1. DA ESPECIFICAÇÃO TÉCNICA PARA SOLUÇÃO SD-WAN
   1.1. Toda a solução entregue deve suportar, no mínimo, os protocolos de roteamento dinâmicos BGP e OSPF, para pilha IPv4 (BGP e OSPF) e para a pilha IPv6, no mínimo em BGP;
   1.2. Toda a solução deve estar implementada pelo protocolo cliente NTP (Network Time Protocol), conforme especificação RFC 1305;
   1.3. A CONTRATADA deverá fornecer à CONTRATANTE a acesso com privilégios de leitura/escrita com perfil administrador global de cada equipamento após o aceite da instalação dos acessos;
   1.4. Não serão consideradas, como ocorrências de indisponibilidade dos acessos, falhas ocasionadas por erros cometidos pelo corpo técnico da CONTRATANTE.
   1.5. Em casos de falhas ocasionadas por erros cometidos pelo corpo técnico da CONTRATANTE, não haverá aplicação de penalidades e glosas.
   1.6. Por acesso entende-se permissão de ingresso utilizando interface web utilizando https, linha de comando utilizando ssh, possibilidade de obtenção de dados via SNMPv3 e syslog. A CONTRATADA deverá permitir que os links, fornecidos por empresas distintas, sejam conectados nos equipamentos da CONTRATADA;
   1.7. As configurações dos links serão de responsabilidade da CONTRATADA. Os parâmetros de endereços lógicos, do link redundante, serão repassados pela CONTRATANTE;
   1.8. Deverá suportar a arquitetura local (instalada na sede da contratante), baseada em nuvem com backbone ou em nuvem;
   1.9. Deve ser capaz de monitorar a latência, o jitter e o descarte de pacotes em cada um dos links individualmente;
   1.10. Os equipamentos deverão ser dimensionados, fornecidos, instalados e configurados, pela CONTRATADA, garantindo-se o desempenho e os níveis de serviços contratados;
   1.11. Para melhor gerência, eficácia na operação, diminuir a curva de aprendizado e complexibilidade para a operação, os appliances SD-WAN deverão ser da mesma marca, promovendo ainda a padronização da solução e gerência única.
2. DO CONTROLADOR/ORQUESTRADOR/SOFTWARE DE GERÊNCIA:
   2.1. A CONTRATADA deverá fornecer à CONTRATANTE a acesso com privilégios de leitura/escrita com perfil administrador global de após o aceite da instalação dos acessos;
   2.2. Deve ser capaz de realizar a redistribuição do balanceamento do tráfego entre os links de comunicação utilizados, em caso de falhas nesses links, ou de acordo com as políticas de qualidade pré-definidas na solução;
   2.3. Deve ser possível criar políticas para a modelagem do tráfego e seleção de melhor caminho de acordo com os seguintes parâmetros:
      2.3.1. IP de Origem;
      2.3.2. IP de Destino;
      2.3.3. Porta TCP/UDP de Destino;
      2.3.4. plicação de camada 7 utilizada (O365 Exchange, SAS, Dropbox, Box, Zoom e etc);
      2.3.5. VLAN ou subnet de origem.
   2.4. Deve ser possível definir qual link atuará como principal;
   2.5. Deve ser possível definir qual link atuará como backup;
   2.6. A solução deverá suportar convergência rápida, em menos de 1 (hum) segundo, de tráfego de um túnel ao outro sem perda de sessões TCP/UDP previamente estabelecidas;
   2.7. A solução deverá permitir o balanceamento de pacotes de uma mesma sessão entre dois ou mais links;

2.8. Deve implementar protocolo de coleta de informações de fluxos que circulam pelo equipamento, como Netflow, sFlow, IPFIX ou similar, contemplando no mínimo as seguintes informações:
  2.8.1. IP de origem/destino;
  2.8.2. Parâmetro "protocol type" do cabeçalho IP;
  2.8.3. Porta TCP/UDP de destino;
  2.8.4. Interface do equipamento em que o tráfego foi identificado.
2.9. Deve permitir a verificação de disponibilidade do link diretamente pelos pacotes de controle SD-WAN, no máximo, a cada 500ms e assim garantir a informação de latência, jitter e perda de pacotes de todos os enlaces existentes, sem a necessidade de probe adicional HTTP para tomada de decisão de direcionamento de tráfego;
2.10. Deve possuir solução de gerenciamento que permita realizar configurações em todos os appliances SD-WAN da rede de forma centralizada;
2.11. O software de gerenciamento deve fornecer, no mínimo, as seguintes informações de cada link dos equipamentos SD-WAN da rede:
  2.11.1. Taxa de transmissão e recepção de dados;
  2.11.2. Status do healthcheck ou status do link;
  2.11.3. Jitter;
  2.11.4. Latência;
  2.11.5. Perda de pacotes.
2.12. A solução deverá ser entregue com todos os componentes da solução para o seu pleno funcionamento e requisitos técnicos definidos para esta solução e devidamente licenciados.

3. EQUIPAMENTOS SD-WAN- REQUISITOS GERAIS:
3.1. Todos os equipamentos e links devem suportar tanto IPv4 quanto IPv6, sendo que este último deve estar implementado de forma nativa em pilha dupla;
3.2. Deverão suportar o tráfego da banda completamente ocupada sem degradação do desempenho, atendendo aos níveis de serviço pretendidos. Para isso deverão apresentar configuração de memória, CPU e capacidade de vazão de dados compatíveis com os circuitos contratados;
3.3. Deverão possuir fonte de alimentação com chaveamento automático de tensão de entrada 110/220 VAC a 60 Hz;
3.4. Os equipamentos SD-WAN deverão possuir duas fontes de energia redundantes;
3.5. Deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
3.6. Todos os equipamentos SD-WAN devem ser do mesmo fabricante e deverão disponibilizar os recursos mínimos explicitados neste Termo de Referência;
3.7. A determinação do mesmo fabricante para todos os equipamentos visa otimizar o treinamento sobre os equipamentos, simplificar procedimentos de configuração, gestão, operação, monitoramento, resolução de problemas e principalmente garantir a compatibilidade entre eles;
3.8. A interligação entre os equipamentos de acesso até os datacenters não deve sofrer gargalo ou enfileiramento durante a transmissão de dados em decorrência de compartilhamento do link ou mau dimensionamento da estrutura de backbone, ou seja, deve-se garantir o tráfego concomitante de todos os links remotos sem perda de performance, aumento no delay, aumento no jitter ou implementação de erros de rede, devendo os parâmetros estarem dentro dos especificados no **Anexo B- Caderno de Métricas;**
3.9. A instalação, manutenção, além das gerências de falhas de todos os equipamentos de telecomunicações e infraestrutura envolvidos na solução SD-WAN, serão de responsabilidade da CONTRATADA;

3.10. A solução de Rede Privada proposta deverá permitir o tráfego de aplicações corporativas (sistemas de informação, troca de arquivos, correio eletrônico, intranet, banco de dados, chamadas VoiP, videoconferências, streaming de vídeo/áudio, CFTV, IPTV, etc.), utilizando a família de protocolos TCP/IP, para a interligação das redes LAN de todas as localidades relacionadas no Anexo A.1- Relação de Demanda e Anexo F- Relação de endereços e velocidades.

3.11. O SD-WAN deve suportar os seguintes tipos de conexões WAN: ADSL/DSL, Cable Modem com Ethernet ou fibra, LT /3G/4G/5G, MPLS, Link de rádio e Link satélite desde que a sua terminação permita conectividade com interfaces ethernet.

3.12. Realizar balanceamento de tráfego de saída entre os links de Wan primários;

3.13. Deverá implementar a criação de tuneis criptografados de forma dinâmica entre os sites;

3.14. Deverá implementar controle tráfego por aplicação;

3.15. Deverá identificar impactos e riscos por aplicação;

3.15.1. Identificação de Aplicações: Detectar, classificar e monitorar o tráfego gerado por diferentes aplicações (e.g., Microsoft Teams, Zoom, aplicativos de e-mail, etc.) em tempo real.

3.15.2. Avaliação de Impactos: Identificar como o tráfego de cada aplicação afeta os recursos da rede (como largura de banda, latência ou perdas de pacote) e seu impacto sobre o desempenho geral da infraestrutura.

3.15.3. Avaliação de Riscos: Mapear potenciais vulnerabilidades de segurança relacionadas a cada aplicação, o nível do risco.

3.16. Deve possuir capacidade para utilizar, pelo menos 3 (três) links de WAN, sendo no mínimo 2 (dois) links simultâneos;

3.17. A solução deve permitir operar em caráter de diagrama hub-spoke;

3.18. Distribuição de tráfego com balanceamento de sessão entre os circuitos existentes;

3.19. Distribuição orientada a qualidade, o dispositivo deve validar o melhor caminho disponível utilizar deste path para manter sessões ativas, caso o melhor caminho entre em degradação por fatores anômalos o dispositivo deverá entender estes fatores e distribuir para os demais circuitos existentes;

3.20. Permitir que a escolha do link WAN de saída seja influenciada por regras definidas pelo administrador de rede da CONTRATANTE e dinamicamente. As regras devem permitir ao menos um dos parâmetros a seguir ou combinação destes:

3.20.1. Endereço IP de origem e/ou destino;

3.20.2. Subredes de origem e/ou destino;

3.20.3. Métricas de Jitter, latência e perda de pacotes por aplicação;

3.20.4. Status da porta de WAN primários (UP ou DOWN);

3.20.5. Suportar o protocolo de tunelamento GRE (General Routing Encapsulation- RFC 2784);

3.20.6. A solução deve ter um tempo máximo de failover e failback de 300 segundos;

3.20.7. Deve permitir topologia da rede WAN malha completa (full mesh);

3.20.8. A solução de SD-WAN deverá ser integrada no próprio appliance, não sendo aceito quaisquer componentes adicionais com esta função.

3.20.9. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de verificações de saúde dos links WAN, permitindo testes de resposta por PING, HTTP, TCP/UDP ECHO, DNS e TWAMP.

3.20.10. A solução de SD-WAN deve suportar o encapsulamento de VRFs entre HUB e Spokes, segregando logicamente a tabela de roteamento nas VRFs entre tuneis IPSec.

3.20.11. A solução de SD-WAN deve suportar a funcionalidade de route leaking entre as VRFs permitindo comunicação entre diferentes tabelas de roteamento, segmentos e acesso internet local.

3.20.12. A solução deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote ou sessão entre eles.

3.20.13. A solução deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões.

3.20.14. A solução deve suportar o anúncio de diferentes comunidades BGP de acordo com o nível de serviço (SLA), evitando assim que o concentrador precise monitorar todos os pontos remotos.

3.20.15. A Solução SD-WAN deverá analisar o fluxo do tráfego em tempo real e realizar a duplicação de pacotes através de regras, distribuir em múltiplos links simultaneamente, realizar a reordenação dos pacotes no outro extremo.

3.20.16. A solução deve possuir capacidade de agregar e balancear, no mínimo, 3 circuitos de dados físicos e 6 lógicos.

3.20.17. A solução deve ser capaz de criar VPN "Full-Mesh" em interface gráfica, de forma automática, sem que o administrador precise configurar site por site.

3.20.18. Deverá permitir habilitar e desabilitar túneis de VPN IPSec a partir da interface gráfica da solução, facilitando o processo de resolução de problemas;

3.20.19. Deve suportar VxLAN sobre túnel IPSec.

3.20.20. Solução deverá ser capaz de prover uma arquitetura similar ao conceito de Auto Discovery VPN – ADVPN, funcionalidade esta que tem o intuito de dinamicamente viabilizar que túneis sejam estabelecidos entre duas localidades remotas, sem necessidade de o tráfego transitar pelo ponto central conhecido por HUB.

3.20.21. Deverá reconhecer, no mínimo, 5000 (cinco mil) aplicações com base na camada 7 do modelo OSI;

3.20.22. Deverá ser capaz de identificar aplicações nas políticas de SD-WAN independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;

3.20.23. Para tráfego criptografado SSL, deve de-criptografar os pacotes a fim de possibilitar a leitura do conteúdo do pacote para checagem de assinaturas de aplicações conhecidas pelo fabricante;

3.20.24. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

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

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

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

3.20.28. Deve ser possível copiar o valor DSCP de uma sessão original visando utilizá-lo na resposta de retorno.

3.20.29. Deve permitir configurar o código de DiffServ (DSCP) do pacote ESP do túnel IPSec;

3.20.30. Deverá permitir marcar com DSCP os testes de link para obter uma avaliação mais realista da qualidade de um determinado link;

4. EQUIPAMENTOS SD-WAN – REQUISITOS DE SEGURANÇA:

4.1. Possibilitar filtragem de pacotes através de listas de controle de acesso baseadas, no mínimo, nas seguintes informações: endereço da camada de rede (IPv4 e IPv6) e portas da camada de transporte;
4.2. O tráfego internet entre a unidade remota e o concentrador SD-WAN, deve ser protegido via túneis VPN IPSEC. Inicialmente toda a saída de Internet será trafegada pelos links de alta velocidade contratados pela CONTRATANTE;
4.3. Deve implementar, no mínimo, VPN IPSec com capacidade de implementar túneis site-to-site do tipo hub-and-spoke;
4.4. Deve permitir o estabelecimento do túnel utilizando uma "chave secreta" ou certificados digitais;
4.5. Deve implementar IKEv1 e IKEv2;
4.6. Suportar no mínimo DIFFIE HELLMAN GROUP:
4.6.1. Diffie-Hellman Group 2 (1024-bit);
4.6.2. Diffie-Hellman Group 5 (1536-bit);
4.6.3. Diffie-Hellman Group 14 (2048-bit).
4.7. Deve oferecer suporte pelo menos aos seguintes algoritmos de criptografia: AES- 128-bit e AES-256-bit;
4.8. Deve oferecer suporte pelo menos aos seguintes algoritmos de autenticação: SHA- 1, SHA-256, SHA-384, SHA-512.
4.9. A solução deverá estar devidamente licenciada por 36 (trinta e seis) meses para atender as funções, funcionalidades e serviços para no mínimo: SD-WAN, Controle de Aplicações, Firewall, VPN site-to-site e client-to-site, Filtro de Conteúdo Web, Prevenção de ameaças, Garantia e suporte remoto diretamente com o fabricante na modalidade de 24x7
4.10. A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
4.11. A solução SD-WAN deve suportar micro-segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.

5. **EQUIPAMENTOS SD-WAN – REQUISITOS DE GERÊNCIA:**
5.1. O equipamento deverá ser compatível com Controlador/orquestrador (software de gerência) fornecido pela CONTRATADA, sendo que a comprovação deverá ser realizada pela matriz de compatibilidade ou da mesma marca do CONTROLADOR/ORQUESTRADOR;
5.2. A CONTRATADA deverá fornecer à CONTRATANTE a acesso com privilégios de leitura/escrita com perfil administrador após o aceite da instalação dos acessos;
5.3. Não serão consideradas, como ocorrências de indisponibilidade dos acessos, falhas ocasionadas por erros cometidos pelo corpo técnico da CONTRATANTE.
5.4. Em casos de falhas ocasionadas por erros cometidos pelo corpo técnico da CONTRATANTE, não haverá aplicação de penalidades e glosas.
5.5. Por acesso entende-se permissão de ingresso utilizando interface web utilizando https, linha de comando utilizando ssh, possibilidade de obtenção de dados via SNMPV3 e syslog.

6. **EQUIPAMENTOS SD-WAN – REQUISITOS DE PERFORMANCE:**
6.1. O Equipamento de Acesso deverá ser dimensionado para operar com carga máxima de 70% para a CPU e memória, mesmo quando utilizando a capacidade total da banda. Caso a recomendação do fabricante aponte que a carga máxima de CPU e memória recomendada seja inferior ao indicado neste Termo, a recomendação do fabricante deverá prevalecer;
6.2. Deverá suportar garantia de performance contra degradação de rede para aplicativos hospedados em Data Center próprio e também aqueles consumidos como serviço na nuvem (Skype, O365, Dropbox, Zoom e etc);

6.3. A solução deverá garantir performance de aplicações que utilizam VPN nos sites remotos e serviços de nuvem (SaaS);
6.4. Deverá garantir performance para os aplicativos em um cenário de link de transporte duplo quando os dois links estão degradados;
6.5. Deverá garantir performance para os aplicativos em um cenário de link de transporte único quando este único link está degradado;
6.6. A Solução deverá possuir mecanismo de QoS para proteger o tráfego das aplicações prioritárias do cliente quanto tiver congestionamento na filial;
6.7. A solução deve implementar algoritmo de correção de erros (FEC – Forward Error Correction), para melhor eficiência de aplicações real time;
6.8. A solução deverá implementar mecanismo de proteção contra degradação total de todos os links por motivo de variação de latência.

7. DO CONCENTRADOR SD-WAN:

7.1. Trata-se do equipamento SD-WAN que será instalado no Datacenter da CONTRATANTE, a fim de comunicar com os acessos remotos por meio de VPN e internet;
7.2. Os Concentradores serão instalados nos dois Datacenters Corporativos (DC) do Governo do Estado de Goiás para concentrar o tráfego de acesso das Unidades Remotas às Aplicações Corporativas (APPC) do Estado de Goiás através de uma Conexão Central (CC) à Internet;
7.3. Os CONCENTRADORES deverão ser instalados nos endereços abaixo, atendendo todas as especificações deste Termo de Referência.

Local	Endereço
DC1	Av. Ver. José Monteiro, 2233 - Nova Vila, Goiânia - GO, 74653-900
DC2	Av. Eng. Atílio Corrêa Lima, 1875 - Cidade Jardim, Goiânia - GO, 74425-030

7.4. As conexões Centrais conectadas a cada Data Center (DC1 e DC2) deverão ser interligadas a POPs distintos da CONTRATADA, sem sobreposição de rotas ou ponto único de falha.
7.5. Todos os equipamentos, materiais, mão de obra, serviços e demais custos necessários, para interligação dos links até o CONCENTRADOR da CONTRATANTE são de responsabilidade da CONTRATADA.
7.6. A CONTRATADA deverá apresentar previamente plano de execução contendo o detalhamento da rota (kmz) desde o POP, Ponto de Entrada e chegada aos respectivos Data Centers (DC1 e DC2).
7.7. Os Pontos de Entrada dos links nas dependências da dos Data Centers são de responsabilidade da CONTRATADA e deverão ser previamente acordadas e aprovadas pela Unidade Central de TI. Evitando sobreposição de rotas e/ou ponto único de falhas em comum entre as CONTRATADAS (primária e secundária).
7.8. Caso necessário, a CONTRATADA deverá realizar os ajustes necessários para adequação ou criação de Pontos de Entrada, incluindo cabeamentos, tubulações, alvenaria, perfuração por método não destrutivo e etc.
7.9. Deve ser montável em rack com tamanho 19 polegadas, conforme especificação EIA-310-D e vir com todos os seus acessórios, bandeja se necessário, para a sua completa instalação, inclusive cabos ópticos, transceivers, Direct Atach Cables, todos compatíveis com o equipamento da Contratante;
7.10. O equipamento destinado ao Layer 3 deverá ser entregue com pelo menos 2 (duas) interfaces de rede LAN, e 2 (duas) interfaces de rede WAN;

7.11. Para a interligação com a rede dos DATACENTERs Coorporativos, cada membro do cluster ou cada switch do cluster deverá ter, no mínimo, quatro interfaces de um dos padrões abaixo:
  7.11.1. 10GBASE-SR;
  7.11.2. 25GBASE-SR;
  7.11.3. 40GBASE-SR4;
  7.11.4. 100GBASE-SR4;
7.12. A solução deve ser fornecida com todos os transceivers de curto alcance correspondentes às interfaces de solicitadas;
7.13. A solução deve ser fornecida com todos os cordões ópticos duplex multimodo LC-LC OM4 10(dez) metros, referente aos transceivers entregues;
7.14. Deverá suportar interligação, por meio de VPN, dos links remotos, conforme as especificações técnicas de segurança, ao concentrador SD-WAN;
7.15. Suportar Balanceamento entre Concentradores instalados em Datacenters Diferentes ou entre caixas ou clusters ou similar, sem queda das VPNs ativas;
7.16. A interligação interna do Roteador Concentrador com a Rede WAN deverá ser feita através de cabos ópticos, transceivers, Direct Atach Cables (desde que compatível com o equipamento da Contratante) sendo que todo e qualquer acessório necessário para interligação aos equipamentos da CONTRATANTE, deverão ser fornecidos pela CONTRATADA;
7.17. Deverá ser disponibilizado ao CONTRATANTE, "string/comunidade SNMPV3", para todas as versões de SNMPV3 existentes nos equipamentos, com privilégio de consulta a todas as variáveis e valores, em todos os equipamentos roteadores implantados;
7.18. A CONTRATADA deverá garantir que o trafego de dados seja protegido de acesso por terceiros;
7.19. A comunicação deverá ser Full-duplex, com as velocidades garantidas, em cada sentido da comunicação, conforme estabelecidos no **Anexo A.1- Relação de Demanda;**
7.20. A configuração em alta disponibilidade deve sincronizar:
  7.20.1. Sessões;
  7.20.2. Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QoS e objetos de rede;
  7.20.3. Associações de Segurança das VPNs;
  7.20.4. Tabelas FIB;
7.21. Deve ser capaz de realizar failover e failback automaticamente dos estados dos links entre os concentradores de forma transparente ao usuário.
7.22. O SD-WAN instalado no datacenter deverá suportar, no mínimo, 100(cem) VPNs do Tipo Site-to-Site.
7.23. Deve suportar, no mínimo, 10.1 Gbps de throughput de Controle de Aplicação.
7.24. Deve suportar, no mínimo, 20.2 Gbps de throughput de VPN IPSec.

8. **EQUIPAMENTOS SD-WAN – REQUISITOS DE REDE/INSTALAÇÃO:**
8.1. Deve possuir pelo menos 4 (quatro) interfaces Gigabit Ethernet (10/100/1000Base-T) sendo que todas sejam do tipo LAN/WAN, para que a CONTRATANTE possa configurá-las de acordo com sua necessidade e conveniência.
8.2. 1 (uma) para conexão para rede móvel. Esta conexão poderá ser USB para instalação de um modem ou suportar a instalação do chip da operadora direto no equipamento;
8.3. O SD-WAN instalado nas localidades remotas deverá suportar, no mínimo, 2(dois) VPNs do Tipo Site-to-Site;
8.4. Deve possuir capacidade de agregar e balancear, no mínimo, 2 circuitos de dados utilizando uma interface dedicada para cada circuito;

8.5. Deve ser capaz de balancear o tráfego das aplicações entre múltiplos links simultaneamente;
8.6. Deve ser capaz de realizar failover e failback automaticamente dos estados dos links, de forma transparente para o usuário;
8.7. Deve ser capaz de monitorar a latência, o jitter e o descarte de pacotes em cada um dos links individualmente;
8.8. Deve possuir serviço de DHCP relay ou UDP Helper, de forma a disponibilizar endereço IPs mesmo que pela WAN/SD-WAN;
8.9. Deve ser capaz de implementar rotas estáticas;
8.10. O equipamento remoto deve suportar topologia de alta disponibilidade, permitindo instalação com dois appliances concentradores SD-WAN;
8.11. SD-WAN TIPO I
8.11.1. Deve suportar, no mínimo, 7.3 Gbps de throughput de Threat Prevention.
8.11.2. Deve suportar, no mínimo, 14.6 Gbps de throughput de VPN IPSec.
8.11.3. Deve suportar, no mínimo, 7.3 Gbps de throughput de Inspeção SSL.
8.11.4. Deve suportar, no mínimo, 7.3 Gbps de throughput de Controle de Aplicação.
8.11.5. Possuir no mínimo 04 (quatro) interfaces 10 Gigabit SFP+ (ou superior);
8.11.5.1. A solução deve ser fornecida com todos os transceivers SFP+ de curto alcance correspondentes às interfaces de 10 Gbps solicitadas;
8.11.6. Possui no mínimo 02 (duas) interfaces 40 Gigabit QSFP28 (ou superior);
8.11.7. A solução deve ser fornecida com todos os transceivers QSFP28 de curto alcance correspondentes às interfaces de 40 Gbps solicitadas;
8.11.8. A solução deve ser fornecida com todos os cordões ópticos duplex multimodo LC-LC OM4 10(dez) metros, referente aos transceivers entregues;
8.11.9. Deve possuir suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
8.11.10. O modo de Alta Disponibilidade deve sincronizar:
8.11.10.1. Todas as sessões;
8.11.10.2. Todas as associações de Segurança das VPNs;
8.11.10.3. Todas as assinaturas de Antivírus, Antispyware, Aplicações Web e IPS;
8.11.10.4. Todas as configurações;
8.11.11. Deve realizar monitoramento de falha de link;
8.11.12. A solução deverá disponibilizar uma ferramenta onde o fabricante disponibilize Hotfixes de segurança e upgrades de versão para instalação simples e com zero-downtime;
8.11.13. A solução deve suportar fazer port-aggregation de interfaces de firewall suportando o protocolo 802.3ad para aumento de throughput e alta disponibilidade de interfaces;
8.12. SD-WAN TIPO II
8.12.1. Deve suportar, no mínimo, 2 Gbps de throughput de VPN IPSec.
8.12.2. Deve suportar, no mínimo, 500 Mbps de throughput de Inspeção SSL.
8.12.3. Deve suportar, no mínimo, 1 Gbps de throughput de Controle de Aplicação.
8.13. SD-WAN TIPO III
8.13.1. Deve suportar, no mínimo, 400 Mbps de throughput de VPN IPSec.
8.13.2. Deve suportar, no mínimo, 100 Mbps de throughput de Inspeção SSL.
8.13.3. Deve suportar, no mínimo, 100 Mbps de throughput de Controle de Aplicação.

9. DA SOLUÇÃO DE GERENCIAMENTO E ATIVIDADES DE PROATIVIDADE:

9.1. Considerando a forte relação de dependência entre os serviços prestados pelo CONTRATANTE e a qualidade, capacidade e disponibilidade da transmissão de dados entre suas unidades e o Datacenter, a CONTRATADA deverá realizar monitoramento 24/7 (24 horas por dia, 7 dias por

semana) dos itens contratados, a fim de facilitar a identificação de falhas e minimizar o tempo de recuperação no caso de incidentes;

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

9.3. Fazer a gestão dos circuitos que a CONTRATADA tenha contratado diretamente à outras Operadoras ou Provedores;

9.4. A CONTRATATANTE informará à CONTRATADA quais links de dados estão interligados à solução CONTRATADA, os contatos necessários, e-mail ou telefone, que será disponibilizado pela CONTRATANTE;

9.5. Quando a CONTRATADA detectar algum evento ou falha de links conectados à sua solução, deverá abrir chamado(s) às empresas dos links, independentemente se estes façam parte ou não de sua solução;

9.6. Após a abertura de chamado, a CONTRATADA enviará ou disponibilizara o protocolo à CONTRATANTE, para que esta possa acompanhar o atendimento do SLA;

9.7. A CONTRATADA deverá prover a informação do restabelecimento do link, seja por e-mail enviando à CONTRATANTE ou disponibilizado pela própria solução;

9.8. A CONTRATANTE e a CONTRATADA poderão definir ou redefinir fluxos para que o acompanhamento ou restabelecimento do(s) link(s) afetado(s) seja(m) realizados o mais breve possível.

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

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

9.11. O acesso deverá ser via web padrão HTTP e suportar a HTTPS;

9.12. A Solução de Gerência da Rede deverá permitir adicionar a nomenclatura conhecida pelo CONTRATANTE para os recursos gerenciados;

9.13. Os serviços requerem a utilização de protocolo SNMPV3 em CPEs com MIBs homologadas pela plataforma e é necessário o fornecimento de acesso Read à Community String dos roteadores e CPEs, SDWAN e FW de Segurança a serem gerenciados;

9.14. Deverá implantar na rede o NAT (Network Address Translation) ou utilizar nos roteadores os endereços de loopback que serão definidos pela gerencia dos serviços.

9.15. No caso de gerenciamento de elementos onde se faça necessária instalação de agentes proprietários para captura das informações de gerenciamento solicitadas, este agente deverá ser “passivo”, ou seja, a plataforma central deve controlar a coleta e o pooling das informações, sendo assim o agente deve aguardar esta requisição para retornar as informações na rede;

9.16. Os agentes devem possuir flexibilidade de parametrização de coleta para que o administrador tenha liberdade de inserir novas métricas ou propriedades de coleta para os elementos monitorados;

9.17. A solução deverá incluir uma ferramenta capaz de monitorar, gravar e gerar relatórios relativos ao atendimento dos requisitos mínimos de qualidade e disponibilidade previstos no Anexo B - Caderno de Métricas e no Anexo C - Acordo de Nível de Serviço, deste Termo de Referência, permitindo consultas dos parâmetros dos equipamentos ativos, e enviar alertas aos responsáveis técnicos da CONTRATANTE em caso de inconformidades ou falhas;

9.18. A solução deverá comprovar o atendimento e implementação de todas as métricas e níveis de serviço acordados nesse Termo e seus anexos. Tais comprovações deverão ser feitas por meio de

monitoramento em tempo real, via software e equipamentos, utilizando protocolos como NQA (Network Quality Assurance) ou IP-SLA;

9.19. A ferramenta de gerenciamento e monitoramento deverá ser implantada no Centro de Operações de Rede (NOC) da CONTRATADA. Essa ferramenta poderá ser composta de softwares licenciados ou não (somente quando utilizar softwares livres), possibilitando o acesso e monitoramento de todos os ativos adquiridos pela CONTRATANTE bem como a aferição dos indicadores do Anexo B - Caderno de Métricas, além da geração de relatórios de eventos e de quaisquer parâmetros monitorados e gravados;

9.20. A CONTRATADA deverá disponibilizar, ao corpo técnico da CONTRATANTE, acesso à ferramenta de monitoramento, permitindo acesso de leitura a todos os parâmetros de monitoramento fornecidos pelo Dashboard da Solução, incluindo indicadores e alertas;

9.21. Os serviços do Gerenciamento que requerem a utilização de protocolo SNMPV3 em CPEs deverão ser compatíveis com as Community String dos roteadores e CPEs, SDWAN ou FW de Segurança a serem gerenciados;

9.22. Além das especificações contidas no Anexo B- Caderno de Métricas, a solução de Gerenciamento deve possuir flexibilidade de parametrização de coleta para que o administrador tenha liberdade de inserir novas métricas ou propriedades de coleta para os elementos monitorados.

9.23. A CONTRATADA deverá justificar tecnicamente o não atendimento da inclusão, o qual poderá ser acatada ou não pela CONTRATANTE;

9.24. ferramenta de gerenciamento e monitoramento deverá manter o histórico dos parâmetros monitorados por, no mínimo 12 (doze) meses;

9.25. O sistema de monitoramento deverá ser capaz de mostrar de forma transparente o tratamento de eventos, visualizando os parâmetros especificados neste TR e em seus anexos.

9.26. Deverá conter, também, informações online, com atraso de no máximo 5 minutos, da topologia da rede e exibição de relatórios de disponibilidade, indicadores do Anexo B- Caderno de Métricas;

9.27. A solução de monitoramento fornecida pela CONTRATADA deverá incluir funcionalidades acessíveis via web pelo CONTRATANTE, contendo no mínimo com as seguintes facilidades:

- 9.27.1. Nome da CONTRATANTE;
- 9.27.2. Identificação do link;
- 9.27.3. Nome da CONTRATANTE;
- 9.27.4. Velocidade do link;
- 9.27.5. Tipo de Link (Rede Governo, IP simétrico ou IP assimétrico)
- 9.27.6. Disponibilidade do link em %;
- 9.27.7. Erros e retramissão em %
- 9.27.8. Perda de Pacotes em %
- 9.27.9. Média de latência no período em milissegundos;
- 9.27.10. Valor em reais;

9.28. A CONTRATANTE poderá, a seu critério, solicitar a Média de latência no período contabilizando apenas dias úteis e horário comercial;

9.29. Atendimento ao acordo de nível de serviço previsto no contrato (Sim ou Não).

9.30. Desconto para cada link em reais;

9.31. A solução deverá ser capaz de emitir relatório para a CONTRATANTE.

9.32. O relatório também poderá ser exportado no formato XLSX ou CSV de acordo com definição da CONTRATANTE.

9.33. O resultado do relatório proporcionara informações importantes para identificação das métricas de SLAs e necessidades de abatimento de valores a serem aplicados em faturas futuras subsequente ao período analisado.
9.34. A Solução deverá ter a capacidade de customizar o horário de monitoramento de acordo com a necessidade.
9.35. Visualizar alarmes;
9.36. Taxa de ocupação do link;
9.37. Visualizar eventos gravados e em andamento;
9.38. Visualizar erros instantâneos e ocorridos ao longo do tempo (minutos, horas, dias, semanas e mês);
9.39. Visualização da utilização de memória e CPU dos Roteadores;
9.40. Visualização de dados para gestão do Service Level Agreement- SLA (Acordo de Nível de Serviço) fornecido por meio do acompanhamento sistemático (diário) dos índices de disponibilidade e desempenho da rede CONTRATADA;
9.41. Enviar alertas para a equipe técnica da CONTRATANTE, via e-mail e telefone, que serão fornecidos na reunião de alinhamento.
9.42. Todas as medições supracitadas deverão ser realizadas a partir do Concentrador até a porta LAN do CPE da unidade remota ou vice-versa;
9.43. Havendo divergências injustificáveis nos índices de SLA colhidos entre a CONTRATADA e CONTRATANTE prevalecerá a da CONTRATANTE.

10. DO MONITORAMENTO:

10.1. CONTRATADA deverá atuar de forma proativa, monitorando permanentemente o estado de todos os equipamentos da solução de SD-WAN, bem como de todos os circuitos de comunicação de dados que serão conectados à solução, abrindo imediatamente a solicitação de reparo do circuito de comunicação de dados ou do equipamento, em caso de falhas, previsão de falha, degradação de desempenho ou evento que leve a indisponibilidade ou degradação da rede;
10.2. A CONTRATADA deverá antecipar-se aos problemas que possam ocorrer na rede, garantindo a qualidade do serviço estabelecida no Anexo C- Acordo de Nível de Serviço, realizando de maneira proativa a abertura, acompanhamento e fechamento de chamados técnicos;
10.3. O processo de recuperação de falhas deverá ser iniciado de maneira proativa pela CONTRATADA, imediatamente após qualquer falha, independentemente da abertura do chamado por parte do CONTRATANTE ou contato telefônico da CONTRATADA com a unidade remota;
10.4. A CONTRATANTE, em caso de dúvidas ou verificações, deverá entrar em contato com a unidade remota ou equipe técnica, via telefone ou e-mail, sem prejuízo ao Acordo de Nível de Serviço e as atividades de recuperação de falhas, que devem seguir de maneira proativa;
10.5. Caberá à CONTRATADA identificar falhas ou degradação da solução SD-WAN e de cada circuito de qualquer natureza, e informar ao Gestor do Contrato ou equipe indicada por ele, antes mesmo da solução dos problemas. Estas anomalias nos circuitos de comunicação de dados identificadas pela CONTRATADA serão utilizadas para cálculo de reincidências, penalidades e acordo de nível de serviço;
10.6. Caso a CONTRATADA não seja capaz de identificar a causa de qualquer falha, esta será denominada indeterminada e a responsabilidade atribuída exclusivamente à CONTRATADA que deverá manter os acordos de nível de serviço pré-estabelecidos;
10.7. A CONTRATADA deverá configurar, de maneira adequada, os ativos de rede para habilitar o log dos eventos da rede do CONTRATANTE, tais como conexões externas e registros de utilização de serviços;

10.8. A CONTRATADA deverá prover acessos dos logs e relatórios por meio de páginas WEBs e mantê-los por, no mínimo, 60 dias online e disponibilizar por meio de solicitação por 12 meses.

10.9. De acordo com a necessidade da CONTRATANTE, a CONTRATADA deverá enviar os logs para um servidor de log dedicado da CONTRANTANTE, por meio do protocolo Syslog.

10.10. A Solução de proatividade visa antecipar-se aos problemas na solução SD-WAN e nos circuitos de dados e garantir o cumprimento do Acordo de Nível de Serviço (ANS) contratado. Para tanto, deverá realiza as seguintes atividades:

10.10.1. Monitorar os circuitos e equipamentos de dados;

10.10.2. Realizar o troubleshooting inicial com à CONTRATANTE;

10.10.3. Realizar o Diagnóstico e Triagem avançada de falhas;

10.10.4. Realizar a abertura, acompanhamento e fechamento de chamados de falhas relacionados com indisponibilidade dos serviços;

10.10.5. Realizar o posicionamento à CONTRATANTE do status das tratativas realizadas;

10.10.6. Suportar à CONTRATANTE com informações detalhadas dos dias, horários e tempos de duração das falhas;

10.10.7. Disponibilizar um Gestor Técnico designado para suporte à CONTRATADA (1º Nível de Escalonamento) e auxilio no portal de gerenciamento da solução;

10.10.8. Oferecer lista de escalonamento completo para eventuais recorrências junto à CONTRATADA;

10.10.9. Operar em regime 24 horas por dia, 7 dias por semana, todos os dias do ano.

11. DOS RELATÓRIOS DE DISPONIBILIDADE:

11.1. Terminado o mês de medição, a CONTRATADA apresentará à CONTRATANTE, até o 5º (quinto) dia útil do mês seguinte o “Relatório de Eventos” incluindo cada circuito CONTRATADO e contendo, no mínimo, as seguintes informações:

11.1.1. Disponibilidade mensal de cada um dos circuitos e da solução SD-WAN, ressaltando aqueles que ficaram abaixo do SLA contratado;

11.1.2. Disponibilidade total por circuito;

11.1.3. Descrição de cada evento ocorrido nos circuitos que ficaram abaixo do SLA contratado, com seus respectivos horários;

11.1.4. Indicação dos circuitos que ultrapassaram o tempo máximo de reparo contratado, para cada evento correspondente.

11.2. A CONTRATANTE poderá solicitar à CONTRATADA um relatório analítico para cada indisponibilidade, contendo a hora de início e a hora de fim da inoperância, os minutos excedentes ao prazo máximo para reparo e o índice de disponibilidade do serviço;

11.3. Sempre que solicitado, a CONTRATADA deverá disponibilizar Relatórios Analíticos para cada Circuito escolhido, e cobrindo o período de tempo estipulado na solicitação, em um prazo inferior a 24 (vinte e quatro) horas corridas, mostrando:

11.3.1. Disponibilidade do Circuito;

11.3.2. Taxa de Perdas de Pacotes;

11.3.3. Latência Média e Máxima Diária;

11.3.4. Ocupação Média e Máxima Diária de Banda do Circuito (Download e Upload);

11.3.5. Alarmes e Eventos.

11.4. Taxas de amostragens, conforme descrito abaixo, dependendo do período solicitado para o relatório:

11.4.1. Últimos 60 minutos: taxa de amostragem de 30 segundos, ou inferior;

11.4.2. Últimas 6 horas: taxa de amostragem de 1 minuto, ou inferior;

11.4.3. Últimas 24 horas: taxa de amostragem de 5 minutos, ou inferior;
11.4.4. Últimos 7 dias: taxa de amostragem de 30 minutos, ou inferior;
11.4.5. Últimos 6 meses: taxa de amostragem de 60 minutos, ou inferior.

11.5. Os Relatórios emitidos pela CONTRATADA serão aceitos em meio eletrônico, desde que no formato PDF. Os mesmos deverão ser devidamente identificados com nome e telefone de contato, do responsável por sua geração e empresa.

12. DA ESPECIFICAÇÃO TÉCNICA PARA LINK DE INTERNET

12.1. Prestação de serviço de acesso IP permanente, dedicado e exclusivo, entre a Rede de Dados do CONTRATANTE e a rede mundial de computadores (Internet), 24 horas por dia e 7 dias por semana, inclusive em feriados, mediante implantação de link de comunicação de dados a ser instalado nos endereços referenciados no Anexo F- Relação de endereços e velocidades, usando infraestrutura de fibra óptica, com fornecimento dos equipamentos necessários à execução do serviço e suporte técnico, nas velocidades especificadas no Anexo A.1- Relação de Demanda;

12.2. Em virtude da segurança e disponibilidade dos sistemas, acessos e serviços publicados, e tendo em vista que o serviço operará em contingência ativa, os Lotes 1 e 2 deverão ter seus itens fornecidos por CONTRATADAS distintas, para que não haja ponto de falha em comum e de modo a garantir a alta disponibilidade do serviço de acesso à Internet. Essa divisão tem por objetivo não permitir a adjudicação dos dois lotes licitados à mesma empresa, de modo a assegurar a segregação dos fornecimentos e a consequente alta disponibilidade, confiabilidade e acessibilidade do sistema;

12.3. Em caso de uma mesma licitante participar dos dois lotes e ofertar o menor lance em ambos, será considerada vencedora apenas naquele lote em que ofertou o menor preço. Caso uma mesma licitante oferte o menor preço nos dois lotes, e os valores sejam idênticos, a licitante será declarada vencedora apenas em um dos lotes, a ser decido pelo pregoeiro;

12.4. As especificações técnicas definidas neste anexo são de caráter obrigatório, e o não atendimento a qualquer uma das características e/ou quantidades mínimas especificadas constitui fundamento para desclassificação das propostas;

12.5. A CONTRATADA implantará o link de comunicação de dados, com, no mínimo, 01 (um) IPv4 e 01 (um) IPv6 Fixos e válidos, por link de acesso contratado, livre para uso pela CONTRATANTE, a qual definirá qual o tipo será utilizado;

12.6. Prover uma conectividade à Internet em full duplex, isto é, a taxa de transmissão fornecida deverá ser simétrica suportando as mesmas velocidades, tanto na entrada de dados quanto na saída, simultaneamente;

12.7. A taxa de transmissão deverá sempre estar disponível na totalidade do fluxo contratado e não deve incluir a taxa de overhead de protocolos até a camada 2 do modelo OSI;

12.8. A conexão deverá ser ATM (AssynchronousTransferMode) ou Ethernet. Entende-se doravante Ethernet por Gigabit Ethernet desde as dependências da CONTRATANTE até a conexão à infraestrutura de comunicação da CONTRATADA. A comunicação de dados deverá ser feita por meio de fibra ótica na última milha;

12.9. As interligações devem ser em conexão permanente, dedicadas e exclusivas, desde as dependências do CONTRATANTE até a conexão à infraestrutura de comunicação da CONTRATADA, obedecendo às recomendações elaboradas pela EIA/TIA (Electronic Industries Alliance / TelecomunicationsIndustryAssociation), pela ABNT (Associação Brasileira de Normas Técnicas) e demais normas, quando couber;

12.10. A CONTRATADA se responsabilizará pelo fornecimento e instalação dos materiais e equipamentos necessários à prestação do serviço, inclusive os roteadores(caso necessário) especificados, assumindo todos os custos dessa instalação;

12.11. A CONTRATADA deverá apoiar a CONTRATANTE em eventuais adaptações nas instalações físicas nas dependências da CONTRATANTE, assim como a infraestrutura externa, para a implantação dos serviços contratados.

12.12. Os links de comunicação de dados contratados poderão funcionar em conjunto entre si. Cada link funcionará como contingência ativa do outro, devendo cada um estar conectado em uma rede de provedor com infraestrutura de comunicação independente da outra CONTRATADA, inclusive com ASNs (Autonomous System Number) distintos, a fim de possibilitar total redundância na conexão à Internet; caso seja necessária a CONTRATADA deverá viabilizar estas características;

12.13. A CONTRATADA deverá, necessariamente, possuir, no mínimo, 2 (dois) POPs (Points of Presence) próprios em Goiânia ou 1(um) em Goiânia e pelo menos 1 (um) em Brasília ou 1 (um) em Goiânia e pelo menos 1 (um) localizado em algum município do Estado de Goiás, de forma que garanta a disponibilidade do serviço contratado;

12.13.1. Os POPs deverão estar próximos a Pontos de Troca de Tráfego (PTTs) na mesma região metropolitana sempre que possível, para maximizar a eficiência e reduzir a latência da conexão. Essa proximidade minimiza o tempo de resposta e melhora a qualidade de serviço, proporcionando uma experiência de Internet superior ao usuário final.

12.13.2. Somente serão aceitos como POPs válidos, para fins de avaliação de propostas, aqueles que possuam redundância nos links de comunicação de dados com o “backbone” da CONTRATADA;

12.14. A CONTRATADA deverá, preferencialmente, possuir conexão direta a um PTT (Ponto de Troca de Tráfego) na mesma região metropolitana dos POPs, especialmente com presença em um PIX do IX.br, a fim de melhorar a performance da troca de tráfego, reduzindo a latência e evitando a necessidade de rotas longas e ineficientes. A proximidade entre POPs e PTTs locais permite que o tráfego entre redes vizinhas permaneça regional, diminuindo custos e melhorando a estabilidade da conexão.

12.15. Somente serão aceitos como POPs válidos, para fins de avaliação de propostas, aqueles que possuam redundância nos links de comunicação de dados com o “backbone” da CONTRATADA, assegurando uma infraestrutura resiliente, com rotas alternativas para o tráfego, e aumentando a confiabilidade do serviço de Internet prestado.

12.16. A CONTRATADA deverá manter links de comunicação de dados com outras prestadoras de serviços de abrangência nacional, garantindo uma capilaridade ampla e eficiente do acesso em todo o território brasileiro.

12.17. O backbone utilizado pela CONTRATADA deverá possuir, no mínimo, três Pontos de Troca de Tráfego (PTTs) distintos, interconectados com provedores que possuam Sistemas Autônomos (AS) independentes, a fim de assegurar redundância e diversidade de rotas, melhorando a resiliência e estabilidade da conexão;

12.18. Um desses pontos de troca de tráfego deverá incluir obrigatoriamente conexão com um provedor de alcance internacional, permitindo maior eficiência e qualidade nas comunicações globais, especialmente em caso de tráfego de redes internacionais;

12.19. Deve oferecer suporte pelo menos aos seguintes algoritmos de criptografia: AES- 128-bit e AES-256-bit;

12.20. Deve oferecer suporte pelo menos aos seguintes algoritmos de autenticação: SHA- 1, SHA-256, SHA-384, SHA-512.

13. SOLUÇÃO ANTI DDoS DOS LINKS DE ACESSO DEDICADO À INTERNET

13.1. Para os Circuitos onde o equipamento seja do tipo CONCENTRADOR deverá ser entregue o serviço DDoS.

13.2. A solução deve ser capaz de implementar mecanismos capazes de detectar e mitigar ataques que façam o uso não autorizado de recursos de rede, automaticamente, tanto para IPv4 e IPv6, para no mínimo:

13.2.1. Ataques de inundação ou volumétricos, incluindo:

13.2.2. SYN Flood;

13.2.3. UDP Flood;

13.2.4. TCP Flood;

13.2.5. ICMP Flood;

13.2.6. Ataques à pilha TCP, incluindo:

13.2.7. Mau uso das flags TCP;

13.2.8. Ataques de RST e FIN;

13.2.9. TCP idle Resets.

13.2.10. Ataques que utilizam fragmentação de pacotes (IP, TCP e UDP);

13.2.11. Ataques de botnets e worms;

13.2.12. Ataques que utilizam falsificação de endereços IP de origem (IP spoofing);

13.2.13. Ataques à camada de aplicação, incluindo os protocolos HTTP e DNS, para no mínimo: HTTP URL Get/Post Flood; SIP Invite Flood; DNS Flood; DNS, NTP, SNMPV3 Reflection/Amplification e Slowloris e Pyloris.

13.3. A solução deve implementar mecanismo de mitigação baseado no desvio de tráfego sob suspeita para um Centro de Mitigação na infraestrutura da CONTRATADA.

13.4. No Centro de Mitigação o tráfego será inspecionado e tratado de forma que o tráfego malicioso seja bloqueado e o tráfego legítimo seja devolvido para a rede para ser roteado até seu destino final;

13.5. A mitigação de ataques deverá ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento na infraestrutura da CONTRATADA, de forma transparente para a CONTRATANTE;

13.6. Deverá ser possível desviar para o Centro de Mitigação somente o tráfego para os IPs sob suspeita de ataque;

13.7. O sistema implantado na rede da CONTRATADA deverá atuar sobre o tráfego somente em momentos de ataque.

13.8. A solução deve suportar a detecção e mitigação automática de ataques, utilizando múltiplas técnicas para mitigação e contramedidas, para no mínimo:

13.8.1. White lists;

13.8.2. Black lists;

13.8.3. Limitação de taxa;

13.8.4. Técnicas desafio-resposta;

13.8.5. Descarte de pacotes malformados;

13.8.6. Bloqueio por localização geográfica (país) de endereços IP;

13.8.7. Técnicas de mitigação de ataques aos protocolos HTTP e DNS;

13.8.8. Manter uma lista dinâmica de endereços IP bloqueados;

13.9. Os endereços IP que não enviarem mais requisições maliciosas deverão ser removidos da lista de IPs bloqueados, após um período de tempo considerado seguro pela CONTRATADA e/ou CONTRATANTE.

13.10. A solução deve implementar mecanismos capazes de detectar e mitigar ataques baseados em modo aprendizagem, através de anomalias estatísticas e desequilíbrio de volume de tráfego, que permite utilização de perfil de tráfego (baseline) tanto de longo quanto de curto prazo, para ataques volumétricos.

13.11. A solução deverá fornecer proteção para Flash Crowd, ou seja, quando ocorre o crescimento do volume de tráfego legítimo acima do esperado (perfil de tráfego/baseline), a solução deverá ser capaz de diferenciar o tráfego legítimo do malicioso, bloqueando apenas o tráfego proveniente de ataques.

13.12. A solução deverá ser capaz de detectar e mitigar os ataques destinados a qualquer endereçamento IP, tanto para IPv4 e IPv6, sob administração da CONTRATANTE;

13.13. Nos procedimentos de mitigação de ataques fica proibido o encaminhamento do tráfego para análise e limpeza fora do território brasileiro, exceto se o tráfego de origem for proveniente do exterior, caso em que será permitido o encaminhamento do mesmo para um centro de mitigação fora do território nacional disponibilizado pela CONTRATADA;

14. FERRAMENTAS DE VISIBILIDADE E ADMINISTRAÇÃO DO SERVIÇO ANTI DDoS

14.1. A CONTRATADA deverá possuir ao menos 1 (um) Centro de Mitigação em território nacional com capacidade de detecção e/ou mitigação de ataques e que seja capaz de tratar o tráfego de ataques demandado. Os acessos contemplados com a solução de segurança Anti DDoS deverão ter sua a gerência e operação executada através de um Centro Operacional de Segurança (ou SOC – Security Operations Center) no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques;

14.2. A solução deve possuir capacidade de analisar a reputação de endereços IP, possuindo base própria de informações, gerada durante a filtragem dos ataques, e interligada com os principais centros mundiais de avaliação de reputação de endereços IP;

14.3. O Bloqueio de ataques DoS e DDoS por ACLs em roteadores de borda da CONTRATADA será aceito desde que tenha solicitação, autorização ou anuência da CONTRATANTE;

14.4. As soluções de detecção e mitigação devem possuir serviço de atualização de assinaturas de ataques e devem ser mantidas atualizadas durante toda a vigência do contrato.

14.5. A CONTRATADA deverá disponibilizar relatórios e informações do tráfego monitorado, bem como os eventos e alertas de segurança contendo, no mínimo, as seguintes informações:

14.5.1. Informações sobre o tipo dos ataques;

14.5.2. Horário de início e fim;

14.5.3. Volume de tráfego bloqueado e não bloqueado;

14.5.4. IPs de destinos;

14.5.5. Os maiores alvos de ataques;

14.5.6. Os maiores ofensores (IP de origem);

14.5.7. Os maiores ofensores por geolocalização (país);

14.5.8. Percentual das origens dos ataques por geolocalização (país);

14.6. CONTRATADA deverá oferecer meios para customizar as configurações e regras, para no mínimo:

14.6.1. Detecção e mitigação automática baseada em limiares de pps (pacotes por segundo) e bps (bits por segundo);

14.6.2. Bloqueio e limitação de taxa para um IP ou range de IPs de destino.

14.7. MODALIDADE DE ATENDIMENTO E PRAZOS DO SERVIÇO ANTI DDoS

14.7.1. A CONTRATADA deverá realizar a detecção de ataques, de forma automática e proativa, e deverá notificar a CONTRATANTE por telefone ou correio eletrônico em até 20 (vinte) minutos a partir do início do ataque, informando o tipo e os alvos do ataque.

14.7.2. pós notificação da suspeita de ataque por parte da CONTRATADA, a CONTRATANTE poderá solicitar a mitigação do ataque. A CONTRATADA terá até 10 (dez) minutos para iniciar a mitigação após solicitação da CONTRATANTE.

14.7.3. A CONTRATANTE poderá optar pela mitigação automática previamente configurada dos ataques detectados e, neste caso, a detecção e a mitigação deverão ocorrer em até 20 (vinte) minutos a partir do início do ataque;

14.7.4. A CONTRATANTE poderá alterar a qualquer momento o modo de mitigação para um determinado tipo e alvo do ataque: mitigação mediante autorização da CONTRATANTE ou mitigação automática.

14.7.5. Caso a CONTRATANTE identifique a existência de tráfego malicioso, a CONTRATADA deverá realizar a mitigação de ataques em até 15 (quinze) minutos após a solicitação formal da CONTRATANTE através dos canais especificados;

14.7.6. A CONTRATANTE poderá solicitar a mitigação do tráfego destinado a um IP específico, conjunto de IPs ou range de IPs;

14.7.7. A CONTRATANTE poderá solicitar a mitigação do tráfego originado de um IP específico, conjunto de IPs ou range de IPs;

14.7.8. A CONTRATANTE poderá solicitar regras de mitigações específicas de acordo com as técnicas listadas.

14.7.9. Não haverá limitação na quantidade de mitigações de ataques e no volume de tráfego bloqueado durante o período de vigência contratual, seja através de detecção proativa ou reativa;

14.7.10. A CONTRATADA deverá disponibilizar um Centro Operacional de Segurança (ou SOC – Security Operations Center) no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, com operação de atendimento conforme definido neste Termo de Referência;

14.7.11. As funcionalidades de monitoramento, detecção e mitigação de ataques devem ser mantidas em operação ininterrupta durante 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

14.7.12. Caso seja constatado que o tráfego de DDoS não tenha sido bloqueado na rede da CONTRATADA após o tempo definido de acordo itens deste Termo de Referência, o tempo de duração do ataque não bloqueado será contabilizado como indisponibilidade do serviço;

14.7.13. Caso seja constatado que o tráfego legítimo tenha sido bloqueado indevidamente por mal funcionamento da solução da CONTRATADA, o tempo de duração do bloqueio indevido será contabilizado como indisponibilidade do serviço.

14.7.14. A CONTRATANTE poderá solicitar a inclusão de novos serviços de forma qualitativa, seja por meio de solicitação à CONTRATADA, ou por meio de aditivo contratual, em comum acordo para adequar as suas necessidades de segurança.

14.8. ESPECIFICAÇÕES DOS LINKS DE INTERNET PARA SOLUÇÃO SD-WAN

14.8.1. A CONTRATADA deverá fornecer serviço dedicado de acesso à internet com, no mínimo, 01 (um) IPv4 e 01 (um) IPv6 Fixos e válidos, por link de acesso contratado, livre para uso pela CONTRATANTE, a qual definirá qual o tipo será utilizado;

14.8.2. A CONTRATADA poderá efetuar reserva ou alocação de banda, para cumprimento de suas obrigações (p.ex.: gerenciamento da rede), desde que esta reserva não ultrapasse 1% (um por cento) da velocidade contratada.

14.8.3. Os links de acesso à internet deverão prover conectividade à Internet em full duplex, isto é, a taxa de transmissão fornecida deverá ser simétrica suportando as mesmas velocidades, tanto na entrada de dados quanto na saída, simultaneamente;

14.8.4. A taxa de transmissão deverá estar sempre disponível na totalidade do fluxo contratado e não deve incluir a taxa de overhead de protocolos até a camada 2 do modelo OSI;

14.8.5. Todos os equipamentos e acessórios necessários para a ativação dos links instalados devem ser fornecidos pela CONTRATADA e totalmente compatíveis com os equipamentos SD-WAN e a solução adotada;

14.8.6. O link deve ser interligado ao equipamento SD-WAN instalado na localidade, via patch cord;

14.8.7. A CONTRATADA deverá disponibilizar meios de aferição da velocidade dos links instalados por meio dos dashboard da solução SD-WAN;

14.8.8. A CONTRATADA deverá possuir link de comunicação de dados com outras prestadoras de abrangência nacional, possibilitando a capilarização do acesso em todo o Brasil;

14.8.9. O backbone da licitante deverá possuir, pelo menos, três pontos de troca de tráfego com provedores que possuam AS independentes;

14.8.10. Um destes pontos de troca deve ser com um provedor internacional;

14.8.11. A licitante deverá aceitar AS-Path prepending em suas políticas de BGP.

14.9. DOS ROTEADORES

14.9.1. Equipamento somente será instalado em caso de necessidade da CONTRATADA;

14.9.2. O equipamento deve operar nas tensões entre 100 e 240 VCA/60Hz, selecionáveis automaticamente.

14.9.3. Os equipamentos a serem instalados nos Datacenters da CONTRATANTE deverão possuir duas fontes de energia redundantes;

14.9.4. Permitir a criação de vlans, conforme especificação 802.1q.

14.9.5. Permitir a criação de links agregados e dinâmicos, conforme especificação 802.3ad

14.9.6. Permitir a inserção de registros estáticos na tabela de endereços da camada de enlace.

14.9.7. CAMADA DE ENLACE

14.9.7.1. Deve possuir os protocolos WANs necessários a implementação do serviço contratado;

14.9.7.2. Deve possuir suporte aos protocolos LAN: IPv4, IPv6 e listas de acesso que possam ser construídas baseadas em:

14.9.7.2.1. Endereços IP de origem e destino;

14.9.7.2.2. Portas TCP e UDP de origem e destino;

14.9.7.2.3. Código e tipo de pacote ICMP (ICMP code e ICMP type);

14.9.7.2.4. Campo IP Precedence;

14.9.7.2.5. Protocolo IP;

14.9.7.2.6. Flags TCP;

14.9.7.2.7. IP Options;

14.9.8. QOS

14.9.8.1. Possibilitar a priorização de quadros Ethernet conforme especificação IEEE 802.1p (COS).

14.9.8.2. Possibiliar a priorização de pacotes de acordo com o conteúdo do campo Type of Service do protocolo IP, conforme especificação RFC 791.

14.9.8.3. Possibilitar a priorização de pacotes de acordo com o conteúdo do campo Differentiated Services Field do protocolo IP, conforme especificação RFC 2474.

14.9.8.4. Possibilitar a Classificação e Reclassificação baseadas em endereço IPv4 e IPv6 de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.

14.9.8.5. Implementar o mecanismo de escalonamento de fila Strict Priority (SP queueing).

14.9.8.6. Implementar pelo menos um dos seguintes mecanismos de escalonamento de fila: Weighted Round Robin (WRR), Shaped Round Robin (SRR) ou Weighted Fair Queue (WFQ).

14.9.8.7. Implementar a RFC2597 (Assured Forwarding PHB Group) e a RFC2598 (An Expedited Forwarding PHB).

14.9.8.8. Possibilitar filtragem de pacotes através de listas de controle de acesso baseadas, no mínimo, nas seguintes informações: endereço da camada de rede (IPv4 e IPv6) e portas da camada de transporte.

14.9.8.9. Possibilitar o espelhamento do tráfego de rede (port mirroring), de uma porta de origem para uma porta de destino do próprio roteador ou para outro equipamento através do seu endereço da camada de rede (IP).

14.9.9. **VPN**

14.9.9.1. Deve implementar, no mínimo, VPN IPSec com capacidade de implementar túneis site-to-site do tipo hub-and-spoke;

14.9.9.2. Deve permitir o estabelecimento do túnel utilizando uma “chave secreta” ou certificados digitais;

14.9.9.3. Deve implementar IKEv1 e IKEv2;

14.9.9.4. Suportar no mínimo DIFFIE HELLMAN GROUP:Diffie-Hellman Group 2 (1024-bit);Diffie-Hellman Group 5 (1536-bit);Diffie-Hellman Group 14 (2048-bit).

14.9.10. **NTP**

14.9.10.1. Suporte ao protocolo cliente NTP (Network Time Protocol), conforme especificação RFC 1305;

14.9.10.2. Port Address Translation (PAT);

14.9.10.3. Network Address Translation (NAT);

14.9.10.4. Servidor DHCP (Dynamic Host Configuration Protocol);

14.9.10.5. Agente DHCP (RFC 1542);

14.9.10.6. IEEE 802.1d Transparent Learning Bridging;

14.9.11. **GERÊNCIA**

14.9.11.1. Possuir interface CLI (Command Line Interface)

14.9.11.2. Implementar protocolo SSHv2 para acesso ao shell do sistema, conforme especificação RFC 4251

14.9.11.3. Implementar protocolo cliente NTP (Network Time Protocol), conforme especificação RFC 1305

14.9.11.4. Implementar protocolo cliente RADIUS para autenticação no sistema, conforme especificação RFC 2865

14.9.12. **MONITORAMENTO**

14.9.12.1. Implementar os protocolos SNMPv2 e SNMPv3, conforme especificações RFC 1157, RFC 1441 e RFC 2571, respectivamente.

14.9.12.2. Realizar coleta de informações de fluxos que circulam pelo equipamento, e exportar os dados resultantes para um servidor de análise utilizando um protocolo padrão de mercado, como Netflow ou Sflow.

14.9.12.3. Os equipamentos devem permitir a medição de parâmetros de qualidade do link, no mínimo de perda de pacotes, latência e jitter por meio dosV protocolos NQA ou IP-SLA

14.9.12.4. Deve ser possível obter no mínimo as seguintes informações de cada fluxo:

14.9.12.4.1. IP de origem/destino;

14.9.12.4.2. Parâmetro “protocol type” do cabeçalho IP;

14.9.12.4.3. Porta TCP/UDP de origem/destino;

14.9.12.4.4. Interface de entrada do tráfego;

14.9.12.4.5. Número do sistema autônomo de origem.

14.9.12.5. Deve ser possível especificar o uso de tal funcionalidade somente para tráfego de entrada, somente para tráfego de saída (e também para ambos os sentidos simultaneamente) em uma dada interface do equipamento.

14.9.13. ACESSÓRIOS:

14.9.13.1. Deverá ser entregue todos os acessórios necessários para a sua instalação nos racks da CONTRATANTE inclusive com o fornecimento de patchcords ou cordão óptico para interligar ao equipamento da CONTRATANTE.

14.9.14. ROTEAMENTO

14.9.14.1. Os Roteadores destinados aos links dos concentradores ou com serviços AntiDDOS deverão possuir os protocolos de roteamento: OSPF e BGP;

14.10. REQUISITOS GERAIS DOS EQUIPAMENTOS

14.10.1. Todos os equipamentos da solução devem ser montados em rack com tamanho 19 polegadas, conforme especificação EIA-310-D e vir com todos os seus acessórios, bandeja se necessário, para a sua completa instalação, inclusive patchcord/linecords para a interligação da solução;

14.10.2. Os equipamentos devem ser novos, ou seja, de primeiro uso. Na data da proposta, nenhum dos modelos poderão estar listados no site do fabricante em listas de end-of-life e end-of sale.

14.10.3. Os equipamentos devem permitir a medição de parâmetros de qualidade do link, no mínimo de perda de pacotes, latência e jitter por meio dos protocolos NQA, IP-SLA ou pela própria solução, a fim de que essas métricas possam ser coletadas através de quaisquer outras ferramentas de monitoramento.

14.10.4. Caso a medição de parâmetros de qualidade do link (perda de pacotes, latência e jitter) seja da própria solução, a medição deve ser coletada, no mínimo, por meio de APIs e o protocolo SNMP (v2c e V3).

14.10.5. A CONTRATADA deverá aplicar nos equipamentos fornecidos à CONTRATANTE ou em outros equipamentos de suas redes, exclusivos ao CONTRATANTE, implementações de segurança tais como: autenticação para acesso aos equipamentos de rede, controle de acesso aos dispositivos e listas de acesso;

14.10.6. O protocolo para monitoramento configurado nos ativos de rede deverá ser SNMPv3, que requer autenticação e dá um nível de segurança maior que as versões anteriores;

14.10.7. O acesso remoto aos dispositivos deverá ser realizado somente via protocolo de acesso remoto criptografado (SSH versão 2) ou Web (https) ou Dashboard da Solução fornecida;

14.10.8. Deverá ser empregado um esquema de autenticação no nível de protocolo de roteamento, para evitar que roteadores não autorizados injetem ou descubram rotas da rede do CONTRATANTE;

14.10.9. Os equipamentos devem estar com o horário sincronizado via NTP, configurado, preferencialmente para um servidor NTP dentro do ambiente do CONTRATANTE, e possuir o máximo possível de detalhes, sem gerar dados em excesso;

14.10.10. Caso a CONTRATADA opte por utilizar o seu serviço NTP, deverá responsabilizar-se pela correta sincronização para que não prejudique a aferição do SLA, descontos e glosas.

14.10.11. A CONTRATADA deverá aplicar e manter atualizados os patches de segurança nos seus equipamentos ou em outros equipamentos locados ao CONTRATANTE.

14.11. DA SEGURANÇA PARA OS ATIVOS DE REDE DA CONTRATADA

14.11.1. A CONTRATADA deverá aplicar nos equipamentos fornecidos à CONTRATANTE ou em outros equipamentos de suas redes, exclusivos ao CONTRATANTE, implementações de segurança tais como: autenticação para acesso aos equipamentos de rede, controle de acesso aos dispositivos e listas de acesso;

14.11.2. O protocolo para monitoramento configurado nos ativos de rede deverá ser SNMPv3, que requer autenticação e dá um nível de segurança maior que as versões anteriores;

14.11.3. O acesso remoto aos dispositivos deverá ser realizado somente via protocolo de acesso remoto criptografado (SSH versão 2) ou Web (https) ou Dashboard da Solução fornecida;

14.11.4. Deverá ser empregado um esquema de autenticação no nível de protocolo de roteamento, para evitar que roteadores não autorizados injetem ou descubram rotas da rede do CONTRATANTE;

14.11.5. Os equipamentos devem estar com o horário sincronizado via NTP, configurado, preferencialmente para um servidor NTP dentro do ambiente do CONTRATANTE, e possuir o máximo possível de detalhes, sem gerar dados em excesso;

14.11.6. Caso a CONTRATADA opte por utilizar o seu serviço NTP, deverá responsabilizar-se pela correta sincronização para que não prejudique a aferição do SLA, descontos e glosas.

14.11.7. A CONTRATADA deverá aplicar e manter atualizados os patches de segurança nos seus equipamentos ou em outros equipamentos locados ao CONTRATANTE.

14.12. ESPECIFICAÇÕES GERAIS

14.12.1. A CONTRATANTE SE RESERVA DO DIREITO EM ESCOLHER O LOTE QUE LHE TRAZER MAIOR VANTAJOSIDADE.

14.13. DO CONTATO E ABERTURA DE CHAMADOS:

14.13.1. A CONTRATADA deverá disponibilizar os seguintes contatos telefônicos:

14.13.1.1. Para abertura de Chamado;

14.13.1.2. Escalonamento e priorização;

14.13.1.3. Do Preposto.

14.13.2. A CONTRATADA poderá disponibilizar grupo de mensagens para o escalonamento e priorização de chamados;

14.13.3. A abertura de chamados deverá ser realizada por telefone (0800 ou de custo local na capital do estado do CONTRATANTE) e por sistema WEB/e-mail;

14.13.4. Considera-se como data e hora de abertura do chamado de reparo a notificação automática da interrupção de um circuito por meio da ferramenta de monitoramento ou a

notificação encaminhada pelo Gestor/Fiscal do contrato, prevalecendo a que ocorrer primeiro;

14.13.5. Para cada chamado técnico deverá ser informado um número de controle (protocolo) para registro, bem como a manutenção de histórico de ações e atividades realizadas, contendo no mínimo:

14.13.5.1. Data e hora de abertura do chamado;

14.13.5.2. Responsável pelo chamado na CONTRATADA;

14.13.5.3. Responsável pelo chamado no CONTRATANTE;

14.13.5.4. Severidade atribuída ao problema;

14.13.5.5. Descrição do problema;

14.13.5.6. Histórico de atendimento;

14.13.5.7. Data e hora do encerramento;

14.13.5.8. Responsável pelo encerramento;

14.13.5.9. Solução adotada para a resolução do problema.

14.13.6. O encerramento dos chamados técnicos será autorizado após a realização de testes com a equipe técnica ou unidade remota da CONTRATANTE ou processo de recuperação de falhas aprovado pela CONTRATANTE;

14.13.7. O número de identificação do chamado técnico deverá ser fornecido a CONTRATANTE no ato de sua abertura;

14.13.8. Uma vez constatada a indisponibilidade pelo serviço de monitoramento, a CONTRATADA poderá aguardar 5 (cinco) minutos ou averiguar se houve problemas alheios ou não imputáveis ao objeto deste contrato a exemplo de falta de energia sem prejuízo aos acordos de nível de serviços definidos neste termo de referência;

14.13.9. Uma vez descartado o problema não imputável, a CONTRATADA deverá dar prosseguimento nas atividades para correção do link;

14.13.10. Todos os incidentes deverão estar devidamente registrados no sistema de chamados da CONTRATADA e devidamente encaminhado no Relatório Analítico para que a CONTRATANTE.

14.14. **DOS CHAMADOS E SUPORTE TÉCNICO**

14.14.1. O suporte técnico deverá ser prestado durante a execução do contrato, a partir do recebimento definitivo do serviço contratado;

14.14.2. A partir do recebimento provisório e findado o prazo de entrega do serviço por motivo de atraso da CONTRATADA, a mesma deve prestar o suporte técnico, nos mesmos moldes deste Termo de Referência, até conseguir entregar os serviços de forma definitiva;

14.14.3. O suporte técnico deverá contemplar as manutenções corretivas e evolutivas para a solução e não poderá acarretar custos adicionais ao CONTRATANTE;

14.14.4. Entende-se por “manutenção corretiva” uma série de procedimentos destinados a recolocar o serviço em pleno estado de funcionamento, removendo definitivamente os defeitos apresentados;

14.14.5. A CONTRATADA deve manter equipe técnica disponível para atendimento presencial, reset de equipamento e testes que sejam necessários para o restabelecimento de qualquer falha no serviço contratado, de maneira a atender dentro do SLA todas as localidades do **Anexo F- Relação de endereços e velocidades;**

14.14.6. Entende-se por “manutenção evolutiva” o fornecimento de novas versões e/ ou releases corretivos e/ou evolutivas de versões de firmware e software que compõem a rede, lançadas durante a vigência do contrato;

14.14.7. O suporte técnico será formalizado pela abertura de chamados técnicos, objetivando a resolução de problemas e dúvidas quanto a questões funcionais e técnicas relacionadas a instalação, configuração, mudanças de configuração, customização e utilização da Solução;

14.14.8. Será disponibilizado pela CONTRATADA um conjunto de, pelo menos, 10 (dez) identificadores e respectivas senhas de acesso para pessoas autorizadas a abrir e acompanhar os chamados de suporte técnico;

14.14.9. O suporte técnico será prestado de forma remota, ou ainda, on-site, nas dependências do CONTRATANTE, caso a natureza do serviço exija a presença de técnico especializado ou quando solicitado pelo Gestor do Contrato (ou outro servidor devidamente autorizado);

14.14.10. A CONTRATADA deverá prestar o suporte técnico via telefone ou e-mail, em idioma português do Brasil;

14.14.11. A CONTRATADA deverá manter o Suporte Técnico disponível para a abertura e acompanhamento de chamados em tempo integral, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, todos os dias do ano, inclusive sábados, domingos e feriados;

14.14.12. A CONTRATADA deverá garantir que a CONTRATANTE efetue um número ilimitado de chamados de suporte técnico durante a vigência do contrato, sem ônus adicional;

14.14.13. Os chamados para suporte técnico terão origem em decorrência de qualquer problema detectado pela Equipe Técnica do CONTRATANTE no tocante ao pleno estado de funcionamento da solução, inclusive problemas relacionados com instalação, configuração, otimização e atualização;

14.14.14. As configurações dos ativos da rede, tais como: regras de QoS, SNMPV3, regras de segurança- ACL's, tabelas de roteamento para cada nível de serviço, serão definidas pelo Gestor do Contrato ou técnico devidamente autorizado, conforme as necessidades do CONTRATANTE e executadas pela CONTRATADA a partir de seu NOC;

14.14.15. Com base em processos de atendimento especializados, a CONTRATADA deverá possuir uma estrutura que garanta a recepção de chamados através de um portal WEB, onde a CONTRATANTE poderá abrir os chamados e acompanhar evolução dos mesmos.

14.14.16. Além do portal WEB, a CONTRATADA deverá disponibilizar atendimento telefônico através de 0800 ou número local em regime 24x7x365 caso a CONTRATANTE queira abrir e acompanhar os chamados sem a necessidade de acesso à internet (web).

14.14.17. A CONTRATADA deverá possuir suporte N2 (especialistas sêniores) e N3 da própria fabricante, para intervir em qualquer necessidade envolvendo o framework da solução fornecida por ela, caso o N1 não consiga atender as solicitações recebidas. Esta célula poderá estar fisicamente nas dependências da CONTRATADA.

14.14.18. Durante a vigência do contrato, o CONTRATANTE poderá solicitar alterações nas configurações dos ativos de rede, as quais deverão ser concluídas no prazo de até 48 (quarenta e oito) horas consecutivas contadas a partir da abertura do chamado.

14.15. DOS NÍVEIS DE ATENDIMENTO:

14.15.1. A CONTRATADA deverá prestar os serviços de acordo com os níveis de atendimentos descritos no Anexo D- Níveis de Atendimento.

14.15.2. DA LISTA DE IMPERFEIÇÕES E EFEITOS REMUNERATÓRIOS

14.15.3. O preço a ser fixado em contrato para a realização do objeto deste Termo de Referência se referirá à execução com qualidade. Portanto, a execução contratual que atinja os objetivos dos serviços sem a qualidade (latência, velocidade e perda de pacote), implicará

no pagamento proporcional pelo serviço realizado, seguindo os critérios previstos neste Termo de Referência;

14.15.4. Tais ajustes visam assegurar ao CONTRATANTE o recebimento dos serviços contratados, mesmo diante de eventuais imperfeições em sua execução, observando o Acordo de Nível de Serviços, tendo como base o que consta nos artigos 11, 33 e 34 da Instrução Normativa n. 02/08 da SLTI/MPOG e alterações complementares;

14.15.5. O objeto deste Termo de Referência será constantemente avaliado pelo(s) Fiscal(is) do Contrato, que analisarão os serviços fornecidos através de ferramenta de monitoramento própria ou fornecida pela CONTRATADA, visando a adequação dos serviços entregues com Anexo C- Acordo de Nível de Serviço;

14.15.6. Diante dos dados constantes no "Acordo de Nível de Serviços", o CONTRATANTE promoverá a tabulação dos mesmos, de modo a identificar a proporção da aceitação da qualidade dos serviços, e assim demonstrará a possibilidade da medida administrativa para o pagamento mensal;

14.15.7. Desde que sejam devidamente registradas em chamado técnico, a violação de qualquer um dos níveis de serviço definidos neste Termo serão desconsideradas pelo CONTRATANTE, mediante a, pelo menos, uma das seguintes ocorrências:

14.15.8. Falta no fornecimento de energia elétrica na localidade, devendo ser comprovada pela CONTRATADA com algum colaborador da localidade, por ligação telefônica na ocorrência ou finalização do problema, ou com relatório da concessionária de energia relatando problema na região daquela localidade;

14.15.9. Falha em algum equipamento de responsabilidade do CONTRATANTE;

14.15.10. Falha decorrente de procedimentos operacionais do CONTRATANTE;

14.15.11. Falha de qualquer equipamento da CONTRATADA que não possa ser corrigida por inacessibilidade causada pela CONTRATANTE;

14.15.12. Eventual interrupção programada, quando se fizer necessária ao aprimoramento e à implantação de adequações dos links de dados, desde que previamente negociada entre CONTRATADA e a CONTRATANTE.

14.15.13. A CONTRATADA deve possuir equipe técnica disponível para se dirigir até a localidade remota, dentro do SLA, sempre que os equipamentos precisarem ser reiniciados ou testados;

14.15.14. As unidades remotas não contam com equipe técnica da CONTRATENTE, sendo assim, os colaboradores locais não estão aptos a reiniciar nem mesmo alterar cabos dos ativos da CONTRATADA;

14.15.15. A critério da CONTRATANTE e anuência dos colaboradores locais, a CONTRATADA poderá solicitar o reinício ou testes nas localidades remotas, porém deverá assumir total responsabilidade por imperícia ou danos causados nos equipamentos, e sem prejuízo aos SLAs estabelecidos neste termo de referência;

14.15.16. A ocorrência de qualquer tipo de interrupção no circuito deverá ser comunicada por e-mail a todos os membros da equipe técnica e gestores do CONTRATANTE responsáveis pelo acompanhamento do contrato e, por ligação telefônica a pelo menos um deles. A lista de membros desta equipe será definida pelo CONTRATANTE quando da realização da reunião de alinhamento;

14.15.17. A lista de membros a que se refere o subitem anterior poderá ser alterada a qualquer momento pelo CONTRATANTE, devendo este, comunicar formalmente a CONTRATADA, através do responsável indicado na reunião de alinhamento;

14.15.18. Caso haja necessidade de interrupção do serviço, a CONTRATADA deverá planejar antecipadamente com o Gestor do Contrato e a interrupção deverá ocorrer fora do horário de expediente.

14.16. DA ARQUITETURA TECNOLÓGICA DA SOLUÇÃO

14.16.1. As soluções pretendidas baseiam-se em Redes de Telecomunicações com serviço de monitoramento com ações preventivas e proativas, com o intuito de prover uma conexão de alta capacidade, disponibilidade e qualidade entre os Datacenters e as Localidades mencionadas no Anexo F- Relação de endereços e velocidades;

14.16.2. Todos os equipamentos fornecidos para prestação do serviço devem estar homologados ou certificados pela ANATEL;

14.16.3. Links ponto a ponto, de internet de alta capacidades ou para uso específico conforme indicação da CONTRATANTE;

14.16.4. Trata-se de Contratação de Empresas Especializadas para fornecimento de Solução SD-WAN, e links WAN (IP), e outro link de Internet (para redundância/backup a ser interligado à solução SD-WAN);

14.16.5. A arquitetura tecnológica da Rede SD-WAN a ser adotada, baseia-se na contratação de serviço de link de dados para suportar comunicações com as Unidades Externas e a SEDE em Goiânia, Unidades Regionais e SGG.

14.16.6. A topologia da rede fornecida pela CONTRATADA, atenderá a necessidade de uma rede de telecomunicação, sendo toda a capacidade demandada nos enlaces que a compõe, gerenciada e utilizada apenas na comunicação de dados entre os Datacenters do CONTRATANTE e as localidades ligadas a ele, devendo suportar padrões IPv4/IPv6 para roteamento, sendo o tipo ou os tipos a serem utilizados, definidos pela CONTRATANTE, ou com a sua anuência;

14.16.7. Cada Unidade Remota deverá receber pelo menos um ponto de rede, representado por um equipamento (de propriedade da CONTRATADA) com interface Gigabit Ethernet para conexão com a rede local da unidade. Os equipamentos deverão ter características mínimas para suportar protocolos de monitoramento;

14.16.8. A concentração da rede será no Datacenter da CONTRATANTE interligados às unidades remotas, conforme os endereços citados no Anexo F- Relação de endereços e velocidades e seus quantitativos previstos no Anexo A.1- Relação de Demanda

14.16.9. Para o Concentradores SD-WAN e Roteador de Internet de alta velocidade que serão instalados no Datacenter, deverão possuir fontes redundantes de energia;

14.16.10. Em linhas gerais, a solução proposta deverá atender, no mínimo, as topologias definidas abaixo pela CONTRATANTE.

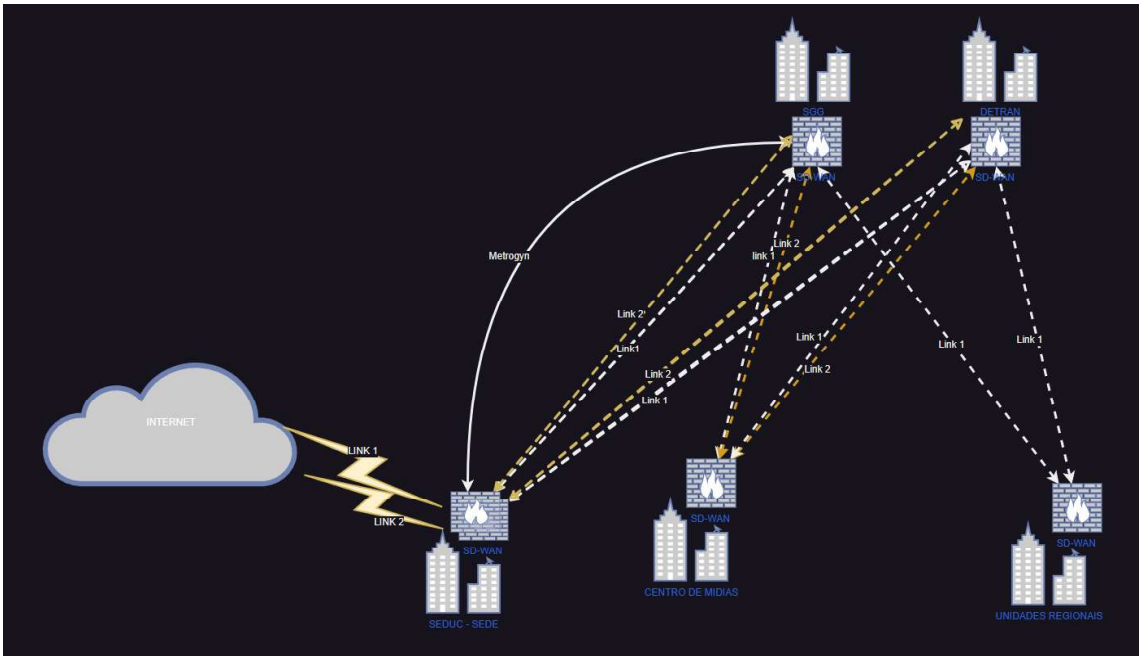

Figura 1 – Topologia SDWAN

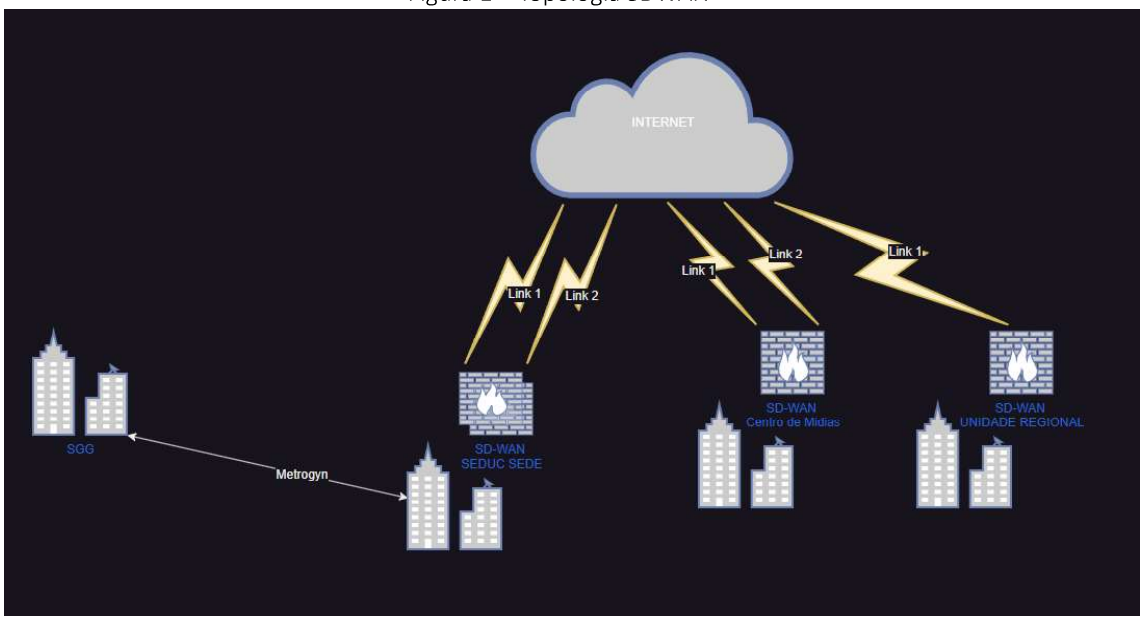

Figura 2 – Topologia Internet

14.17. DA REUNIÃO DE ALINHAMENTO

14.17.1. Homologado o resultado da licitação e tendo o contrato assinado, deverá ser realizada até o 10º (décimo) dia útil após a assinatura do Contrato, uma reunião presencial de alinhamento, na sede do CONTRATANTE, com o objetivo de se apresentar o preposto, identificar as expectativas e diretrizes para elaborar o Projeto de Implantação, nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e em seus Anexos, e esclarecer possíveis dúvidas do objeto, conforme agendamento efetuado pelo Gestor do Contrato;

14.17.2. O Projeto de Implantação deverá indicar o Cronograma de Implantação com as entregas intermediárias e será elaborado de comum acordo entre a CONTRATADA e o CONTRATANTE, desde que observado o prazo máximo de entrega total do serviço contratado.

14.18. DO PROJETO DE IMPLANTAÇÃO

14.18.1. A CONTRATADA deverá apresentar, ao Gestor do Contrato, em até 30 (trinta) dias consecutivos, contados a partir do primeiro dia útil seguinte à data da realização da reunião de alinhamento, o Projeto de Implantação dos serviços contratados, contendo no mínimo:

14.18.2. O detalhamento das etapas que serão seguidas, datas de início e fim de cada atividade, conforme Cronograma de Implantação aprovado na reunião de alinhamento;

14.18.3. Quando couber, a definição das marcas e modelos de equipamentos que serão utilizados.

14.19. ESTRATÉGIA DA IMPLANTAÇÃO

14.19.1. Os enlaces de acesso para as Unidades descritas no Anexo A.1- Relação de Demanda e Anexo F- Relação de endereços e velocidades deverão ser fornecidos pela CONTRATADA, sem ônus adicional ao CONTRATANTE, incluindo, dentre os materiais, cabos externos, cabos de entrada, tubulações e a completa infraestrutura externa necessária para o perfeito cumprimento do objeto;

14.19.2. Para a instalação de estruturas físicas nos edifícios do CONTRATANTE, a CONTRATADA deverá entregar para a aprovação da Diretoria competente da CONTRATANTE, o projeto executivo com detalhamento da intervenção a ser executada para aprovação prévia;

14.19.3. A infraestrutura interna (sala de equipamentos para acomodar os equipamentos internos, energia elétrica estabilizada) será disponibilizada pelo CONTRATANTE, possibilitando que a CONTRATADA instale seus equipamentos e faça os ajustes para a entrega do circuito, sempre sob supervisão e orientação do Gestor do Contrato ou outro servidor devidamente designado;

14.19.4. A CONTRATADA deverá responsabilizar-se pela execução e custeio de toda e qualquer obra de infraestrutura, interna e externa, necessárias para a execução da instalação. Será também de responsabilidade da CONTRATADA a recomposição original das instalações do CONTRATANTE, caso ocorram danos no momento da instalação. Ex: demolição e recomposição de gesso, emassamento e pintura, recomposição