridade;
- 3.5.1.23 Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;
- 3.5.1.24 Deve ter a capacidade de agendar intervalos de tempo onde as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço;
- 3.5.1.25 Uma vez que o tráfego é identificado, as políticas de shaping/QoS podem ser compartilhadas a todos os acessos que fizerem match na regra ou por IP. Ex: 10 Mbps de banda garantida por IP ou para todos os IPs que fizerem match na regra;
- 3.5.1.26 Deve possibilitar a definição de bandas distintas para download e upload;



- 3.5.1.27 A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);
- 3.5.1.28 A solução de SD-WAN deve suportar IPv6;
- 3.5.1.29 Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;
- 3.5.1.30 Deve ser capaz de bloquear acesso à aplicações;
- 3.5.1.31 Deve suportar NAT dinâmico bem como NAT de saída;
- 3.5.1.32 Deve suportar balanceamento de tráfego por sessão e pacote;
- 3.5.1.33 As funcionalidades de SD-WAN devem ser fornecidas no NGFW;
- 3.5.1.34 Deve implementar balanceamento de link por custo configurado do link;
- 3.5.1.35 Deve suportar o balanceamento de, no mínimo, 5 links;
- 3.5.1.36 Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec;
- 3.5.1.37 Deve suportar o balanceamento de links LTE (4G) sem restrições de uso, podendo ser usado em conjunto com outros links e não ser somente o backup para todos os outros links;
- 3.5.1.38 Deve gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde;
- 3.5.1.39 Deve suportar Zero-Touch Provisioning;
- 3.5.1.40 Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes;
- 3.5.1.41 Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Estes valores serão utilizados pela solução para decidir qual link será utilizado;
- 3.5.1.42 A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links;
- 3.5.1.43 A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS;
- 3.5.1.44 As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e Protocolo;
- 3.5.1.45 Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD- WAN;
- 3.5.1.46 Deve suportar envio de BGP route-map para BGP neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link;
- 3.5.1.47 Deve ser possível utilizar o balanceamento round Robin na agregação de duas ou mais IPSEC VPNs determinando o peso para cada VPN;



- 3.5.1.48 Deve ser possível especificar o número mínimo de interfaces ativas em uma regra de SD-WAN para que esta regra seja válida;
- 3.5.1.49 A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;
- 3.5.1.50 Deve dispor de opção que maximize o uso da largura de banda utilizando os links WANs que estejam dentro do nível de saúde estipulado;
- 3.5.1.51 Deve possuir capacidade de classificação de tráfego com probes de SLA, garantindo dessa forma a priorização do tráfego em momentos de congestionamento, evitando oscilações do link SD-WAN;
- 3.5.1.52 A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW) e SD- WAN, não sendo permitido appliances virtuais ou solução open source (produto montado);
- 3.5.1.53 Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- 3.5.1.54 Por funcionalidades de SD-WAN entende-se: roteamento inteligente, uso do melhor link por aplicação, abstração do tráfego em relação aos circuitos físicos e controle do tráfego por aplicação;
- 3.5.1.55 As funcionalidades de segurança e SD-WAN que compõem a solução podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação, acompanhem os mesmos termos de garantia, atualizações e manutenção, suporte e gerenciamento centralizado;
- 3.5.1.56 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- 3.5.1.57 Todos os equipamentos fornecidos não devem ultrapassar a medida máxima de 2U cada;
- 3.5.1.58 O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- 3.5.1.59 Os dispositivos de proteção de rede devem possuir suporte a VLANs;
- 3.5.1.60 Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM);
- 3.5.1.61 Deve suportar BGPv4/BGP4+, OSPFv2/v3, RIP e roteamento estático;
- 3.5.1.62 Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
- 3.5.1.63 Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;



- 3.5.1.64 Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet lógicas;
- 3.5.1.65 Deve suportar NAT dinâmico (Many-to-Many);
- 3.5.1.66 Deve suportar NAT estático (1-to-1);
- 3.5.1.67 Deve suportar NAT estático bidirecional 1-to-1;
- 3.5.1.68 Deve suportar Tradução de porta (PAT);
- 3.5.1.69 Deve suportar NAT de Origem;
- 3.5.1.70 Deve suportar NAT de Destino;
- 3.5.1.71 Deve suportar NAT de Origem e NAT de Destino simultaneamente;
- 3.5.1.72 Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- 3.5.1.73 Deve suportar NAT46, NAT64;
- 3.5.1.74 Deve implementar o protocolo ECMP;
- 3.5.1.75 Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
- 3.5.1.76 Enviar log para sistemas de monitoração externos;
- 3.5.1.77 Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
- 3.5.1.78 Proteção anti-spoofing;
- 3.5.1.79 Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 3.5.1.80 Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
- 3.5.1.81 Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego.
- 3.5.1.82 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
- 3.5.1.83 A configuração em alta disponibilidade deve sincronizar:
- 3.5.1.84 Sessões;
- 3.5.1.85 Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QoS e objetos de rede;
- 3.5.1.85.1 Associações de Segurança das VPNs;
- 3.5.1.85.2 Tabelas FIB;
- 3.5.1.86 O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
- 3.5.1.87 Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;
- 3.5.1.88 Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;



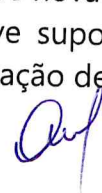
- 3.5.1.89 Controle, inspeção e descriptografia de SSL para tráfego de Saída (Outbound);
- 3.5.1.90 O equipamento deve possuir suporte a 256 VLAN Tags 802.1Q;
- 3.5.1.91 O equipamento deve possuir suporte a agregação de links 802.3ad LACP;
- 3.5.1.92 POLÍTICAS
 - 3.5.1.92.1 Deverá suportar controles por zonas de segurança;
 - 3.5.1.92.2 Deverá suportar controles de políticas por porta e protocolo;
 - 3.5.1.92.3 Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
 - 3.5.1.92.4 Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
 - 3.5.1.92.5 Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
 - 3.5.1.92.6 Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);
 - 3.5.1.92.7 Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
 - 3.5.1.92.8 Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
 - 3.5.1.92.9 Suporte a objetos e regras IPv6;
 - 3.5.1.92.10 Suporte a objetos e regras multicast;
 - 3.5.1.92.11 Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
 - 3.5.1.92.12 Deverá ter a capacidade de permitir a criação de regras de segurança específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows podendo tomar ações como: colocar o dispositivo em VLAN de quarentena, aplicar bloqueios e filtros na interface do firewall.
- 3.5.1.93 APLICAÇÕES
 - 3.5.1.93.1 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
 - 3.5.1.93.2 Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
 - 3.5.1.93.3 Reconhecer pelo menos 2300 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

- 3.5.1.93.4 Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google- docs;
- 3.5.1.93.5 Deve inspecionar o payload do pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
- 3.5.1.93.6 Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
- 3.5.1.93.7 Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 3.5.1.93.8 Deve suportar a descriptografia do tráfego SSL (IPv4 e IPv6) e espelhar este tráfego para uma interface específica;
- 3.5.1.93.9 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;
- 3.5.1.93.10 Identificar o uso de táticas evasivas via comunicações criptografadas;
- 3.5.1.93.11 Atualizar a base de assinaturas de aplicações automaticamente;
- 3.5.1.93.12 Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
- 3.5.1.93.13 Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 3.5.1.93.14 Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
- 3.5.1.93.15 Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
- 3.5.1.93.16 Deve permitir exceções de aplicações caso uma regra de controle de aplicação seja configurada para permitir ou bloquear uma categoria de aplicação;



- 3.5.1.93.17 O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 3.5.1.93.18 Deve alertar o usuário quando uma aplicação for bloqueada;
- 3.5.1.93.19 Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc.) possuindo granularidade de controle/políticas para os mesmos;
- 3.5.1.93.20 Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos;
- 3.5.1.93.21 Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
- 3.5.1.93.22 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc.);
- 3.5.1.93.23 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação e categoria da aplicação;
- 3.5.1.93.24 Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
- 3.5.1.94 PREVENÇÃO E AMEAÇAS
- 3.5.1.94.1 Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
- 3.5.1.94.2 Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 3.5.1.94.3 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
- 3.5.1.94.4 Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;
- 3.5.1.94.5 As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
- 3.5.1.94.6 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 3.5.1.94.7 Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
- 3.5.1.94.8 Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 3.5.1.94.9 Deve permitir o bloqueio de vulnerabilidades;

- 3.5.1.94.10 Deve permitir o bloqueio de exploits conhecidos;
- 3.5.1.94.11 Deve incluir proteção contra ataques de negação de serviços;
- 3.5.1.94.12 Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
- 3.5.1.94.13 Detectar e bloquear a origem de portscans;
- 3.5.1.94.14 Bloquear ataques efetuados por worms conhecidos;
- 3.5.1.94.15 Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
- 3.5.1.94.16 Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 3.5.1.94.17 Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- 3.5.1.94.18 Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
- 3.5.1.94.19 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB/CIFS, SMTP, IMAP e POP3;
- 3.5.1.94.20 Identificar e bloquear comunicação com botnets;
- 3.5.1.94.21 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 3.5.1.94.22 Os eventos devem identificar o país de onde partiu a ameaça;
- 3.5.1.94.23 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e Worms;
- 3.5.1.94.24 Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
- 3.5.1.94.25 Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
- 3.5.1.94.26 Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;
- 3.5.1.94.27 A solução de sandbox deve ser capaz de criar assinaturas e ainda incluí-las na base de antivírus do firewall, prevenindo a reincidência do ataque;
- 3.5.1.94.28 A solução de sandbox deve ser capaz de incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas (Blocklist), impedindo que esses endereços sejam acessados pelos usuários de rede novamente;
- 3.5.1.94.29 Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;



- 3.5.1.94.30 A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado;
- 3.5.1.95 FILTRO DE URL
- 3.5.1.95.1 Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 3.5.1.95.2 Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
- 3.5.1.95.3 Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
- 3.5.1.95.4 A identificação pela base do Active Directory deve permitir SSO, de forma que o usuários não precise logar novamente na rede para navegar pelo firewall;
- 3.5.1.95.5 Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 3.5.1.95.6 Possuir pelo menos 60 categorias de URLs;
- 3.5.1.95.7 Deve possuir a função de exclusão de URLs do bloqueio;
- 3.5.1.95.8 Permitir a customização de página de bloqueio;
- 3.5.1.96 IDENTIFICAÇÃO DO USUÁRIO
- 3.5.1.96.1 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
- 3.5.1.96.2 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 3.5.1.96.3 Deve possuir integração e suporte a Microsoft Active Directory para no mínimo o sistema operacional Windows Server 2012 R2;
- 3.5.1.96.4 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;
- 3.5.1.96.5 Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 3.5.1.96.6 Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 3.5.1.96.7 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a

navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

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

3.5.1.96.9 Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

3.5.1.97 FILTRO DE DADOS E GEOLOCALIZAÇÃO

3.5.1.97.1 Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP);

3.5.1.97.2 Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

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

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

3.5.1.98 VPN

3.5.1.98.1 Suportar VPN Site-to-Site e Cliente-To-Site;

3.5.1.98.2 Suportar IPSec VPN;

3.5.1.98.3 Suportar SSL VPN;

3.5.1.98.4 A VPN IPSEC deve suportar criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard);

3.5.1.98.5 A VPN IPSEC deve suportar Autenticação MD5, SHA1, SHA256, SHA384 e SHA512;

3.5.1.98.6 A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Group 15 até 21;

3.5.1.98.7 A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

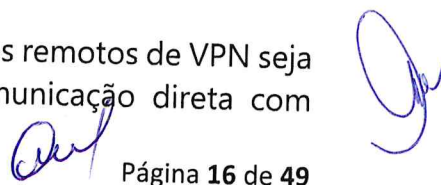
3.5.1.98.8 A VPN IPSEC deve suportar Autenticação via certificado IKE PKI;

3.5.1.98.9 Deve possuir interoperabilidade com no mínimo os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

3.5.1.98.10 A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

3.5.1.98.11 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

3.5.1.98.12 Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com



dispositivos locais como proxies;

3.5.1.98.13 Atribuição de DNS nos clientes remotos de VPN;

3.5.1.98.14 Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

3.5.1.98.15 Suportar autenticação via AD/LDAP, certificado e base de usuários local;

3.5.1.98.16 Suportar leitura e verificação de CRL (certificate revocation list);

3.5.1.98.17 Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

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

3.5.1.98.19 O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8/8.1 (32 e 64 bit), Windows 10 (32 e 64 bit);

3.5.2 ESPECIFICAÇÕES TÉCNICAS MÍNIMAS NECESSÁRIAS DO EQUIPAMENTO FIREWALL

3.5.2.1 Throughput de, no mínimo, 14 Mpps de Firewall (pacote por segundo);

3.5.2.2 Suporte a, no mínimo, 1.4 milhões de conexões simultâneas (TPC);

3.5.2.3 Suporte a, no mínimo, 54 mil novas conexões por segundo (TPC);

3.5.2.4 Throughput de no mínimo 10,8 Gbps de VPN IPSec, com pacotes de no mínimo 512 bytes;

3.5.2.5 Estar licenciado para, ou suportar sem o uso de licença, 1.900 túneis de VPN IPSEC Site- to-Site simultâneos;

3.5.2.6 Estar licenciado para, ou suportar sem o uso de licença, 14.500 túneis de clientes VPN IPSEC simultâneos;

3.5.2.7 Suportar no mínimo 2.4 Gbps de throughput de IPS;

3.5.2.8 Suporte a, no mínimo, 2 Gbps de throughput de controle de aplicação;

3.5.2.9 Suportar no mínimo 1 Gbps de throughput de Inspeção SSL;

3.5.2.10 Throughput de, no mínimo, 900 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware;

3.5.2.11 Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;

3.5.2.12 Possuir ao menos 4 interfaces RJ45;

3.5.2.13 Deve incluir porta USB compatível com modem 3G/4G, permitindo ainda que este link WAN seja utilizado nas regras de SD- WAN;

3.5.2.14 Possuir fonte de alimentação com fonte DC de 100–240V AC, 50–60hz;



3.5.2.15 Em caso de uma atualização do sistema que acrescentem novas funcionalidades elas devem funcionar sem a necessidade de aquisição de nova licença;

3.5.2.16 Caso o fabricante remova o produto de linha, o mesmo deve substituir o produto entregue pela nova geração com capacidade e funcionalidades igual ou superior ao removido da linha de produção;

3.5.2.17 Deve possuir garantia de hardware e software durante a vigência do contrato;

3.5.2.18 Deve possuir licenciamento perpetuado para as funcionalidades;

3.5.2.19 As funcionalidades a seguir devem seguir funcionando, mesmo após o vencimento do contrato de suporte e licenciamento: SD-WAN, controle de aplicação e stateful firewall;

3.5.2.20 Deve possuir licenciamento durante a vigência do contrato para as subscrições de filtro de conteúdo, Antivírus, Controle de aplicação, IPS e outras que façam parte do produto e da oferta;

3.6 CARACTERÍSTICAS DA SOLUÇÃO DE PABX EM NUVEM

3.6.1 A solução de PABX Virtual deverá ser:

3.6.1.1 Em nuvem (Cloud) e baseada em protocolo SIP (Session Initiation Protocol), conforme RFC 3261, incluindo serviço de telefonia avançada STFC (Serviço Telefônico Fixo Comutado).

3.6.1.2 Todos os elementos da Solução como Gateways, roteadores, adaptadores ATA, telefones IP, softphone, servidores devem interoperar utilizando apenas SIP, conforme RFC 3261.

3.6.1.3 Será admitido o uso de funcionalidades extras do fabricante encapsuladas no protocolo SIP;

3.6.1.4 Não serão aceitas soluções que necessitem de conversão de protocolos SIP ou que utilizem exclusivamente protocolos proprietários para conexão e funcionamento entre os ramais IP/SIP e a Solução PABX Virtual em Nuvem;

3.6.1.5 Será admitido que equipamentos (gateways, roteadores etc.) sejam utilizados para conversão de protocolos SIP com outras tecnologias de entroncamento com a PSTN;

3.6.1.6 Será admitido que equipamentos (gateways, roteadores etc.) sejam gerenciados de forma centralizada via protocolo padrão H.248, especificamente para esta função de gerenciamento, desde que mantenha toda a comunicação baseada no protocolo SIP, conforme RFC 3261.

3.6.1.7 A solução deve seguir o plano geral de metas da ANATEL e possuir números válidos na rede nacional de telefonia do tipo discagem direta a ramal (DDR).

3.6.1.8 Todos os Ramais deverão poder ser vinculados a um número público



- (DDR) ou apenas ramal com numeração interna (não DDR).
- 3.6.1.9 Solução deve permitir o encaminhamento de chamadas, programada por número telefônica em caso de falha na rede para qualquer outro destino telefônico como por exemplo um outro número fixo ou um número celular.
- 3.6.1.10 Deverá suportar roteamento das chamadas oriundas da rede pública de telefonia (PSTN), de outros sistemas internos interligados via IP, ou de dispositivos SIP integrados à Solução;
- 3.6.1.11 Todo e qualquer tipo de tráfego de carga útil envolvendo a solução deve ocorrer em modo ponto a ponto, ou ponto-multiponto, ou multiponto-multiponto.
- 3.6.1.12 Exceção desta regra com relação às comunicações gravadas, que não necessariamente precisam seguir esse padrão.
- 3.6.1.13 A infraestrutura de rede local (switches, cabeamento estruturado, etc.), links de acesso à Internet para todas as unidades serão oferecidos pela CONTRATANTE.
- 3.6.1.14 Preferencialmente, as ligações entre ramais IP devem considerar o uso da rede de dados do TRT existente e rotas de menor custo.
- 3.6.1.15 Deve garantir o funcionamento da Solução com as principais marcas e modelos de Telefones IP/SIP e Adaptadores para Telefones Analógicos (ATA) de mercado, sejam de fabricação nacional ou estrangeira, que utilizem o protocolo SIP padrão definido pela RFC 3261 e obedeçam aos requisitos de segurança especificados neste Termo de Referência;
- 3.6.1.16 Deve ser responsável pelo controle de sessões, facilidades de telefonia, funções de roteamento, seleção e busca de gateways, tradução de endereços e bilhetagem de todas as chamadas;
- 3.6.1.17 Deve suportar integrações com serviços de rede DNS e NTP (NTP ou SNTP);
- 3.6.1.18 Deve suportar crescimento ilimitado usuários/ramais licenciados, sem necessidade de instalação de novos equipamentos, componentes ou sistemas, bastando para este aumento a aquisição e ativação das licenças de usuários/ramais adicionais.
- 3.6.1.19 Esta capacidade deve ser suportada independentemente de os usuários estarem na rede interna ou acessando de fora da rede, através de um SBC;
- 3.6.1.20 A solução deve ser independente dos dispositivos de rede, ou seja, deve garantir as mesmas funcionalidades, independente do fabricante dos ativos de rede que o TRT já possui, resguardadas as questões relacionadas ao oferecimento de recursos mínimos de infraestrutura de QoS, banda, jitter, delay e perda de pacotes;
- 3.6.1.21 Deve possuir recursos de classificação e marcação de pacotes, de



forma que seja possível realizar a priorização do tráfego de voz através da aplicação dos principais mecanismos de QoS (Quality of Service) com base em endereços de IP de origem/destino, portas TCP (Transmission Control Protocol)/UDP (User Datagram Protocol) de origem e destino ou seguindo os padrões recomendados de ToS (Type of Service), DSCP (Differentiated Services Code Point) e campo CoS (Class of Service) do frame ethernet;

3.6.1.22 Todo o provisionamento dos telefones IP deverá ser feito de forma automatizada na mesma solução, de tal forma que não seja necessário digitar as credenciais de autenticação do SIP nos telefones e nem nos portais de administração dos telefones IP;

3.6.1.23 Deve permitir a interoperabilidade e a comutação tradicional com a Rede de Telefonia Pública Computada (RTPC).

3.6.1.24 A interconexão com a RTPC deverá obedecer aos padrões de sinalização de troncos digitais vigentes no Brasil (Integrated Services Digital Network – ISDN e R2 Digital – R2D) ou acesso via SIP Trunk;

3.6.1.25 Todo o tráfego de voz deve ser prioritariamente através do protocolo G.729 (qualquer das variações G.729, G.729A, G.729B ou G.729AB) e o fall back para G.711.

3.6.1.26 Serviços básicos de centrais telefônicas exigidos:

3.6.1.26.1 Disponibilizar portal web para administração dos serviços com pelo menos 2 níveis de administração: Nível Administrador da Empresa e nível Ramal;

3.6.1.26.2 Até 5 Dispositivos por usuários: permite que o ramal possa ser vinculado a vários tipos de dispositivos, sejam aparelhos IP, softphone mobile ou softphone para desktop

3.6.1.26.3 Discagem por ramal para chamadas internas inclusive entre as localidades do mesmo DDD;

3.6.1.26.4 Desvio de chamadas - deve ser suportado os desvios incondicionais, por ocupado, por não atendimento e indisponível, com suporte para ativação/desativação remota de desvios;

3.6.1.26.5 Chamada em espera – permitir em Espera ou Recuperar Automaticamente uma Chamadas;

3.6.1.26.6 Música para chamadas em retenção e em espera, devendo ser permitido o upload das músicas pelo portal de administração;

3.6.1.26.7 Conferência de voz, com no mínimo 15 usuários.

3.6.1.26.8 Cadeado eletrônico – Solicita código para fazer chamadas;

3.6.1.26.9 Não perturbe – deve permitir o bloqueio de chamadas recebidas internas, externas e a cobrar por terminal;

3.6.1.26.10 Bloqueio de chamadas originadas LDN (longa distância nacional), LDI (longa distância internacional), de chamadas para celular e de Chamadas para 0300, 0500 e 0900 por terminal;



- 3.6.1.26.11 Transferência de chamadas - Permitir o envio de uma chamada para outra linha;
- 3.6.1.26.12 Captura direta;
- 3.6.1.26.13 Retorno automático de chamada;
- 3.6.1.26.14 Discagem rápida discando as teclas de 0 a 9;
- 3.6.1.26.15 Toque simultâneo/paralelo, com possibilidade de ativação remota do toque paralelo para busca do usuário;
- 3.6.1.26.16 Identificação do número chamador (BINA);
- 3.6.1.26.17 Identificação do número conectado;
- 3.6.1.26.18 Restrição de identificação do número de origem (Número de A);
- 3.6.1.26.19 Estacionamento de chamadas (call park);
- 3.6.1.26.20 Grupo de captura;
- 3.6.1.26.21 Agenda centralizada pessoal;
- 3.6.1.26.22 Correio de Voz;
- 3.6.1.27 Facilidades de grupo:
 - 3.6.1.27.1 As facilidades de Grupo devem prover um número virtual a ser escolhido na faixa de ramais de um site para associar via portal de administração do serviço os ramais associados as facilidades e que compartilham do recurso;
 - 3.6.1.27.2 O Número Virtual deve suportar que um número 0800 seja comutado a ele, ou seja deve ser um número válido na rede nacional de telefonia.
- 3.6.1.28 Facilidade de Grupo de Busca:
 - 3.6.1.28.1 Os Grupos devem ser montados associando usuários/ terminais que fazem parte de um mesmo Código Nacional (DDD) a um número virtual.
 - 3.6.1.28.2 Deve permitir que usuários dentro de uma área definida pelo Código Nacional (Nível de Grupo), sejam inseridos em subgrupos capazes de tratar chamadas destinadas a este grupo. Os métodos possíveis devem ser:
 - 3.6.1.28.3 Circular – Envia as chamadas para os usuários/terminais inseridos no grupo de forma linear, enviando a chamada para a primeira pessoa disponível no grupo, começando com o próximo número depois de onde a última chamada foi enviada.
 - 3.6.1.28.4 Regular - Envia as chamadas para os usuários/ terminais inseridos no grupo iniciando sempre pelo primeiro usuário/ terminal definido pelo Administrador do Serviço.
 - 3.6.1.28.5 Simultâneo – Toca em todos os usuários/ terminais inseridos no grupo, o primeiro usuário/ terminal a atender a chamada é conectado.
 - 3.6.1.28.6 Uniforme - Quando uma chamada é concluída, o usuário move-se para a parte inferior da fila de chamadas de uma forma aleatória. A próxima chamada recebida vai para o usuário que esteve inativo por mais tempo. Se um usuário recebe uma chamada que não foi direcionada a ele através do grupo de busca, esta não é contabilizada para o recebimento de chamadas uniformes.



3.6.1.28.7 Ponderada – Envia as chamadas para os usuários/terminais que estejam disponíveis e que possuam maior peso para atendimento ao tipo de chamada e questão.

3.6.2 DATACENTER

3.6.2.1 A solução de PABX em nuvem deverá ser hospedada em datacenters que possuam no mínimo as certificações ISO 27001, ISO 27017, ISO 27018, SOC1, SOC2, SOC3, PCI DSS, CSA STAR E HITRUST CSF. Será aceito certificação TIER III em substituição às certificações exigidas.

3.6.2.2 O tráfego de voz entre ramais e de / para o serviço telefônico fixo comutado (STFC) deverá exclusivamente ser processado e transitado em datacenters situados em território brasileiro. Todos os Session Corder Controlers (SBC) de voz deverão estar obrigatoriamente hospedados em datacenters situados em território brasileiro.

3.6.2.3 A solução PABX e nuvem deve possuir redundância geográfica de datacenters, de modo a não haver ponto único de falha e garantir a disponibilidade.

3.6.2.4 Deverá ser apresentado junto com a proposta a comprovação que o datacenter possui as certificações exigidas, bem como informados os respectivos endereços dos mesmos no Brasil.

3.6.3 STFC

3.6.3.1 A LICITANTE deverá possuir licença de STFC (Serviço de Telefonia Fixa Comutada) junto a ANATEL (Agência Nacional de Telecomunicações) para a prestação dos serviços. Deverá ser anexada à proposta.

3.6.3.2 Para ligações entre ramais não deverá existir limite quanto à quantidade simultânea.

3.6.3.3 Para ligações externas, de / para STFC, deverá ser disponibilizado um quantitativo de canais (ligações simultâneas) igual ou superior a 30% da quantidade total de ramais.

3.6.3.4 Todos os ramais deverão ser fornecidos com número DDR (Discagem Direta a Ramal).

3.6.3.5 Caso seja opção da CONTRATANTE, a CONTRATADA deverá efetuar a portabilidade dos números atualmente utilizados, sem ônus adicionais.

3.6.3.6 Para as localidades onde não seja possível realizar a portabilidade dos números atuais, nem o fornecimento de novos números fixos pertencentes à mesma área local, a CONTRATADA poderá oferecer outras alternativas para o direcionamento das ligações, tais como Número Único Nacional 0800 ou tronco SIP com número móvel.

3.6.3.7 O serviço telefônico nas modalidades Local e Longa Distância,



compreendem a realização de chamadas locais para telefones e para telefones moveis por meio de Troncos, bem como recepção de chamadas diretamente nos ramais.

3.6.3.8 Serviço Telefônico FIXO – FIXO (LOCAL), na modalidade Local, assim entendidas as ligações oriundas da Área Local em que está compreendida as unidades da Prefeitura Municipal de Ibitité, para telefones fixo nesta mesma área.

3.6.3.9 Serviço Telefônico FIXO – Móvel (LOCAL), na modalidade Local, assim entendidas as ligações oriundas da Área Local em que está compreendida as unidades da Prefeitura Municipal de Ibitité, para telefones móveis nesta mesma área.

3.6.3.10 Serviço Telefônico FIXO – FIXO (Longa Distância), na modalidade Longa Distância Nacional compreendido por todo território nacional. Abrange as ligações originadas em telefones fixo e destinadas a telefones fixos compreendidas por códigos nacionais (DDD).

3.6.3.11 Serviço Telefônico FIXO – Móvel (Longa Distância), na modalidade Longa Distância Nacional compreendido por todo território nacional. Abrange as ligações originadas em telefones fixo e destinadas a telefones moveis compreendidas por códigos nacionais (DDD).

3.6.4 A contratada deverá possuir CSP próprio para realização das chamadas de Longa Distância Nacional, comprovada via:

3.6.4.1 <https://sistemas.anatel.gov.br/stel/Consultas/STFC/PrestadorasCSP/tela.asp>.

3.6.5 Não será permitido a subcontratação do tráfego STFC, sendo obrigatório que os números DDR disponibilizados sejam da própria CONTRATADA junto à ABR Telecom, bem como deverá ser apresentado pelo menos 01 (um) contrato de interconexão com outras operadoras que compreenda a área local a ser atendida.

3.6.6 Os números a serem portados deverão manter a titularidade em nome da CONTRATANTE, não sendo permitida a transferência de titularidade dos mesmos.

3.6.7 As ligações de âmbito internacional (DDI) que porventura ocorrerem deverão ser cobradas conforme tarifário da licitante vencedora, atendendo legislação específica.

3.6.8 CARACTERÍSTICAS GERAIS DA PLATAFORMA

3.6.8.1 Cada Todo o gerenciamento e operação do sistema deverá ser disponibilizado através de interface Web, sem a necessidade de instalação de aplicativos ou clientes locais.

3.6.8.2 A ferramenta de gerenciamento deverá permitir a configuração de perfis de usuários, no mínimo 03 (três), definindo níveis de acesso a cada perfil.



- 3.6.8.3 Deverá possuir painéis para acompanhamento em tempo real (dashboard), que apresentem pelo menos as seguintes informações:
- 3.6.8.3.1 Disponibilidade da solução, apresentando para um período pré-determinado, o tempo de indisponibilidade da plataforma.
 - 3.6.8.3.2 Disponibilidade de cada ramal telefônico, com indicação de status/cor: disponível/verde, ocupado/vermelho, indisponível/cinza.
 - 3.6.8.3.3 Deverá permitir a visualização de todos os ramaís telefônicos da solução, com identificação do seu número, setor, local e data de instalação.
 - 3.6.8.3.4 Visualização de todas as chamadas em curso, por perfil de tráfego (ramal-ramal, local, móvel, LDN).
 - 3.6.8.3.5 Visualização do consumo de minutagem, por perfil de tráfego (ramal-ramal, local, móvel, LDN).
 - 3.6.8.3.6 Visualização da lista telefônica pública e privada.
- 3.6.8.4 Deverá permitir a emissão de relatórios que apresentem as seguintes informações:
- 3.6.8.4.1 Disponibilidade da solução.
 - 3.6.8.4.2 Disponibilidade de cada ramal.
 - 3.6.8.4.3 Ramaís telefônicos da solução, com identificação do seu número, setor, local e data de instalação.
 - 3.6.8.4.4 Quantidade de chamadas realizadas e recebidas, atendidas, não atendidas, ocupadas, com falhas, congestionadas, por ramal e global e por data.
 - 3.6.8.4.5 Quantidade de chamadas realizada, por ramal, por perfil de tráfego (ramal-ramal, local, móvel, LDN), por consumo de minutagem e por data.
- 3.6.8.5 Tráfego de dados, identificando a hora de cada dia com maior número de chamadas.
- 3.6.8.6 Evolução do consumo de minutagem, por perfil de tráfego, mês a mês, no mínimo dos últimos 06 (seis) meses.
- 3.6.8.7 Não serão aceitas soluções ou sistemas baseados ou derivados da solução de código aberto, como Asterisk e/ou Freeswitch.
- 3.6.8.8 A solução deverá seguir diretrizes de boas práticas de segurança de sistemas, conforme ISO 27024.
- 3.6.8.9 Todos os aparelhos telefônicos deverão ser novos, de primeiro uso e acompanhados dos manuais, não serão aceitos equipamentos reformados ou reconicionados.
- 3.6.8.10 A infraestrutura de rede local (switches, cabeamento estruturado etc). e acesso das unidades à Internet serão disponibilizados pela CONTRATANTE.
- 3.6.8.11 Todos os ramaís deverão permitir as seguintes funcionalidades básicas:
- 3.6.8.11.1 Suportar que um mesmo número de ramal (número único de ramal) seja usado em qualquer dispositivo do usuário (terminal IP ou softphone) com



correio de voz.

3.6.8.11.2 Discagem por ramal para chamadas internas inclusive entre as localidades.

3.6.8.11.3 Desvio incondicional de chamadas. (permite encaminhar todas as chamadas recebidas para outro número de telefone, como um telefone residencial ou celular).

3.6.8.11.4 Desvio de chamada em caso de ocupado. (permite encaminhar todas as chamadas recebidas para outro número de telefone, se o telefone estiver ocupado).

3.6.8.11.5 Desvio de chamada por não atendimento. (permite encaminhar todas as chamadas recebidas para outro número de telefone, quando não atender o telefone).

3.6.8.11.6 Desvio de chamada quando indisponível. (permite encaminhar todas as chamadas recebidas para outro número de telefone, quando seu terminal estiver indisponível).

3.6.8.11.7 Possibilidade de criação de grupos de atendimento.

3.6.8.11.8 Transferência de chamadas. (O serviço de transferência de chamadas permite que o usuário transfira uma chamada para um destino especificado. As transferências de chamadas podem ser cegas, com consulta de terceiros ou com consulta de três vias).

3.6.8.11.9 Identificação do número chamador (BINA). (A entrega de ID da linha de chamada retransmite a identidade de um chamador para o dispositivo do usuário, se o dispositivo for capaz de exibir essas informações).

3.6.8.11.10 Rediscagem de chamadas perdidas e da última efetuada.

3.6.8.11.11 Restrição de identificação do número de origem (Número de A). (permite impedir que seu número seja mostrado ao ligar para outros números).

3.6.8.11.12 Bloqueio de chamadas originadas LDN, LDI, de chamadas para celular, de prefixo de operadoras e de Chamadas para 0800, 0300 ou 0500 por terminal.

3.6.8.12 Todos os ramais devem ser fornecidos com licença de softphone, para atendimento de ligações internas e externas, que implemente as seguintes funcionalidades mínimas:

3.6.8.12.1 Deve ser do mesmo fabricante da solução de comunicação ofertada e utilizar obrigatoriamente o protocolo SIP.

3.6.8.12.2 Deve permitir ligações e conferências de áudio e videoconferência, com até 25 participantes internos na mesma conferência / videoconferência, sem limite de quantidade de sessões simultâneas.

3.6.8.12.3 Possuir versões para instalação em sistemas operacionais Windows 10, iOS 15.5 ou superior e Android 8 ou superior, sendo que uma única licença deverá permitir seu registro em todos os sistemas operacionais acima descrito,



de forma simultânea.

3.6.8.12.4 Possuir publicação nas lojas de aplicativos da Apple (App Store) e Android (Google Play).

3.6.8.12.5 Permitir ao usuário ter a capacidade de monitorar em seu softphone o estado de presença dos contatos da organização (integrados a solução) e que utilizem o mesmo softphone.

3.6.8.12.6 Permitir ao usuário a ocultação de seu estado de presença para outro usuário ou para grupo de usuários.

3.6.8.12.7 Permitir que o usuário, durante uma ligação, possa alternar entre dispositivos (mantendo a sessão da ligação), e que durante a ligação o status do usuário fique como "ocupado"

3.6.8.12.8 Deve suportar transferência de chamadas

3.6.8.12.9 Deve suportar retenção de chamada

3.6.8.12.10 Deve suportar serviços de presença, chat, áudio e vídeo, compartilhamento de tela e transferência de arquivos

3.6.8.12.11 Deve suportar codecs de áudio G.711, G.729 e G.722

3.6.8.12.12 Deve suportar codecs de vídeo H.264 com resoluções QCIF, CIF, VGA e HD.

3.6.8.13 Suporte SIP/TLS com mecanismos de segurança com algoritmo de criptografia AES-256 e com suporte a função hash SHA384

3.6.8.14 Suporte a SRTP com AES-128 Counter Mode para proteção e Hash Message Authentication Code (HMAC)-SHA-1 para autenticação.

3.6.8.15 Possuir quadro branco, permitindo que todos os usuários de uma sessão de videoconferência escrevam / desenhe em tela compartilhada.

3.6.8.16 Permitir o compartilhamento de tela e conteúdo, sem a necessidade de estabelecimento de ligação de voz e/ou vídeo.

3.6.8.17 Permitir fundo de tela virtual em sessões de videoconferência.

3.6.8.18 Permitir o uso da logomarca da CONTRATANTE na tela de usuário.

3.6.8.19 Permitir que os usuários consultem dados estatísticos que demonstrem em determinado período de tempo, no mínimo, quais as suas principais conexões, tempo e quantidade de reuniões realizadas, novas conexões e total de conexões.

3.6.8.20 Permitir o ajuste da redução de ruído, de forma que o usuário possa optar entre remover todo o ruído de fundo, remover somente o ruído de fundo que não seja voz e otimizar redução de ruídos de forma a permitir frequências de música.

3.6.9 SBC – SESSION BORDER CONTROLLER

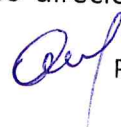
3.6.9.1 A solução deverá possuir Session Border Controller com as seguintes características mínimas:



- 3.6.9.1.1 Deverá ser instalado juntamente com a solução em nuvem, com as mesmas características de hospedagem.
- 3.6.9.1.2 Não é obrigatório que seja do mesmo fabricante da Plataforma de Voz SIP centralizada, desde que resguardada inteira interoperabilidade e compatibilidade com o restante da solução e cumpra as funções aqui descritas.
- 3.6.9.1.3 Deve suportar sessões com terminais SIP de voz e vídeo.
- 3.6.9.1.4 Deve suportar RFC 3261.
- 3.6.9.1.5 Deve suportar proteção DoS/DdoS.
- 3.6.9.1.6 Deve suportar Buffer de jitter dinâmico.
- 3.6.9.1.7 Deve suportar supressão de silêncio/ruído de conforto.
- 3.6.9.1.8 Deve suportar Codecs: G.711, G.723.1, G.726, G.729A/B, GSM-FR, AMR-NB, AMR-WB (G.722.2), SILK-NB/WB, Opus-NB/WB.
- 3.6.9.1.9 Criptografia e autenticação TLS, DTLS, SRTP, HTTPS, SSH, autenticação SIP Digest cliente/servidor, RADIUS Digest.
- 3.6.9.1.10 Deve suportar terminação e mediação RTP/SRTP.
- 3.6.9.1.11 Deve suportar transporte com TLS.
- 3.6.9.1.12 Deve suportar IPv4/IPv6.
- 3.6.9.1.13 Deve suportar VLAN para conexão com localidades remotas.
- 3.6.9.1.14 Deve suportar manipulação de cabeçalho SIP.
- 3.6.9.1.15 Deve suportar SIP trunking com services SIP de operadores de telefonia com perfil SIP configurável.
- 3.6.9.1.16 Deve suportar roteamento estático configurável.
- 3.6.9.1.17 Deve suportar múltiplas interfaces e redes WAN.
- 3.6.9.1.18 Deve suportar separação de endereçamento IP para sinalização e mídia.
- 3.6.9.1.19 Deve suportar media anchoring.
- 3.6.9.1.20 Deve suportar redundância.
- 3.6.9.1.21 Deve suportar transcoding de áudio e vídeo.
- 3.6.9.1.22 Deve suportar regras de firewall e possuir detecção de intrusão (IDS)
- 3.6.9.1.23 Deve suportar protocolo HTTPS.
- 3.6.9.1.24 A CONTRADADA deverá garantir que haja atualização de versões estáveis das plataformas de software e atualização de versões de firmware do SBC durante todo o período da contratação.

3.6.10 LICENÇA DE RAMAL:

- 3.6.10.1 Além das funcionalidades básicas solicitadas, as licenças de ramais deverá permitir:
- 3.6.10.2 Deverá permitir o uso simultâneo de até 5 dispositivos, podendo ser telefones IP e/ou softphone, de forma que uma ligação direcionada para o



ramal toque simultaneamente em todos os dispositivos, bem como o usuário possa gerar ligações de seu ramal em qualquer um dos dispositivos.

3.6.10.3 Conferência de voz nos telefones IP com até 15 participantes.

3.6.10.4 Captura de chamadas (A Captura de Chamada é um serviço multiusuário que permite que usuários selecionados respondam a qualquer linha que esteja tocando em seu grupo de captura de chamada).

3.6.10.5 Chefe-secretária, de forma que o ramal do chefe possa ser atendido por um grupo de secretárias e, posteriormente encaminhadas ao ramal do chefe.

3.6.10.6 Música em chamadas em espera (O serviço de usuário do Music On Hold permite que um usuário toque músicas personalizadas para os chamadores quando a chamada é retida ou estacionada).

3.6.10.7 Cadeado eletrônico (Códigos de autorização para efetuar chamadas).

3.6.10.8 Não perturbe (Quando o usuário ativa o serviço Não Perturbe (DND), todas as chamadas para o usuário são processadas como se o usuário estivesse ocupado e não pudesse receber chamadas).

3.6.10.9 Desvio Noturno (O Night Forwarding permite que as chamadas externas recebidas no usuário sejam redirecionadas para um destino especificado em um horário estabelecido).

3.6.10.10 Retorno automático de chamadas (O Automatic CallBack permite ao originador ser notificado quando o lado chamado, em caso de ocupado, ficar livre).

3.6.10.11 Deverá ser fornecido ao menos 1 licença com até 1.000 participantes internos e externos na mesma sessão de áudio e/ou videoconferência, sem limite de quantidade de sessões simultâneas, permitindo a gravação das reuniões, transmissão ao vivo (Live Streaming) da reunião nas plataformas Youtube e Facebook / Instagram, whiteboarding e compartilhamento de conteúdo.

3.6.11 LICENÇAS DE URA

3.6.11.1 A Solução de PABX Virtual em Nuvem deve possuir sistema de autoatendimento eletrônico com as seguintes características:

3.6.11.2 Deve permitir fazer o atendimento automático utilizando uma mensagem de boas-vindas, menu de navegação com a seleção através de 1 dígito DTMF.

3.6.11.3 Deve permitir, no mínimo, 5 menus de navegação distintos, com mensagens personalizadas para cada um dos menus.

3.6.11.4 O menu deve possuir pelo menos 2 níveis (menu principal e, pelo menos, um submenu).

3.6.11.5 Deve permitir que toda sua configuração possa ser feita através de



um Portal de administração da unidade de autoatendimento.

3.6.11.6 A árvore de menus do autoatendimento deve ser montada associando usuários/terminais que fazem parte de um mesmo Código Nacional (DDD) ou terminais Fixos ou Móveis a um Número Virtual de atendimento.

3.6.11.7 Deve permitir Menus distintos de Horário comercial, após expediente e feriados a serem configurados via portal de administração do serviço.

3.6.11.8 Deve permitir que além das opções do Menu principal, que seja possível a opção de retornar para o Menu Anterior.

3.6.11.9 Os anúncios de áudio devem ser gerenciados via portal de administração do serviço, com possibilidade de carga de substituição (upload) de trechos de áudio.

3.6.12 APARELHO IP

3.6.12.1 Possuir homologação da Anatel.

3.6.12.2 Ser homologado com o sistema de telefonia IP utilizado na nuvem.

3.6.12.3 Deve permitir acesso a todas as facilidades / funções do PABX em nuvem.

3.6.12.4 Áudio HD com Redução de ruído, no viva-voz e no fone.

3.6.12.5 Tela de no mínimo 2 polegadas (128x48 pixels).

3.6.12.6 2 linhas SIP.

3.6.12.7 Conferência de 3 vias.

3.6.12.8 1000 lista telefônica local, identificador de chamadas, chamada em espera, transferência de chamada.

3.6.12.9 Suportar Fone de ouvido sem fio EHS.

3.6.12.10 Chamada de áudio.

3.6.12.11 Built-in alto-falantes HD.

3.6.12.12 Áudio de banda larga.

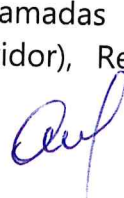
3.6.12.13 Suportar os codecs G.711a/u, G.726-32K, G.729A, iLBC, G.722 e Opus.

3.6.12.14 Deve suportar as funcionalidades de AEC, VAD, CNG, BNE, NR, PLC.

3.6.12.15 Deve possuir 4 teclas programáveis.

3.6.12.16 Deve possuir 9 teclas de função (Reter/Transferir/Conferência/Agenda/MWI/Fone de ouvido/Rediscagem).

3.6.12.17 Deve suportar as funcionalidades: Chamar, Atender, Rejeitar, Silenciar, Ativar som (Microfone), Chamada em espera, Retomar, Intercomunicador, Visor de ID do chamador, Discagem rápida, Chamada Anônima (Ocultar ID do Chamador), Desvio de Chamadas (Sempre/Ocupado/Sem Resposta), Transferência de chamadas (assistida/não assistida), Call Parking/Pick-up (Dependendo do servidor), Remarcar, Não



perturbe, Atendimento Automático, Mensagem de voz (com servidor).

3.6.12.18 Suportar 2 ângulos ajustáveis, 45° ou 50° modo de instalação para cenário de desktop pode atender às necessidades de vários ambientes de escritório.

3.6.12.19 Deve possuir 02 interfaces de rede RJ-45 10/100/1000 Base-T para conexão de desktop e conectividade com a Rede LAN.

3.6.12.20 Função PoE (IEEE 802.3af) registra como dispositivo de classe 1 e suporta 802.3az.

3.6.12.21 Suporte aos protocolos SIP2.0 over UDP/TCP/TLS, RTP/RTCP/SRTP, STUN, DHCP, IPv6, LLDP, PPPoE, 802.1x, L2TP, OpenVPN, SNMP, FTP/TFTP, HTTP/HTTPS, TR-069.

3.6.12.22 Devem ser fornecidos com fonte de alimentação AC 100V-240V.

3.7 CARACTERÍSTICAS DA PRESTAÇÃO DO SERVIÇO MÓVEL PESSOAL (SMP)

3.7.1 Prestação do Serviço Móvel Pessoal (SMP), regulamentado pela ANATEL, utilizando tecnologia 4G ou superior, mediante o fornecimento de aparelhos telefônicos móveis, sob a forma de comodato, nas quantidades previstas na planilha de preços, com uma linha habilitada para cada aparelho.

3.7.2 As chamadas locais e de longa distância nacional, entre terminais móveis adquiridos pela CONTRATANTE, pertencentes ao mesmo plano, deverão ser gratuitas para utilização dentro da área de cobertura da CONTRATADA, independentemente da quantidade de chamadas realizadas.

3.7.3 A CONTRATADA deverá reparar ou substituir os aparelhos que apresentarem defeito, de acordo com os seguintes procedimentos:

3.7.3.1 Repor qualquer aparelho utilizado pelo CONTRATANTE, na hipótese de roubo ou furto, em até 30 dias úteis, a partir da apresentação do Registro de Ocorrência Policial, ficando a CONTRATANTE, nessa hipótese responsável pelo custo de reposição, considerando o preço apurado através de pesquisa de mercado realizada pela CONTRATANTE.

3.7.3.2 Repor qualquer aparelho utilizado pelo CONTRATANTE, na hipótese de perda ou de dano, em 30 dias úteis, contadas da data da comunicação da ocorrência de perda, ou da emissão de laudo do fabricante ou da Assistência Técnica autorizada da rede credenciada em relação à natureza dano.

3.7.3.3 Repor, a expensas da CONTRATADA, qualquer aparelho utilizado pelo CONTRATANTE, na hipótese de defeito de fabricação, em até 30 dias úteis, a partir da comunicação da CONTRATANTE, acompanhada de laudo do fabricante ou da Assistência Técnica da rede credenciada.

3.7.3.4 O reparo ou substituição dos aparelhos, no caso de defeito de fabricação, não pode representar nenhum ônus para a CONTRATANTE.



3.7.3.5 Os aparelhos móveis que serão fornecidos por ocasião das reposições previstas deverão possuir características técnicas, no mínimo, iguais ou superiores às características dos aparelhos substituídos.

3.7.4 Responsabilizar-se pelo imediato bloqueio da linha a partir da comunicação pelo CONTRATANTE de roubo, furto ou perda do aparelho, não cabendo ao CONTRATANTE o pagamento de quaisquer serviços contratados que porventura venham a ser utilizados indevidamente.

3.7.5 Características das linhas:

3.7.5.1 Ligações ilimitadas para qualquer operadora, inclusive em Roaming.

3.7.5.2 Utilização de dados com limite de 02 Gigabytes de consumo por linha.

3.7.5.3 Gerenciador On-line

3.7.6 A CONTRATADA deverá atender aos seguintes requisitos mínimos:

3.7.6.1 Executar os serviços contratados, em conformidade com as especificações e condições discriminadas neste Memorial Descritivo, dentro de elevados padrões de qualidade, observando as normas legais e regulamentares e cumprindo, além das responsabilidades resultantes do contrato, as previstas na Lei nº 9.472/97, no contrato de prestação do SMP e no Termo de Autorização assinado com a ANATEL e demais disposições regulamentares pertinentes aos serviços.

3.7.6.2 Manter o sigilo e a inviolabilidade dos serviços, respeitadas as hipóteses e condições constitucionais e legais de quebra de sigilo das Telecomunicações e os regulamentos do Serviço Móvel Pessoal.

3.7.6.3 Responsabilizar -se pelo cumprimento dos postulados legais vigentes, de âmbito federal, estadual ou municipal, como também assegurar os direitos e o cumprimento de todas as obrigações estabelecidas pela regulamentação da ANATEL, inclusive quanto aos preços praticados no instrumento contratual.

3.7.7 Emitir mensalmente relatório detalhado dos serviços cobrados, relativos ao Serviço Móvel Pessoal incluindo, no mínimo, para cada chamada, as seguintes informações:

3.7.7.1 Área de Registro de origem e Área de Registro ou localidade de destino da chamada.

3.7.7.2 Código de Acesso chamado.

3.7.7.3 Data e horário (hora, minuto e segundo) do início da chamada.

3.7.7.4 Duração da chamada (hora, minuto e segundo).

3.7.7.5 Valor da chamada, explicitando os casos de variação horária.

3.7.8 O serviço contratado deverá possuir cobertura em todos os estados da federação, por meios próprios ou por convênio (Roaming) com outras operadoras não sendo necessária à realização de qualquer alteração na configuração do aparelho ou troca do aparelho ou chip para execução desses serviços.

3.7.9 A CONTRATADA deverá possibilitar aos usuários dos aparelhos, na condição de assinante viajante, receber a prestação do SMP em redes de outras prestadoras de serviço (roaming nacional).

3.7.10 O roaming a que se refere o item anterior funcionará apenas nos locais onde houver cobertura de serviço SMP devendo ocorrer de forma automática, conforme regulamentação da ANATEL.

3.7.11 Para as linhas habilitadas, deverão ser disponibilizadas as identificações de chamadas, serviço de envio e recebimento de mensagens de texto, transferência de chamadas, chamadas em espera, conta detalhada e deverá ser fornecido um serviço de gestão das linhas pela web (online), onde seja possível controlar o consumo e criar perfis com o tipo de ligação e permissões do que cada linha pode realizar.

3.7.12 Os serviços deverão ser executados de forma contínua, ou seja, 24h (vinte e quatro horas) por dia, sete dias por semana, exceto nas interrupções programadas para manutenção preventiva, previamente informada à CONTRATANTE e nos casos fortuitos e de força maior.

3.7.13 O encaminhamento das chamadas deverá ser feito de maneira que o usuário receba sinais audíveis, facilmente identificáveis e com significados nacionalmente padronizados, nos termos da regulamentação, que lhe permitam realizar uma comunicação perfeita.

3.7.14 As chamadas deverão ser realizadas com boa qualidade de transmissão, em níveis adequados, com níveis de ruído e interferência desprezíveis e com baixa incidência de queda e/ou interrupção das ligações, nos termos da regulamentação.

3.8 PONTO DE ACESSO SEM FIO

3.8.1 Os Pontos de Acesso Wi-Fi deverão ser do mesmo fabricante da solução de Firewall/SD-WAN

3.8.1.1 A exigência de que os Pontos de Acesso Wi-Fi sejam do mesmo fabricante da solução de Firewall/SD-WAN visa garantir integração nativa, aplicação unificada de políticas de segurança, maior interoperabilidade e gestão centralizada do ambiente de rede. Essa padronização reduz riscos de incompatibilidade, simplifica a operação, melhora o suporte técnico e assegura maior eficiência, desempenho e segurança na infraestrutura de TI.

3.8.2 Deverão ser fornecidos dois modelos pontos de acesso WiFi segura e confiável para redes corporativas:

3.8.3 Access Point Tipo 1 – Indoor - 6 devices

3.8.3.1 Ponto de acesso (AP) que permita acesso dos dispositivos à rede através da rede wireless e que possua todas as suas configurações centralizadas em controlador wireless hospedado na nuvem do fabricante;



- 3.8.3.2 Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;
- 3.8.3.3 Deve estabelecer automaticamente a conexão com o controlador wireless na nuvem do fabricante;
- 3.8.3.4 Deve permitir ser gerenciado remotamente através de links WAN;
- 3.8.3.5 Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax, de forma simultânea;
- 3.8.3.6 Deve possuir capacidade tri-band, com rádios 2.4GHz, 5GHz e 6GHz operando simultaneamente, permitindo configurações independentes para cada rádio;
- 3.8.3.7 O ponto de acesso deve suportar funcionamento de rádio dedicado para monitoramento de radiofrequência, segurança wireless e identificação de interferências (wIDS/wIPS), podendo este recurso ser realizado por compartilhamento dinâmico de rádio conforme arquitetura do fabricante;
- 3.8.3.8 Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;
- 3.8.3.9 Deve permitir a conexão de no mínimo 256 (duzentos e cinquenta e seis) clientes wireless simultaneamente;
- 3.8.3.10 Deve possuir 2 (duas) interfaces Ethernet, sendo:
- 3.8.3.10.1 1 (uma) interface Multi-Gigabit (100Mb/1Gb/2,5Gb) com conector RJ-45 para conexão à rede LAN;
- 3.8.3.10.2 1 (uma) interface 10Mb/100Mb/1Gb;
- 3.8.3.11 Deve suportar agregação de links conforme padrão IEEE 802.3ad, quando aplicável à arquitetura do fabricante;
- 3.8.3.12 Deve permitir sua alimentação através de Power over Ethernet (PoE) conforme o padrão IEEE 802.3at (PoE+);
- 3.8.3.13 O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve poder ocorrer de forma centralizada, através de túnel estabelecido entre o ponto de acesso e o controlador wireless;
- 3.8.3.14 Quando o encaminhamento de tráfego for centralizado, o tráfego deve ser protegido por túnel seguro (IPSec ou equivalente);
- 3.8.3.15 A solução deve suportar Split Tunneling por SSID, permitindo listas de exceção para tráfego local;
- 3.8.3.16 Adicionalmente, deve suportar modo de encaminhamento Bridge Mode (Local Switching), no qual o tráfego é comutado localmente na interface Ethernet do ponto de acesso;
- 3.8.3.17 Deve permitir operação em modo Mesh;
- 3.8.3.18 Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais por rádio;



-
- 3.8.3.19 Deve suportar MU-MIMO;
 - 3.8.3.20 Deve suportar OFDMA;
 - 3.8.3.21 Deve suportar modulação de até 1024-QAM;
 - 3.8.3.22 Deve implementar o recurso Target Wake Time (TWT) configurável por SSID;
 - 3.8.3.23 Deve suportar operação em 5 GHz com canais de 20, 40 e 80 MHz;
 - 3.8.3.24 Deve possuir antenas internas ao equipamento, adequadas às bandas de 2.4 GHz, 5 GHz e 6 GHz;
 - 3.8.3.25 Em conjunto com o controlador wireless, deve otimizar automaticamente o desempenho e a cobertura RF, com ajuste dinâmico de potência e canais;
 - 3.8.3.26 Em conjunto com o controlador wireless, deve permitir a identificação de interferências provenientes de equipamentos Wi-Fi e não-Wi-Fi nas frequências de 2.4 GHz, 5 GHz e 6 GHz;
 - 3.8.3.27 Deve suportar mecanismos de detecção e mitigação de pontos de acesso não autorizados (Rogue APs);
 - 3.8.3.28 Em conjunto com o controlador wireless, deve implementar mecanismos de proteção contra ataques à infraestrutura wireless (WIDS/WIPS);
 - 3.8.3.29 Deve permitir a criação de múltiplos SSIDs, com no mínimo 14 (quatorze) SSIDs simultâneos, com políticas distintas de segurança e rede;
 - 3.8.3.30 Deve suportar os métodos de autenticação WPA2 (AES) e WPA3;
 - 3.8.3.31 Deve implementar o protocolo IEEE 802.1X, com associação dinâmica de VLANs baseada em atributos RADIUS;
 - 3.8.3.32 Deve suportar os métodos de autenticação EAP-TLS, EAP-TTLS e PEAP;
 - 3.8.3.33 Deve implementar os padrões IEEE 802.11r, 802.11k e 802.11v, visando otimização de roaming;
 - 3.8.3.34 Deve suportar gerenciamento via SNMP;
 - 3.8.3.35 Deve suportar integração via REST API;
 - 3.8.3.36 Deve possuir estrutura adequada para operação em ambientes internos, permitindo instalação em paredes e tetos, acompanhando os respectivos kits de fixação;
 - 3.8.3.37 Deve operar em ambientes com temperatura entre 0 °C e 45 °C;
 - 3.8.3.38 Deve possuir sistema antifurto do tipo Kensington Security Lock ou equivalente;
 - 3.8.3.39 Deve possuir indicadores luminosos (LED) para status do equipamento;
 - 3.8.3.40 O ponto de acesso deverá ser totalmente compatível e gerenciado pelos controladores wireless em nuvem deste processo;

- 3.8.3.41 Quaisquer licenças e/ou softwares necessários para pleno funcionamento das características descritas deverá ser fornecidos;
- 3.8.3.42 Deve possuir certificação Wi-Fi Alliance;
- 3.8.3.43 Deve estar homologado pela ANATEL na data de execução do pregão.

3.8.4 Access Point Tipo 2 – Outdoor - 6 devices

- 3.8.4.1 O Ponto de Acesso (AP) deverá ser destinado a uso externo (OUTDOOR), de classe corporativa, projetado para operação contínua em ambientes abertos, com gerenciamento centralizado por controladora ou plataforma de gestão em nuvem do fabricante, permitindo provisionamento automático, monitoramento, aplicação de políticas e operação remota através de enlaces WAN.
- 3.8.4.2 Deve permitir a conexão simultânea de dispositivos que implementem os padrões IEEE 802.11a/b/g/n/ac/ax/be (Wi-Fi 7).
- 3.8.4.3 Deve operar de forma tri-band, com rádios de serviço nas bandas 2,4 GHz, 5 GHz e 6 GHz, operando simultaneamente.
- 3.8.4.4 Deve possuir arquitetura quad-radio, incluindo um rádio dedicado exclusivamente para varredura, monitoramento e segurança wireless, permitindo análise contínua do espectro sem impacto no atendimento aos clientes.
- 3.8.4.5 Deve ser adequado a cenários de alta densidade, suportando no mínimo 512 clientes por rádio nos rádios de serviço, garantindo desempenho em ambientes externos com grande concentração de usuários.
- 3.8.4.6 Deve utilizar antenas externas, apropriadas para ambientes externos, com conectores RP-SMA.
- 3.8.4.7 Deve disponibilizar múltiplos conectores RP-SMA, compatíveis com operação tri-band (2,4 GHz, 5 GHz e 6 GHz) e com a arquitetura de múltiplos rádios, permitindo ajuste fino de cobertura, ganho e padrão de irradiação conforme o cenário outdoor.
- 3.8.4.8 As antenas devem ser compatíveis com instalação em áreas abertas, garantindo cobertura adequada e resistência às condições ambientais.
- 3.8.4.9 Deve suportar MU-MIMO e OFDMA em uplink e downlink, otimizando eficiência espectral em ambientes externos congestionados.
- 3.8.4.10 Deve suportar modulações avançadas compatíveis com Wi-Fi 7, incluindo 4096-QAM, quando aplicável, e larguras de canal ampliadas na banda de 6 GHz, conforme regulamentação vigente.
- 3.8.4.11 Deve suportar Target Wake Time (TWT), configurável por SSID ou política, visando eficiência energética e melhor gerenciamento de dispositivos conectados.
- 3.8.4.12 Deve suportar WIDS/WIPS, com detecção e mitigação de pontos de acesso não autorizados (Rogue APs).



- 3.8.4.13 O rádio dedicado de varredura deve permitir operação em modos background ou dedicado, garantindo identificação de interferências, ameaças e ataques wireless.
- 3.8.4.14 Deve permitir captura de pacotes (Packet Sniffer) e análise de espectro, facilitando diagnóstico, troubleshooting e identificação de fontes de interferência Wi-Fi e não-Wi-Fi.
- 3.8.4.15 Deve possuir, no mínimo:
- 3.8.4.15.1 1 (uma) interface Ethernet RJ-45 Multi-Gigabit (10/100/1000/2,5G/5G/10G) para uplink principal de dados;
- 3.8.4.15.2 1 (uma) interface Ethernet RJ-45 adicional 10/100/1000 (1 GbE) para conectividade complementar ou redundância.
- 3.8.4.16 Deve permitir alimentação via Power over Ethernet (PoE), compatível com a arquitetura de múltiplos rádios e alta capacidade de processamento, mantendo operação completa do equipamento conforme a disponibilidade energética.
- 3.8.4.17 Deve possuir rádio Bluetooth Low Energy (BLE) integrado, permitindo aplicações de localização, beacon, inventário e suporte a soluções IoT em ambientes externos.
- 3.8.4.18 O equipamento deve possuir grau de proteção ambiental adequado para uso externo, resistente à poeira, umidade e intempéries, não sendo aceitas soluções baseadas em caixas ou invólucros adicionais para atingir tal proteção.
- 3.8.4.19 Deve operar em faixa estendida de temperatura, compatível com ambientes externos, garantindo funcionamento contínuo sob variações climáticas.
- 3.8.4.20 Deve permitir instalação em postes, paredes ou fachadas, acompanhando os respectivos kits de fixação adequados para uso outdoor.
- 3.8.4.21 O ponto de acesso deverá ser totalmente compatível com a plataforma de gerenciamento proposta neste processo.
- 3.8.4.22 Todas as licenças, softwares e funcionalidades necessárias ao pleno funcionamento do equipamento deverão estar contempladas.
- 3.8.4.23 Deve estar homologado pela ANATEL na data de execução do pregão.

4. CARACTERÍSTICAS DO CAPTIVE PORTAL

- 4.1 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall.
- 4.2 DAS FUNCIONALIDADES



4.2.1 Portal Personalizável, Social Login, Integração com Redes Sociais, Optin - Termo de aceite (Autorização), Bloqueio de Usuários (Uso suspeito), Dashboard Personalizável, Idioma (Português), Envio Automático de Relatórios via E-mail, Reconhecimento do Usuário, Reconhecimento do Usuário - Interação entre Empresas, Fluxo de Visitantes, Visitantes Novos x Retornantes, Mapa de Calor, Presença, Social Dashboard (UX), Rede Corporativa, Rede Visitante, Geofencing (gatilho para envio de conteúdo por localidade ou zona). Envio por e-mail ou sms, Validação de CPF, Lista de Inscritos / Contatos, Planos de acesso diferentes de acordo com Lista de Inscritos, Envio de Relatórios e pesquisas via FTP, Integração com Google Analytics, E-mail de Boas Vindas, Definição de Idade Mínima para acesso ao Wi-Fi, Relatórios Automáticos com estatísticas de Wi-Fi campanhas e nps, Servidor de gerenciamento de upload de mídias para customização HTML, Token para registro e login via SMS, Monitoramento de quedas de acessos, Geração de Voucher com personalização de plano de acesso, Mensagem automática de Feliz Aniversário na tela de retorno, Verificação de e-mail para registro, Optin Personalizável para Mídias, Optin Personalizável para Pesquisas, Integração de Mídia via API, Gerenciamento de níveis de acessos para diversos perfis (Marketing, TI, Admin), Estruturação de Grupo e Subgrupos, Integração com PMS, Sistema de Dupla aprovação para inserção de campanhas, Limite de funcionamento do Wi-Fi, Recorrência de usuários na rede Wi-Fi, Roaming, Autonomia do cliente para customização da página de login;

4.3 DOS RELATÓRIOS

4.3.1 Registro de Usuários, Relatório de Resultados de Campanhas, Taxas de Uso da Rede, Frequência, Dias e Horários de Pico, Tipos de Aparelho, Relatório Guest Wifi, Total de Visitas, Tempo de Permanência, Passantes Próximo ao Local, Conversão de Entrada, Total de Visitas Por Zonas, Comparação de Datas, Fluxo de Visitantes Entre Zonas, Smartzones (zonas temporárias para eventos ou campanhas temporárias).

4.4 DAS FERRAMENTAS

4.4.1 Motor de Disparo, Criação de Campanhas, Agendamento de Campanhas, E-mail Marketing, SMS, NPS, Modal, Pesquisas, Inserção de Vídeos, Inserção de Imagens, Inserção de Galeria, Inserção de Mídia por AP, Integrações com CRM, Integração com DATA LEAK, Pesquisa Call to Action, Divulgação de Mídia para Lista de Inscritos, Pesquisa na tela de Login, Disparo de sms para usuários online, Coleta de Dados Adicionais, TAG BigData, Calendário, Mídia Programática, Cupons.



5. DOS LOCAIS DE PRESTAÇÃO DO SERVIÇO E NÚMEROS A SER PORTADOS

5.1 Órgão deverá disponibilizar a relação dos endereços e velocidades que deverão ser entregues na solução.

6. TREINAMENTOS:

6.1 FIREWALL:

6.1.1 A contratada deverá oferecer um treinamento de 08 horas para os funcionários, a ser ministrado em formato presencial ou remoto. A data e horário para a realização do treinamento serão definidos em acordo com o alinhamento de ambas as partes.

6.1.2 O objetivo do treinamento é capacitar os funcionários para desempenhar melhor suas funções, aprimorando as habilidades e conhecimentos técnicos necessários para o desenvolvimento de suas atividades. O treinamento deve ser desenvolvido por profissionais qualificados e com experiência.

6.1.3 PABX em nuvem:

6.1.4 A CONTRATADA deverá fornecer treinamento da solução de Voz na Nuvem para os usuários.

6.1.5 Devem ser previstos, pelo menos os seguintes treinamentos:

6.1.6 Orientação sobre usos do equipamento para usuários administrativos – no momento da instalação. Esta instrução deverá ser realizada, presencialmente ou remoto, sem ônus para o CONTRATANTE.

7. DOS PRAZOS DE EXECUÇÃO DOS SERVIÇOS

7.1.1 ELABORAÇÃO DO PLANO DE IMPLANTAÇÃO

7.1.2 A CONTRATADA deverá apresentar um Plano de Implantação em no máximo 15 dias corridos a partir da assinatura do Contrato.

7.1.3 A execução do Plano de Implantação somente poderá ser iniciada após a sua aprovação pela CONTRATANTE.

7.1.4 O detalhamento do Plano de Implantação deverá conter no mínimo:

7.1.5 Cronograma com macro atividades a serem desenvolvidas para a implantação de todos os serviços previstos neste Termo de Referência. O cronograma deverá conter as seguintes informações:

7.1.5.1 Identificação dos responsáveis das atividades.

7.1.5.2 Duração das atividades.

7.1.5.3 Sequenciamento das atividades.

7.1.5.4 Projeto com topologias (física e lógica) da rede, elementos envolvidos, localização dos POPs, faixas de endereçamento IP, detalhamento da gerência, bem como a arquitetura do serviço, incluindo a estratégia de roteamento.

7.2 DA INSTALAÇÃO DOS SERVIÇOS

7.2.1 A CONTRATADA terá até 10 dias corridos após a assinatura do contrato para instalar os serviços especificados no Termo de Referência.

7.2.2 A instalação do circuito e CPE somente será considerada concluída após a aprovação, pelo Gestor do Contrato, que ocorrerá em até 5 (cinco) dias corridos após notificação da CONTRATADA.

7.2.3 Todos os equipamentos deverão suportar alimentação com tensão de 110/220 Volts (corrente alternada) bifásica com frequência de 60 Hz.

7.3 DO GERENCIAMENTO DA IMPLANTAÇÃO

7.4 Disponibilizar e alocar 1 (um) profissional que será responsável pelo gerenciamento das atividades do projeto de implantação, por parte da CONTRATADA.

7.5 Obter informações e esclarecimentos necessários para que possa elaborar o Plano de Implantação do Serviço. Serão abordados e discutidos os seguintes pontos:

7.5.1 Instalação dos circuitos.

7.5.2 Datas e horários de restrição para implantação.

7.5.3 Requisitos de infraestrutura necessários para a instalação dos equipamentos.

7.5.4 Requisitos para a elaboração e entrega do Plano de Implantação do Serviço.

7.5.5 Serviços que deverão ser configurados na implantação.

7.5.6 Demais assuntos de interesse correlatos à implantação dos serviços.

8. QUALIFICAÇÃO TÉCNICA

8.1 Atestado(s) de Capacidade Técnica em nome do licitante, emitido(s) por pessoa jurídica de direito público ou privado, que comprove(m) a prestação satisfatória dos serviços pertinentes ao objeto desta Seleção;

8.2 O(s) atestado(s) deverão conter, no mínimo, as seguintes informações:

8.2.1 Dados da empresa: nome, CNPJ.

8.2.2 Dados da empresa cliente: nome, razão social, CNPJ, endereço.

8.2.3 Descrição dos serviços prestados com dados que permitam identificar a compatibilidade e similaridade com o objeto da seleção, incluindo as quantidades e taxas de transmissão dos serviços.

8.2.4 Grau de satisfação do cliente, com manifestação expressa do signatário, quanto à qualidade dos serviços prestados.

8.2.5 Dados do emissor do atestado: nome, cargo, telefone e e-mail de contato.

8.2.6 Local, data de emissão e assinatura do emissor.

8.3 Serão aceitos os somatórios de atestados para o atendimento da solução;

8.4 Os atestados poderão ser objetos de diligência a fim de se esclarecer



quaisquer dúvidas quanto ao seu conteúdo, inclusive com solicitação dos respectivos contratos que lhe deram origem, visitas ao local, etc.;

8.5 Sobre o serviço de Anti-DDoS do link de internet o vencedor deverá anexar um documento com a estratégia de mitigação para fins de comprovação técnica.

8.6 Caso a PROPONENTE não seja o Fabricante do produto ofertado deverá anexar documentação comprovando que é credenciada e tem o mais alto nível de parceria pelo Fabricante, para comercialização, serviços de instalação, suporte, garantia e treinamento;

8.7 O licitante da solução deverá comprovar que possui certificação técnica junto ao fabricante da solução ofertada, comprovando a capacitação técnica dos profissionais que serão responsáveis pelas tarefas de instalação, configuração e suporte dos produtos, mediante a entrega de cópia do certificado técnico destes profissionais junto ao fabricante, que deverá ocorrer no prazo máximo de 10 (dez) dias após a assinatura do contrato.

8.8 Deverá apresentar documentos que comprovem o vínculo do profissional certificado junto a licitante vencedora do certame, no prazo máximo de 10 (dez) dias após a assinatura do contrato.

8.9 Apresentar catálogos, prospectos, folders, manuais e outros documentos e informações sob a marca, fabricante, modelo e outros dados pertinentes que permitam a clara e segura identificação do produto ofertado, em idioma português ou inglês, em original ou cópia, não sendo aceitos documentos impressos de qualquer natureza produzidos com a finalidade específica de possibilitar e qualificar tecnicamente a proposta da licitante. Os documentos poderão ser entregues em formato eletrônico;

8.10 Para comprovação dos requisitos técnicos dos equipamentos SD-WAN a CONTRATANTE deverá apresentar uma matriz de responsabilidade comprovando o ponto a ponto, informando o nome do documento e o link se o arquivo for online.

8.10.1 Será necessário comprovar no ponto a ponto, os itens que citados nas ESPECIFICAÇÕES TÉCNICAS MINIMAS NECESSÁRIAS DO EQUIPAMENTO FIREWALL;

8.11 Deverá apresentar certificados ou comprovação que os equipamentos são homologados pela ANATEL;

8.12 Apresentar autorização SCM (Serviço de Comunicação Multimídia) da ANATEL;

8.13 Apresentar autorização SMP (Serviço Móvel Pessoal) da ANATEL;

8.14 Apresentar a licença de STFC (Serviço de Telefonia Fixa Comutada) junto a ANATEL (Agência Nacional de Telecomunicações) para a prestação do serviço;

8.15 Deverá comprovar que possui pelo menos um Ponto de Presença (PoP) local no município que se encontra;



8.16 Apresentar Comprovante de Cadastro da Operadora na ABR Telecom, a mesma poderá ser comprovada através de uma ficha cadastral ou Print da tela de acesso da operadora junto a ABR;

8.17 Será exigida a comprovação da execução de, no mínimo, **50% (cinquenta por cento)** do quantitativo total estimado do objeto contratado, admitindo-se a somatória de atestados para fins de atendimento deste percentual, desde que comprovem a execução de serviços de natureza similar.

9. CENTRAL DE ATENDIMENTO E SUPORTE TÉCNICO

9.1.1 A fim de manter os serviços em funcionamento adequado aos parâmetros contratuais, a CONTRATADA deverá:

9.1.2 Possuir um Centro de Operações de Rede (Network Operations Center – NOC) disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável por monitorar o funcionamento dos serviços e realizar as ações corretivas necessárias para restabelecer a normalidade dos serviços.

9.1.3 Possuir uma equipe especializada (SOC - Security Operation Center), disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável pelo monitoramento, detecção e mitigação de ataques, realizando as ações corretivas necessárias para garantir o bom funcionamento dos serviços.

9.1.4 A CONTRATADA deverá disponibilizar à CONTRATANTE uma Central de Atendimento Técnico, acessível via chamada telefônica gratuita (0800), disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável por prestar suporte técnico, receber chamados de serviços e prestar informações acerca do andamento destes.

9.1.5 O limite de atuação da CONTRATADA para fins de manutenção, reparo e configuração será a porta LAN de seus roteadores ou switches, de forma a garantir os níveis de serviço contratados.

9.1.6 Enviar à CONTRATANTE, por e-mail, notificações de abertura, andamento e fechamento de chamados, realização de manutenção preventiva ou corretiva e fatos relevantes para a prestação e utilização dos serviços.

9.1.7 Enviar à CONTRATANTE, por e-mail, uma lista de recorrência ("escalation list") contendo os nomes, números de telefone e endereços de e-mail das pessoas que devem ser acionadas em caso de problemas no atendimento técnico. A lista de recorrência deverá ser mantida atualizada e sua versão mais recente deverá ser enviada à CONTRATANTE sempre que houver alteração.

9.1.8 A CONTRATADA deverá iniciar o atendimento no prazo máximo de 1 (uma) hora, contada a partir da data e hora do chamado.

9.1.9 Todo acesso às instalações da CONTRATANTE por pessoal técnico da CONTRATADA, ou de seu preposto, deverá ser previamente agendado.

9.1.10 Manutenções e/ou intervenções programadas nos serviços, quando

necessárias, mesmo no caso daquelas que não impliquem inoperância dos serviços contratados ou alteração nas suas características, que necessitem a presença do técnico da CONTRATADA, deverão ser autorizadas pela CONTRATANTE.

9.1.11 Qualquer manutenção e/ou intervenção de caráter emergencial para solução de falhas, inoperâncias e/ou indisponibilidades, verificadas na rede, deverá ser agendada e acordada previamente com a CONTRATANTE.

10. DISPONIBILIDADE

10.1.1 Índice de Disponibilidade:

10.1.2 Os circuitos de comunicação deverão estar disponíveis 24 horas por dia, todos os dias do ano.

10.1.3 A CONTRATADA deverá garantir disponibilidade mensal de no mínimo fornecido à CONTRATANTE, calculada da seguinte forma:

$$DMA = [(43200 - TTICM) / 43200] \times 100$$

Onde:

TTICM: Tempo Total de Interrupção do Circuito (em minutos) no Mês.

DMA(%): Disponibilidade Mensal Atingida

10.1.4 Para efeito de cálculo de TTICM, será considerado o período em minutos entre o primeiro minuto do primeiro dia e o último minuto do último dia do calendário do mês a que se refere a fatura.

10.1.5 O serviço será considerado indisponível quando não for possível a conexão entre o equipamento da CONTRATANTE e o da CONTRATADA, a partir do registro do chamado técnico na Central de Atendimento da CONTRATADA, sendo considerado disponível após o fechamento do chamado técnico, com a devida anuência da CONTRATANTE, na Central de atendimento da CONTRATADA.

10.1.6 Entende-se como início do atendimento a primeira mensagem trocada pela CONTRATANTE com a CONTRATADA informando a ocorrência ou início da ligação efetuada a central de atendimento da CONTRATADA independentemente do atendimento do operador.

10.1.7 O prazo máximo de recuperação dos circuitos será 2 (duas) horas, todos os dias do mês, inclusive sábados, domingos e feriados.

10.1.8 As indisponibilidades informadas pela gerência e supervisão da CONTRATADA, bem como os registros na Central de Atendimento da CONTRATADA serão validadas pelos sistemas de gerência e supervisão da CONTRATANTE.

10.1.9 No caso de interrupção programada por necessidade da CONTRATANTE, a mesma não afetará o índice de disponibilidade da CONTRATADA.

10.1.10 As interrupções programadas solicitadas pela CONTRATANTE serão previamente combinadas com a CONTRATADA.



10.1.11 Desconto por interrupção:

10.1.12 Para cada interrupção do circuito que for comprovadamente de responsabilidade da CONTRATADA, será calculado um desconto referente ao tempo de interrupção desse circuito, cujo valor apurado será ressarcido à CONTRATANTE na Nota Fiscal/Fatura dos serviços com vencimento no mês seguinte ao da apuração.

10.1.13 O valor do desconto será obtido a partir do seguinte cálculo:

$$VD = (VC / 43200) \times n$$

Onde:

VD = Valor do Desconto

VC = Valor mensal pago pelo circuito ativo

n = Quantidade de minutos em que o serviço ficou interrompido.

11. NÍVEIS MÍNIMOS DE SERVIÇO

11.1 A CONTRATADA deverá fornecer o serviço com os seguintes níveis mínimos de disponibilidade os quais são utilizados para mensurar o desempenho e a qualidade dos circuitos:

Disponibilidade	Nível Mínimo de Serviço
Link dedicado Internet	> = 99,5%
Link Banda Larga	> = 95%

12. SUBCONTRATAÇÃO

12.1 É vedada a subcontratação do objeto, permitindo-se exclusivamente a locação de infraestrutura passiva de terceiros (como dutos e postes), permanecendo a CONTRATADA integralmente responsável pela fibra óptica (iluminação própria), roteamento, trânsito IP e mitigação de ataques DDoS.

12.2 Não será permitido a subcontratação do tráfego STFC, sendo obrigatório que os números DDR disponibilizados sejam da própria CONTRATADA junto à ABR Telecom, bem como deverá ser apresentado pelo menos 01 (um) contrato de interconexão com outras operadoras que compreenda a área local a ser atendida ou que a mesma seja concessionária da região.

12.3 A CONTRATADA deve ser detentora do plano de numeração registrado junto a ABR Telecom da região solicitada, não podendo ser subcontratado a parte inerente ao objeto STFC;



13. FORMA DE APURAÇÃO DO PREÇO

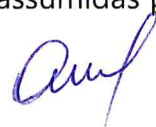
- 13.1 O Preço unitário em moeda Brasileira (Real (R\$)), (CIF), por item, para o item cotado;
- 13.2 Especificação clara do item de acordo com este Termo de Referência;
- 13.3 Nos preços de cada produto deverão estar incluídos, obrigatoriamente, impostos, fretes, taxas e demais incidências;
- 13.4 Na cotação de preços e nos lances serão aceitos somente 02 (dois) dígitos após a vírgula
- 13.5 Para julgamento e classificação das propostas será adotado o critério de menor preço GLOBAL, observadas as especificações constantes no Termo de Referência;
- 13.6 O pagamento dos serviços será de forma mensal para a quantidade contratada em casa mês;

LOTE 01				
Item	Especificação	QTD Mensal		Valor Médio Total Mensal
1	Solução Voz em nuvem com ligações ilimitadas mais 14 aparelhos telefônicos com e sem fio	01		R\$ 1.273,33
2	Solução de segurança com caixa Firewall	01		R\$ 693,33
3	Soluções de conectividade (serviço banda larga em fibra ótica)	03		R\$ 524,90
4	Telefonia celular 4G/5G mobilidade	02		R\$ 129,30
5	Solução de wi-fi + Segurança integrada	02		R\$ 516,60
VALOR ESTIMADO MÉDIO MENSAL				R\$ 3.137,47
VALOR ESTIMADO MÉDIO ANUAL				R\$ 37.649,64

14. DAS OBRIGAÇÕES

14.1 OBRIGAÇÕES DA CONTRATANTE

- a) Exigir o cumprimento de todas as obrigações assumidas pela Contratada,




de acordo com as cláusulas contratuais e os termos de sua proposta.

- b) Comunicar oficialmente à CONTRATADA sobre quaisquer falhas verificadas na fiscalização do cumprimento dos serviços prestados.
- c) Notificar a Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção.
- d) Efetuar o pagamento devido pela execução do(s) serviço(s) dentro do prazo estipulado, desde que cumpridas todas as formalidades e exigências contratuais.
- e) Acompanhar as visitas, inspeções, reuniões solicitadas pela CONTRATADA.
- f) Prestar, por meio do Gestor do Contrato, as informações e os esclarecimentos pertinentes ao(s) serviço(s) contratado(s) que venham a ser solicitados pela CONTRATADA.
- g) Registrar os incidentes e problemas ocorridos durante a execução do Contrato.
- h) Proporcionar os recursos necessários, técnicos e logísticos, dentro dos locais de instalação dos equipamentos para que a CONTRATADA possa executar os serviços conforme as especificações estabelecidas no Termo de Referência.
- i) Permitir acesso dos empregados da CONTRATADA, desde que devidamente credenciados, às suas dependências para a realização dos serviços.
- j) Aplicar as sanções previstas, assegurando à CONTRATADA o contraditório e à ampla defesa.

14.2 OBRIGAÇÕES DA CONTRATADA

- a) Prestar os esclarecimentos que forem solicitados pelo CONTRATANTE, bem como dar ciência ao mesmo, imediatamente e por escrito, de qualquer anormalidade que verificar.
- b) Comunicar imediatamente ao CONTRATANTE qualquer alteração ocorrida na conta bancária, endereço e outras informações necessárias para recebimento de correspondências e pagamento.
- c) Responsabilizar-se pelo exato cumprimento de todas as obrigações e exigências decorrentes da legislação trabalhista e previdenciária, ficando claro inexistir entre seus empregados e o CONTRATANTE vínculo empregatício ou de qualquer outra natureza, razão pela qual correrão por conta exclusiva da CONTRATADA todos os ônus decorrentes de rescisões de contratos de trabalho e atos de subordinação de seu pessoal.
- d) Arcar com todos os encargos sociais trabalhistas, tributos de qualquer espécie que venham a ser devidos em decorrência da execução do serviço contratado, bem como custos relativos ao deslocamento e estada de seus profissionais, caso exista.
- e) Manter, durante a execução do contrato, em compatibilidade com as

obrigações assumidas, todas as condições de habilitação exigidas em razão da natureza das atividades prestadas e do certame licitatório.

- f) Fazer diagnóstico das falhas no serviço relatadas pelo CONTRATANTE dentro do prazo estipulado.
- g) Providenciar a recuperação de falhas na prestação do serviço, comunicadas pelo CONTRATANTE mantendo-o informado sobre as ações efetivadas até a completa normalização da prestação do serviço.
- h) Respeitar o sistema de segurança do CONTRATANTE e fornecer todas as informações solicitadas por ele.
- i) Credenciar junto ao CONTRATANTE um representante, para prestar esclarecimentos e atender às reclamações que porventura surgirem durante a execução do contrato.
- j) O CONTRATANTE não aceitará a transferência de responsabilidade da CONTRATADA para terceiros.
- k) Prestar o serviço contratado conforme especificações, prazos e demais condições estabelecidas no Termo de Referência.
- l) Utilizar melhores práticas, capacidade técnica, materiais, equipamentos, recursos humanos e supervisão técnica e administrativa, para garantir a qualidade do serviço e o atendimento às especificações contidas neste Contrato e no Termo de Referência.
- m) Reportar formal e imediatamente ao Gestor do Contrato quaisquer problemas, anormalidades, erros e irregularidades que possam comprometer a execução do(s) serviço(s)
- n) Atender e prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos da área de tecnologia da Informação do CONTRATANTE, referentes a qualquer problema detectado ou ao andamento de atividades previstas.
- o) Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o Contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas neste instrumento, caso os prazos, indicadores e condições não sejam cumpridos.
- p) Manter seus profissionais nas dependências do CONTRATANTE adequadamente trajados e identificados com uso permanente de crachá, com foto e nome visível.
- q) Manter-se, durante toda a execução do contrato, em conformidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na seleção.

15. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR



15.1. O prestador de serviço será selecionado por meio da realização do Procedimento de Seleção Simplificada, **que culminará com a seleção da proposta de menor preço total**, de acordo com a Lei Federal nº 14.341/2022 e conforme previsão estabelecida na Resolução nº 02 de 14 de setembro de 2023 – Regulamento de Compras e Contratações;

15.2. Os documentos exigidos, para fins de habilitação jurídica, são as CND's Federal, Estadual e Municipal e Cartão do CNPJ, que serão exigidas do vencedor do certame e deverão estar em situação negativa ou positiva com efeito de negativa, sendo motivo de desclassificação, a falta de uma delas e havendo a necessidade de contrato, o documento de constituição da empresa com identificação do responsável, que firmará o contrato, deverá ser apresentado.

15.3. Havendo empate a Amvale exercerá o direito de contratar quem melhor atender seus interesses.

16. PAGAMENTO

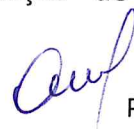
16.1. Os serviços contratados serão executados pelo valor global do contrato, conforme itens discriminados e pagos conforme relatório da execução do serviço.

16.2. O pagamento decorrente da concretização do objeto pelo Procedimento de Seleção Simplificada será efetuado mensalmente pelo Departamento Administrativo, por processo legal, em até 10 (dez) dias úteis do mês subsequente, após o recebimento da nota fiscal/fatura.

16.3. Os pagamentos à Contratada somente serão realizados mediante o efetivo e integral prestação dos serviços contratados, que será comprovado por meio de conferência e recebimento, por parte do representante da Amvale no momento da apresentação da NF.

16.4. A nota fiscal deverá ser emitida pela Contratada em inteira conformidade com as exigências legais contratuais, especialmente as de natureza fiscal.

16.5. O gestor e/ ou fiscal e/ ou o Departamento Administrativo da AMVALE, identificando qualquer divergência na nota fiscal, deverá devolvê-la à Contratada, para que sejam feitas as correções necessárias, sendo que o prazo estipulado acima será contado somente a partir da reapresentação do documento devidamente sanados os vícios.



16.6. O pagamento devido pela AMVALE será efetuado por meio de transferência eletrônica (TED, PIX, TEV) ou boleto bancário com os dados a serem informados pela Contratada ou, eventualmente, por outra forma que vier a ser convencionada entre as partes.

16.7. Uma vez paga a importância discriminada na nota fiscal, a Contratada dará a AMVALE plena, geral e irretratável quitação dos valores nela discriminados, para nada mais vir a reclamar ou exigir a qualquer título, tempo ou forma.

16.8. Todo o pagamento que vier a ser considerado contratualmente indevido será objeto de ajuste nos pagamentos futuros ou cobrados da Contratada

16.9. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

17. DO ENVIO DA PROPOSTA:

17.1. A proposta deverá ser encaminhada pelo e-mail oficial de compras da Amvale: comprasamvale@gmail.com ou entregue fisicamente na sede da Amvale na Rua Dr. Hildebrando Pontes nº 291, Bairro Morada das Fontes, Uberaba – MG.

17.2. A proposta deverá ser datada e ter prazo de validade de no mínimo 15(quinze) dias;

17.3. Na proposta deverá constar todos os dados da empresa participante do certame (razão social, endereço, CNPJ, telefone etc.);

17.4. A proposta deverá ser enviada pelo e-mail oficial da empresa, preferencialmente por meio de documento assinado enviado anexo ao e-mail.

18. DO PRAZO PARA ENTREGA DA PROPOSTA:

18.1. A partir da data da publicação, o prazo é de 3 (três) dias, para o envio das propostas.

18.2. Para a contagem dos prazos, exclui-se o dia da publicação e inclui-se o

último, contados em dias úteis.

18.3. O e-mail se conta até as 23h:59min do envio e fisicamente dentro do horário das 8h às 17h30min do último dia do prazo.

18.4. O período de recebimento das propostas deste Termo de Referência será **de 30/07/2026 até 04/08/2026.**

18.5. Uma vez enviada a proposta, os fornecedores não poderão retirá-la, substituí-la ou modificá-la.

19. DA FUNDAMENTAÇÃO LEGAL

19.1. O Regulamento de Compras e Contratações da Amvale, aprovado pela Resolução Interna nº 02/2023, regulamenta os procedimentos e estabelece direitos e obrigações entre as partes, e pode ser encontrado no site oficial da Amvale: <http://amvale.org.br> e os participantes do certame, quando da apresentação da proposta, se dão por ciente de todo o seu conteúdo.

Uberaba – MG, 29 de julho de 2026.



Marli de Souza Pereira
Diretora Administrativa
AMVALE



Vanessa Silva Faria
Superintendente
AMVALE